Conselho da
União Europeia

Bruxelas, 6 de abril de 2016
(OR. en)

5418/16

Dossiê interinstitucional:
2012/0010 (COD)

DATAPROTECT 1
JAI 37
DAPIX 8
FREMP 3
COMIX 36
CODEC 51

ATOS LEGISLATIVOS E OUTROS INSTRUMENTOS

Assunto:	Posição do Conselho em primeira leitura tendo em vista a adoção da DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho

DIRETIVA (UE) 2016/…
DO PARLAMENTO EUROPEU E DO CONSELHO

de …

relativa à proteção das pessoas singulares
no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes
para efeitos de prevenção, investigação, deteção ou repressão
de infrações penais ou execução de sanções penais,
e à livre circulação desses dados,
e que revoga a Decisão-Quadro 2008/977/JAI do Conselho

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

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

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité das Regiões[1],

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

[1] JO C 391 de 18.12.2012, p. 127.
[2] Posição do Parlamento Europeu de 12 de março de 2014 (JO ...) e posição do Conselho de … . Posição do Parlamento Europeu de ... e decisão do Conselho de ... .

Considerando o seguinte:

(1) A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia ("Carta") e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

(2) Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, particularmente o direito à proteção dos dados pessoais. A presente diretiva destina-se a contribuir para a realização de um espaço de liberdade, segurança e justiça.

(3) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A partilha e a recolha de dados pessoais registaram um aumento significativo. A tecnologia permite o tratamento de dados pessoais numa escala sem precedentes para o exercício de funções como a prevenção, investigação, deteção ou repressão de infrações penais e a execução de sanções penais.

(4) A livre circulação de dados pessoais entre as autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública a nível da União, e a sua transferência para países terceiros e organizações internacionais deverão ser facilitadas, assegurando simultaneamente um elevado nível de proteção dos dados pessoais. Este contexto obriga ao estabelecimento de um regime de proteção de dados pessoais sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras.

(5) A Diretiva 95/46/CE do Parlamento Europeu e do Conselho[1] é aplicável a todo os tratamentos de dados pessoais nos Estados-Membros, nos setores público e privado. Não é, porém, aplicável ao tratamento de dados pessoais "no exercício de atividades não sujeitas à aplicação do direito comunitário", como as atividades realizadas nos domínios da cooperação judiciária em matéria penal e da cooperação policial.

(6) A Decisão-Quadro 2008/977/JAI do Conselho[2] é aplicável no domínio da cooperação judiciária em matéria penal e da cooperação policial. O seu âmbito de aplicação limita-se ao tratamento de dados pessoais transmitidos ou disponibilizados entre Estados-Membros.

---

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

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

(7) É crucial assegurar um nível elevado e coerente de proteção dos dados pessoais das pessoas singulares e facilitar o intercâmbio de dados pessoais entre as autoridades competentes dos Estados-Membros, a fim de assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação policial. Para tal, o nível de proteção dos direitos e liberdades individuais no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais – incluindo a salvaguarda e a prevenção de ameaças à segurança pública – deverá ser equivalente em todos os Estados-Membros. A proteção eficaz dos dados pessoais na União exige não só que sejam reforçados os direitos dos titulares dos dados e as obrigações de quem trata dados pessoais, mas também que haja reforço dos poderes equivalentes para controlar e assegurar a conformidade com as regras de proteção dos dados pessoais nos Estados-Membros.

(8) O artigo 16.º, n.º 2, do TFUE atribui ao Parlamento Europeu e ao Conselho a competência para estabelecerem regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, bem como as regras relativas à livre circulação desses dados.

(9) Nesse sentido, o Regulamento (UE) 2016/… do Parlamento Europeu e do Conselho[1*], estabelece regras gerais para proteger as pessoas singulares relativamente ao tratamento de dados pessoais e assegurar a livre circulação de dados pessoais na União.

(10) Na Declaração 21 sobre a proteção de dados pessoais no domínio da cooperação judiciária em matéria penal e da cooperação policial, anexada à Ata Final da Conferência Intergovernamental que adotou o Tratado de Lisboa, a conferência reconheceu que, atendendo à especificidade dos domínios em causa, poderão ser necessárias disposições específicas sobre proteção de dados pessoais e sobre a livre circulação dos dados pessoais, nos domínios da cooperação judiciária em matéria penal e da cooperação policial, com base no artigo 16.º do TFUE.

---

[1] Regulamento (UE) 2016/… do Parlamento Europeu e do Conselho, de …, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L …).

[*] JO: inserir o número do regulamento que consta no st 5419/16 e a referência de publicação.

(11) Por conseguinte, esses domínios deverão ser objeto de uma diretiva que estabeleça regras específicas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, no respeito da natureza específica dessas atividades. Essas autoridades competentes podem incluir não só as autoridades públicas como, por exemplo, as autoridades judiciárias, a polícia ou outras autoridades de aplicação da lei, mas também outros organismos ou entidades designados pelo direito dos Estados-Membros para o exercício da autoridade e dos poderes públicos para efeitos da presente diretiva. Caso esses organismos ou entidades tratem dados pessoais para efeitos que não sejam os da presente diretiva, é aplicável o Regulamento (UE) 2016/…[*]. O Regulamento (UE) 2016/…[*] é, pois, aplicável nos casos em que um organismo ou uma entidade recolhe dados pessoais para outros efeitos e, em seguida, os trata a fim de dar cumprimento a uma obrigação legal a que está sujeito. Pode ser o caso das instituições financeiras quando retêm, para efeitos de investigação, deteção ou repressão de infrações penais, certos dados pessoais por si tratados e os fornecem apenas às autoridades nacionais competentes em casos específicos e nos termos do direito dos Estados-Membros. Os organismos ou entidades que tratam dados pessoais em nome dessas autoridades no âmbito da presente diretiva deverão estar vinculados por contrato ou por outro ato jurídico e pelas disposições aplicáveis aos subcontratantes nos termos da presente diretiva, sem prejuízo da aplicação do Regulamento (UE) 2016/…[*] ao tratamento de dados pessoais pelo subcontratante não abrangido pela presente diretiva.

[*] JO: inserir o número do regulamento que consta no st 5419/16.

(12) As funções de polícia ou de outras autoridades de aplicação da lei centram-se principalmente na prevenção, investigação, deteção ou repressão de infrações penais, incluindo as atividades policiais sem conhecimento prévio de que um incidente constitui ou não uma infração penal. Estas funções podem incluir o exercício da autoridade através de medidas coercivas, tais como as atividades da polícia em manifestações, grandes eventos desportivos e distúrbios. Essas funções incluem também a manutenção da ordem pública enquanto atribuição da polícia ou de outras autoridades de aplicação da lei, quando necessárias para a salvaguarda e prevenção de ameaças à segurança pública e aos interesses fundamentais da sociedade protegidos por lei, e à prática de infrações penais. Os Estados-Membros podem atribuir às autoridades competentes outras funções que não sejam necessariamente executadas para efeitos de prevenção, investigação, deteção ou repressão de infrações penais, nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública, de modo que o tratamento dos dados pessoais para esses outros efeitos, na medida em que se insira na esfera do direito da União, seja abrangido pelo âmbito de aplicação do Regulamento (UE) 2016/…*.

(13) O conceito de infração penal, na aceção da presente diretiva, deverá ser um conceito autónomo do direito da União, tal como interpretado pelo Tribunal de Justiça da União Europeia ("Tribunal de Justiça").

* JO: inserir o número do regulamento que consta no st 5419/16.

(14) Uma vez que a presente diretiva não deverá aplicar-se ao tratamento de dados pessoais efetuado no exercício de atividades não sujeitas ao direito da União, não deverão ser consideradas atividades abrangidas pela presente diretiva as atividades relacionadas com a segurança nacional e as atividades das agências ou unidades que se dedicam a questões de segurança nacional e ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades inseridas no âmbito de aplicação do Título V, Capítulo 2, do Tratado da União Europeia (TUE).

(15) A fim de assegurar o mesmo nível de proteção para as pessoas singulares através de direitos suscetíveis de proteção judicial no conjunto da União e evitar divergências que criem obstáculos ao intercâmbio de dados pessoais entre as autoridades competentes, a presente diretiva deverá prever regras harmonizadas para a proteção e a livre circulação de dados pessoais tratados para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública. A aproximação das legislações dos Estados-Membros não deverá implicar uma diminuição da proteção dos dados pessoais, devendo, pelo contrário, ter por objetivo garantir um elevado nível de proteção na União. Os Estados-Membros não deverão ser impedidos de prever garantias mais elevadas do que as estabelecidas na presente diretiva para a proteção dos direitos e liberdades do titular dos dados no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes.

(16) A presente diretiva não prejudica o princípio do direito de acesso do público aos documentos oficiais. Ao abrigo do Regulamento (UE) 2016/…*, os dados pessoais que constem de documentos oficiais na posse de uma autoridade pública ou de um organismo público ou privado para o exercício de funções de interesse público podem ser divulgados por essa autoridade ou organismo nos termos do direito da União ou do Estado-Membro que for aplicável à autoridade ou organismo público, a fim de conciliar o acesso do público a documentos oficiais com o direito à proteção dos dados pessoais.

(17) A proteção conferida pela presente diretiva deverá abranger as pessoas singulares, independentemente da sua nacionalidade ou lugar de residência, relativamente ao tratamento dos seus dados pessoais.

(18) A fim de se evitar um sério risco de ser contornada, a proteção das pessoas singulares deverá ser neutra em termos tecnológicos e não deverá depender das técnicas utilizadas. A proteção das pessoas singulares deverá aplicar-se ao tratamento de dados pessoais por meios automatizados, bem como ao tratamento manual se os dados pessoais estiverem contidos ou se destinarem a um ficheiro. Os ficheiros ou conjuntos de ficheiros, bem como as suas capas, que não estejam estruturados de acordo com critérios específicos, não deverão ser incluídos no âmbito de aplicação da presente diretiva.

* JO: inserir o número do regulamento que consta no st 5419/16.

(19) O Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho[1] aplica-se ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n.º 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, deverão ser adaptados aos princípios e regras do Regulamento (UE) 2016/…[*].

(20) A presente diretiva não obsta a que os Estados-Membros especifiquem as operações e os procedimentos de tratamento na legislação processual penal nacional no que se refere ao tratamento de dados pessoais pelos tribunais e as outras autoridades judiciais, em particular no que respeita aos dados pessoais que constem de uma decisão judicial ou de um registo relacionado com uma ação penal.

---

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

[*] JO: inserir o número do regulamento que consta no st 5419/16.

(21) Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios que possam ser razoavelmente utilizados, quer pelo responsável pelo tratamento quer por qualquer outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta tanto a tecnologia disponível à data do tratamento dos dados como a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, isto é, informações que não digam respeito a nenhuma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal forma anónimos que o seu titular já não possa ser identificado.

(22) As autoridades públicas a quem os dados pessoais forem divulgados de acordo com obrigações jurídicas no exercício da sua missão oficial, tais como as autoridades fiscais e aduaneiras, as unidades de investigação financeira, as autoridades administrativas independentes, ou as autoridades dos mercados financeiros, responsáveis pela regulamentação e supervisão dos mercados de valores mobiliários não poderão ser consideradas destinatárias se receberem dados pessoais que forem necessários para efetuar um inquérito específico de interesse geral, em conformidade com o direito da União ou dos Estados-Membros. Os pedidos de divulgação enviados pelas autoridades públicas deverão ser sempre feitos por escrito, fundamentados e ocasionais e não deverão dizer respeito à totalidade de um ficheiro ou levar à interconexão de ficheiros. O tratamento de dados pessoais por essas autoridades públicas deverá estar em conformidade com as regras de proteção de dados aplicáveis de acordo com as finalidades do tratamento.

(23) Os dados genéticos deverão ser definidos como todos os dados pessoais relacionados com as características genéticas, hereditárias ou adquiridas, de uma pessoa, e que dão informações únicas sobre a fisionomia ou a saúde do indivíduo, resultantes, designadamente, da análise de cromossomas, do ácido desoxirribonucleico (ADN), do ácido ribonucleico (ARN) ou de qualquer outro elemento que permita obter informações equivalentes. Tendo em conta a complexidade e a natureza sensível das informações genéticas, existe um elevado risco de utilização injustificada e de reutilização para diversos fins não autorizados por parte do responsável pelo tratamento. As discriminações com base em características genéticas deverão ser proibidas.

(24) Deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. Tal abrange informações sobre a pessoa singular recolhidas durante a sua inscrição para a prestação de serviços de saúde e durante essa prestação a que se refere a Diretiva 2011/24/UE do Parlamento Europeu e do Conselho[1] em relação a uma pessoas singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir dados genéticos e amostras biológicas; ou quaisquer informações sobre, por exemplo, uma doença, deficiência, risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico atual do titular dos dados, independentemente da sua fonte, por exemplo um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico *in vitro*.

---

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

(25) Todos os Estados-Membros fazem parte da Organização Internacional da Polícia Criminal (Interpol). No exercício das suas atribuições, a Interpol recebe, conserva e divulga dados pessoais a fim de auxiliar as autoridades competentes na prevenção e no combate à criminalidade internacional. Por conseguinte, é conveniente reforçar a cooperação entre a União e a Interpol mediante a promoção de um eficaz intercâmbio de dados pessoais, assegurando ao mesmo tempo o respeito pelos direitos e liberdades fundamentais no que se refere ao tratamento dos dados pessoais. Caso sejam transferidos dados pessoais da União para a Interpol e para países que destacaram membros para a Interpol, a presente diretiva deverá aplicar-se, em particular, no que diz respeito às disposições sobre transferências internacionais. A presente diretiva não deverá prejudicar as regras específicas previstas na Posição Comum 2005/69/JAI do Conselho[1] e na Decisão 2007/533/JAI do Conselho[2].

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

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

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

(27) Para efeitos de prevenção, investigação ou repressão de infrações penais, é necessário que as autoridades competentes tratem os dados pessoais, recolhidos no contexto da prevenção, investigação, deteção ou repressão de infrações penais específicas para além desse contexto, a fim de obter uma melhor compreensão das atividades criminais e de estabelecer ligações entre as diferentes infrações penais detetadas.

(28) A fim de preservar a segurança do tratamento e de evitar o tratamento em violação da presente diretiva, os dados pessoais deverão ser tratados de uma forma que garanta um nível adequado de segurança e confidencialidade, nomeadamente para evitar o acesso ou a utilização desses dados e do equipamento utilizado para o seu tratamento por parte de pessoas não autorizadas, e que tenha em conta as técnicas e tecnologias mais avançadas, os custos da sua aplicação em função dos riscos e a natureza dos dados pessoais a proteger.

(29) Os dados pessoais deverão ser recolhidos para finalidades determinadas, explícitas e legítimas abrangidas pelo âmbito de aplicação da presente diretiva e não deverão ser tratados para fins incompatíveis com os da prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais – nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública. Se os dados pessoais forem tratados, pelo mesmo ou por outro responsável pelo tratamento, para uma finalidade abrangida pelo âmbito de aplicação da presente diretiva que não aquela para a qual foram recolhidos, esse tratamento deverá ser permitido, na condição de que esse tratamento seja autorizado em conformidade com as disposições legais aplicáveis e necessário e proporcionado para a prossecução dessa outra finalidade.

(30) É conveniente aplicar o princípio da exatidão dos dados tendo em conta a natureza e a finalidade do tratamento em causa. Especialmente quando se trata de processos judiciais, as declarações que contêm dados pessoais são baseadas em perceções subjetivas da pessoa singular e nem sempre são verificáveis. Este princípio não deverá, por conseguinte, aplicar-se à exatidão da própria declaração, mas simplesmente ao facto de tal declaração ter sido feita.

(31) O tratamento de dados pessoais nos domínios da cooperação judiciária em matéria penal e da cooperação policial implica necessariamente o tratamento de dados pessoais relativos a categorias diferentes de titulares de dados. Importa, portanto, estabelecer, se aplicável e tanto quanto possível, uma clara distinção entre dados pessoais de diferentes categorias de titulares de dados, tais como suspeitos, pessoas condenadas por um crime, vítimas e terceiros, designadamente testemunhas, pessoas que detenham informações ou contactos úteis, e os cúmplices de pessoas suspeitas ou condenadas. Tal não deverá impedir a aplicação do direito à presunção de inocência, tal como garantido pela Carta e pela CEDH, de acordo com a interpretação da jurisprudência do Tribunal de Justiça e do Tribunal Europeu dos Direitos do Homem, respetivamente.

(32) As autoridades competentes deverão assegurar que não sejam transmitidos nem disponibilizados dados pessoais incorretos, incompletos ou desatualizados. A fim de assegurar a proteção das pessoas singulares e a exatidão, exaustividade ou atualidade e fiabilidade dos dados pessoais transmitidos ou disponibilizados, as autoridades competentes deverão acrescentar, na medida do possível, as informações necessárias em todas as transmissões de dados pessoais.

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

(34) O tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais – incluindo a salvaguarda e a prevenção de ameaças à segurança pública – deverá abranger qualquer operação ou conjunto de operações efetuadas sobre dados pessoais ou conjuntos de dados pessoais para esses efeitos, com ou sem meios automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comparação ou interconexão, a limitação do tratamento, o apagamento ou a destruição. As regras previstas na presente diretiva deverão, em especial, aplicar-se à transmissão de dados pessoais para as finalidades nela previstas aos destinatários a que esta se não aplique. Tais destinatários são as pessoas singulares ou coletivas, autoridades públicas, agências ou qualquer outro organismo a que os dados tenham sido disponibilizados de forma lícita pela autoridade competente. Caso os dados tenham sido inicialmente recolhidos por uma autoridade competente para uma das finalidades prosseguidas pela presente diretiva, o Regulamento (UE) 2016/…[*] deverá aplicar-se ao tratamento desses dados para fins que não os da presente diretiva se tal tratamento for autorizado pelo direito da União ou dos Estados-Membros. As regras previstas no Regulamento (UE) 2016/…[*] deverão, em especial, aplicar-se à transmissão de dados pessoais para fins que se não insiram no âmbito de aplicação da presente diretiva. O Regulamento (UE) 2016/…[*] deverá aplicar-se ao tratamento de dados pessoais por um destinatário que não seja uma autoridade competente ou que não atue nessa qualidade, na aceção da presente diretiva, e à qual os dados pessoais sejam disponibilizados de forma lícita por uma autoridade competente. Ao transporem a presente diretiva, os Estados-Membros deverão também especificar mais pormenorizadamente a aplicação das regras do Regulamento (UE) 2016/…[*], sob reserva das condições nele previstas.

[*] JO: inserir o número do regulamento que consta no st 5419/16.

(35) Para ser lícito, o tratamento de dados pessoais nos termos da presente diretiva deverá ser necessário para a execução de uma missão de interesse público por uma autoridade competente com base no direito da União ou dos Estados-Membros para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Estas funções deverão abranger a proteção dos interesses vitais do titular dos dados. O exercício das funções de prevenção, investigação, deteção ou repressão de infrações penais conferidas institucionalmente por lei às autoridades competentes permite-lhes exigir que as pessoas singulares cumpram o que lhes é solicitado. Neste caso, o consentimento do titular dos dados, na aceção do Regulamento (UE) 2016/…*, não deverá constituir a fundamento jurídico do tratamento de dados pessoais pelas autoridades competentes. Caso seja obrigado a cumprir uma obrigação legal, o titular dos dados não tem verdadeira liberdade de escolha, pelo que a sua reação não poderá ser considerada uma livre manifestação da sua vontade. Tal não deverá obstar a que os Estados-Membros prevejam por lei a possibilidade de o titular dos dados consentir que os seus dados pessoais sejam tratados para as finalidades previstas na presente diretiva, nomeadamente que sejam efetuados testes de ADN no âmbito de investigações penais ou controlada a sua localização por meio de etiquetas eletrónicas tendo em vista a execução de sanções penais.

* JO: inserir o número do regulamento que consta no st 5419/16.

(36) Os Estados-Membros deverão prever que, caso o direito da União ou dos Estados-Membros aplicável à autoridade transmissora competente preveja condições específicas aplicáveis em circunstâncias específicas ao tratamento de dados pessoais, como a utilização de códigos de tratamento, a autoridade competente deverá informar o destinatário dos dados pessoais dessas condições e da obrigação de as respeitar. Tais condições poderão, por exemplo, incluir a proibição de transmitir os dados pessoais a terceiros, ou que sejam utilizados para fins que não os fins para os quais foram transmitidos, ou, ainda, não informar o titular dos dados em caso de limitação do direito de obter informações sem a aprovação prévia da autoridade transmissora competente. Essas obrigações deverão aplicar-se igualmente às transferências da autoridade transmissora competente para destinatários situados em países terceiros ou para organizações internacionais. Os Estados-Membros deverão assegurar que essa autoridade competente não aplique a destinatários situados noutros Estados-Membros nem a agências, organismos e órgãos criados nos termos do Título V, Capítulos 4 e 5, do TFUE condições diferentes das aplicáveis a transmissões de dados similares no Estado-Membro da autoridade transmissora competente.

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

(38) O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão que avalie aspetos pessoais que lhe digam respeito e se baseie exclusivamente no tratamento automatizado, com efeitos legais que lhe sejam adversos ou o afetem de forma significativa. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, incluindo informação específica ao titular dos dados e o direito de obter a intervenção humana e, em especial, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação ou de contestar a decisão. A definição de perfis que conduza a discriminação contra pessoas singulares com base em dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, deverá ser proibida, nas condições estabelecidas nos artigos 21.º e 52.º da Carta.

(39) Para que os titulares de dados possam exercer os seus direitos, as informações que lhes sejam dirigidas, inclusive no sítio web do responsável pelo tratamento, deverão ser de fácil acesso e compreensão e formuladas em termos claros e simples. Essas informações deverão ser adaptadas às necessidades das pessoas vulneráveis, como as crianças.

(40) Deverão ser previstas regras para facilitar o exercício, pelo titular dos dados, dos direitos que lhe são conferidos pelas disposições adotadas por força da presente diretiva, incluindo procedimentos para solicitar, a título gratuito, o acesso aos seus dados pessoais e a sua retificação e apagamento dos dados pessoais e a limitação do tratamento. O responsável pelo tratamento deverá ser obrigado a responder aos pedidos do titular dos dados sem demora injustificada, salvo se aplicar limitações aos direitos do mesmo em conformidade com a presente diretiva. Além disso, se os pedidos forem manifestamente infundados ou excessivos, por exemplo quando o titular dos dados solicitar informações de forma injustificada e repetida ou abusar do seu direito a receber informações, nomeadamente prestando informações falsas ou suscetíveis de induzir em erro, o responsável pelo tratamento deverá poder cobrar uma taxa razoável ou recusar dar seguimento ao pedido.

(41) Caso o responsável pelo tratamento solicite que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados, essas informações deverão ser tratadas apenas para essa finalidade específica e não deverão ser conservadas durante mais tempo do que o necessário para o efeito.

(42) Deverão ser facultadas ao titular dos dados pelo menos as seguintes informações: a identidade do responsável pelo tratamento, a existência da operação de tratamento, as finalidades do tratamento, o direito de apresentar reclamação e a existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais e a sua retificação ou apagamento ou a limitação do tratamento. Tal poderá ser efetuado no sítio web da autoridade competente. Além disso, em casos específicos e no intuito de que seja permitido o exercício dos seus direitos, o titular dos dados deverá ser informado sobre o fundamento jurídico do tratamento e a duração da conservação dos dados, na medida em que tais informações adicionais sejam necessárias, tendo em conta as circunstâncias específicas em que os dados são tratados, a fim de garantir a lealdade do tratamento no que respeita ao titular dos dados.

(43) As pessoas singulares deverão ter o direito de aceder aos dados recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de tomar conhecimento do tratamento e verificar a sua licitude. Por conseguinte, cada titular de dados deverá ter o direito de ser informado das finalidades a que se destina o tratamento dos seus dados, da sua duração e de quem são os destinatários, inclusive em países terceiros. Nos casos em que essa comunicação inclua informações relativas à origem dos dados pessoais, tais informações não deverão revelar a identidade das pessoas singulares, em especial de fontes confidenciais. Para que esse direito seja respeitado, basta que o titular dos dados esteja na posse de um resumo completo desses dados num formulário inteligível, ou seja, um formulário que permita que o titular dos dados tome conhecimento desses dados e verifique a sua exatidão e o seu tratamento em conformidade com a presente diretiva, de modo a que possa exercer os direitos que esta lhe confere. Esse resumo poderá ser concedido por via de uma cópia dos dados pessoais sujeitos a tratamento.

(44) Os Estados-Membros deverão poder adotar medidas legislativas que visem atrasar, limitar ou recusar a informação prestada a titulares de dados ou restringir, total ou parcialmente, o acesso aos dados pessoais que lhes digam respeito, desde que tal constitua uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos da pessoa singular em causa, para não prejudicar os inquéritos, investigações ou procedimentos oficiais ou legais, procurar não prejudicar a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais, salvaguardar a segurança pública ou a segurança nacional ou ainda proteger os direitos e as liberdades de terceiros. O responsável pelo tratamento deverá avaliar, através de uma análise concreta de cada caso individualmente, se o direito de acesso deverá ser total ou parcialmente restringido.

(45) As recusas ou restrições do acesso deverão, em princípio, ser comunicadas por escrito ao titular dos dados com os motivos de facto ou de direito que fundamentam a decisão.

(46) As restrições dos direitos do titular dos dados devem respeitar a Carta e a CEDH, de acordo com a interpretação na jurisprudência do Tribunal de Justiça e do Tribunal Europeu dos Direitos do Homem, respetivamente, e devem respeitar, em particular, o conteúdo essencial desses direitos e liberdades.

(47) As pessoas singulares deverão ter direito a que os dados inexatos que lhe dizem respeito sejam retificados, em especial no que diz respeito a factos, e a que sejam apagados, caso o seu tratamento não seja conforme com o disposto na presente diretiva. No entanto, o direito de retificação não deverá afetar, por exemplo, o conteúdo do depoimento de uma testemunha. As pessoas singulares deverão ter direito a que o tratamento seja limitado, sempre que conteste a exatidão dos dados pessoais e não possa ser apurado se os dados são exatos ou não ou, ainda, quando os dados pessoais tiverem de ser conservados para efeitos de prova. Em particular, os dados pessoais não deverão ser apagados, mas apenas limitados se, num dado caso, existirem motivos razoáveis para crer que o seu apagamento poderá prejudicar interesses legítimos do titular. Nesse caso, os dados limitados só deverão ser tratados para a finalidade que impediu o seu apagamento. Para limitar o tratamento de dados pessoais pode recorrer-se a métodos como a transferência de determinados dados para outro sistema de tratamento, nomeadamente para efeitos de arquivo, ou impedir o acesso a esses dados. Nos ficheiros automatizados, as limitações ao tratamento deverão, em princípio, ser impostas por meios técnicos; deverá ser indicado de forma bem clara no sistema que o tratamento dos dados pessoais está sujeito a limitações. Tal retificação ou apagamento dos dados pessoais ou a limitação do tratamento deverão ser comunicados aos destinatários a quem os dados tenham sido divulgados e às autoridades competentes que estão na origem dos dados inexatos. Os responsáveis pelo tratamento deverão igualmente abster-se de qualquer comunicação ulterior desses dados.

(48) Caso o responsável pelo tratamento recuse ao titular dos dados o direito à informação, o acesso aos dados pessoais ou a sua retificação ou apagamento ou a limitação do tratamento, o titular dos dados deverá ter o direito de solicitar que a autoridade nacional de controlo verifique a licitude do tratamento. O titular dos dados deverá ser informado desse direito. Quando a autoridade de controlo agir em nome do titular dos dados, deverá, pelo menos, informá-lo de que foram realizadas todas as verificações ou revisões necessárias. A autoridade de controlo deverá também informar o titular de dados do seu direito de intentar ação judicial.

(49) Caso os dados pessoais sejam tratados no âmbito de uma investigação criminal ou de um processo judicial em matéria penal, os Estados-Membros deverão poder dispor que o exercício do direito à informação, ao acesso aos dados pessoais e à sua retificação ou apagamento, bem como à limitação do tratamento, seja feito nos termos das regras nacionais aplicáveis aos processos judiciais.

(50) Deverá ser estabelecida a responsabilidade do responsável pelo tratamento de dados pessoais realizado por si próprio ou em seu nome. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas adequadas e eficazes e deverá estar em condições de demonstrar que as atividades de tratamento são efetuadas em conformidade com a presente diretiva. Tais medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento de dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares. As medidas tomadas pelo responsável pelo tratamento deverão incluir a elaboração e execução de garantias específicas para o tratamento de dados pessoais de pessoas singulares vulneráveis, como crianças.

(51) Os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderão resultar de operações de tratamento de dados suscetíveis de causar danos físicos, materiais ou morais, em especial caso o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a outros prejuízos importantes de natureza económica ou social; ou caso os titulares dos dados possam ficar privados dos seus direitos e liberdades ou do exercício do controlo sobre os respetivos dados pessoais; caso sejam tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical; caso sejam tratados dados genéticos ou dados biométricos a fim de identificar uma pessoa de forma inequívoca ou caso sejam tratados dados relativos à saúde ou à vida sexual ou orientação sexual ou, ainda, a condenações e infrações penais ou medidas de segurança conexas; caso sejam avaliados aspetos de natureza pessoal, nomeadamente análises e previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; ou caso sejam tratados dados pessoais de pessoas singulares vulneráveis, em particular crianças; ou caso o tratamento incida sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados.

(52) A probabilidade e a gravidade dos riscos deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento. Os riscos deverão ser aferidos com base numa avaliação objetiva, de modo a determinar se é provável que as operações de tratamento de dados impliquem um risco elevado. Entende-se por "risco elevado" um risco particular que prejudique os direitos e liberdades dos titulares de dados.

(53) A proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige que sejam tomadas medidas técnicas e organizativas adequadas para assegurar o cumprimento dos requisitos da presente diretiva. A execução dessas medidas não poderá depender exclusivamente de considerações económicas. A fim de poder demonstrar a conformidade com a presente diretiva, o responsável pelo tratamento deverá adotar diretrizes internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a conceção e da proteção de dados por defeito. Sempre que o responsável pelo tratamento tenha efetuado uma avaliação do impacto na proteção de dados nos termos da presente diretiva, os resultados da referida avaliação deverão ser tidos em conta para efeitos de desenvolvimento dessas medidas e procedimentos. As medidas poderão incluir, nomeadamente, o recurso à pseudonimização, efetuada o mais cedo possível. O recurso à pseudonimização para efeitos da presente diretiva poderá facilitar, designadamente, a livre circulação de dados pessoais no espaço de liberdade, segurança e justiça.

(54) A proteção dos direitos e liberdades dos titulares de dados, bem como a responsabilidade dos responsáveis pelo tratamento e dos subcontratantes, inclusive no que diz respeito à supervisão e às medidas adotadas pelas autoridades de controlo, exigem uma clara repartição de responsabilidades nos termos da presente diretiva, designadamente caso o responsável pelo tratamento dos dados determine as finalidades e os meios do tratamento conjuntamente com outros responsáveis ou uma operação de tratamento de dados seja efetuada em nome de um responsável pelo tratamento.

(55) O tratamento executado por um subcontratante deverá ser regido por um ato jurídico, que pode ser um contrato que vincule o subcontratante ao responsável pelo tratamento e estipule, nomeadamente, que o subcontratante só deverá agir segundo instruções do responsável pelo tratamento. O subcontratante deverá ter em consideração o princípio da proteção de dados desde a conceção e por defeito.

(56) A fim de comprovar o cumprimento da presente diretiva, o responsável pelo tratamento ou o subcontratante deverá manter registos de todas as categorias de atividades de tratamento sob a sua responsabilidade. Os responsáveis pelo tratamento dos dados e os subcontratantes deverão ser obrigados a cooperar com a autoridade de controlo e a facultar-lhe esses registos, a pedido, para fiscalização dessas operações de tratamento. O responsável pelo tratamento ou o subcontratante que trate dados pessoais em sistemas de tratamento não automatizados deverá dispor de métodos eficazes, tais como registos cronológicos ou outros, para demonstrar a licitude do tratamento, permitir o autocontrolo e garantir a integridade e segurança dos dados.

(57) Deverão ser conservados registos cronológicos pelo menos de operações em sistemas de tratamento automatizado, como a recolha, alteração, consulta, divulgação – incluindo transferências –, interconexão ou apagamento. A identificação da pessoa que consultou ou divulgou dados pessoais deverá ser registada e a partir dessa identificação será talvez possível determinar a justificação das operações de tratamento. Os registos cronológicos deverão ser utilizados exclusivamente para efeitos de verificação da licitude do tratamento, autocontrolo, garantia da integridade e segurança dos dados e ações penais. O autocontrolo abrange igualmente as ações disciplinares internas das autoridades competentes.

(58) Deverá ser efetuada uma avaliação do impacto na proteção de dados pelo responsável pelo tratamento quando as operações de tratamento forem suscetíveis de criar um risco elevado para os direitos e liberdades dos titulares dos dados devido à sua natureza, âmbito ou finalidades, a qual deve incluir, em particular, as medidas previstas, as garantias e os mecanismos previstos para assegurar a proteção dos dados pessoais e demonstrar a conformidade com a presente diretiva. As avaliações do impacto deverão ter como objeto os sistemas e processos pertinentes das operações de tratamento, mas não casos individuais.

(59) A fim de assegurar a proteção efetiva dos direitos e liberdades dos titulares dos dados, o responsável pelo tratamento ou o subcontratante deverá, em certos casos, consultar a autoridade de controlo antes do tratamento.

(60) A fim de preservar a segurança e evitar o tratamento em violação da presente diretiva, o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e deverá aplicar medidas que os atenuem, como, por exemplo, a cifragem. Estas medidas deverão assegurar um nível de segurança adequado, nomeadamente no que respeita à confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função do risco e da natureza dos dados pessoais a proteger. Ao avaliar os riscos para a segurança dos dados, deverão ser tidos em conta os riscos apresentados pelo tratamento dos dados, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados, de dados pessoais transmitidos, conservados ou tratados de outro modo, riscos esses que podem conduzir, em particular, a danos físicos, materiais ou morais. O responsável pelo tratamento e o subcontratante deverão assegurar que o tratamento de dados pessoais não seja efetuado por pessoas não autorizadas.

(61) Se não forem tomadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, tais como a perda de controlo dos dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação de identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social importante para as pessoas singulares em causa. Por conseguinte, logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, deverá comunicá--la à autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar, em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares. Se não for possível efetuar a comunicação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem mais demora injustificada.

(62) Caso a violação de dados pessoais seja suscetível de criar um elevado risco para os direitos e liberdades das pessoas singulares, estas deverão ser informadas sem demora injustificada, a fim de permitir que tomem as precauções necessárias. Da comunicação deverá constar a natureza da violação de dados pessoais e recomendações destinadas à pessoa singular em causa para atenuar potenciais efeitos adversos. A comunicação aos titulares dos dados deverá ser feita o mais rapidamente possível, em estreita cooperação com a autoridade de controlo, e de acordo com as orientações fornecidas por esta ou por outras autoridades competentes. Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá que se envie uma comunicação rápida aos titulares dos dados, enquanto a necessidade de aplicar medidas adequadas contra violações de dados recorrentes ou similares poderá justificar um prazo maior para a comunicação. Se não for possível, através do atraso ou da restrição da comunicação à pessoa singular em causa de uma violação de dados pessoais, evitar criar entraves a inquéritos, investigações ou procedimentos oficiais ou legais, evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais, salvaguardar a segurança pública, preservar a segurança nacional ou ainda proteger os direitos e as liberdades de terceiros, essa comunicação poderá, em circunstâncias excecionais, ser omitida.

(63) O responsável pelo tratamento deverá designar uma pessoa para o assistir no controlo do cumprimento, a nível interno, das disposições adotadas por força da presente diretiva. Os Estados-Membros poderão isentar desta obrigação os tribunais e outras autoridades judiciais independentes no exercício da sua função jurisdicional. Essa pessoa pode ser um membro do pessoal do responsável pelo tratamento, que tenha recebido uma formação específica no domínio da legislação e das práticas em matéria de proteção de dados a fim de adquirir conhecimentos especializados nesta matéria. O nível de conhecimentos especializados necessários deverá ser determinado, em particular, em função do tratamento de dados efetuado e da proteção exigida para os dados pessoais tratados pelo responsável pelo tratamento. As suas funções podem ser exercidas a tempo parcial ou a tempo inteiro. Um encarregado da proteção de dados poderá ser nomeado conjuntamente por vários responsáveis pelo tratamento, tendo em conta a dimensão e estrutura organizativa destes, por exemplo no caso de partilha de recursos em unidades centrais. Essa pessoa pode igualmente ser nomeada para diferentes funções no interior das estruturados responsáveis pelo tratamento . Essa pessoa deverá ajudar o responsável pelo tratamento e os empregados que tratem dados pessoais, informando-os e aconselhando-os a respeito do cumprimento das suas obrigações relevantes em matéria de proteção de dados. Essas pessoas encarregadas da proteção de dados deverão estar em condições de desempenhar as suas funções e cumprir os seus deveres de forma independente e de acordo com o direito dos Estados-Membros.

(64) Os Estados-Membros deverão assegurar que as transferências para um país terceiro ou para uma organização internacional só possam ser realizadas se forem necessárias para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais – nomeadamente, a salvaguarda e a prevenção de ameaças à segurança pública – e se o responsável pelo tratamento no país terceiro ou na organização internacional for uma autoridade competente na aceção da presente diretiva. Apenas as autoridades competentes, na qualidade de responsáveis pelo tratamento, podem efetuar transferências, salvo se os subcontratantes tiverem instruções explícitas para efetuar a transferência em causa por conta dos responsáveis pelo tratamento. Tal transferência pode ser efetuada caso a Comissão tenha decidido que o país terceiro ou a organização internacional em causa garante um nível de proteção adequado, ou quando tiverem sido apresentadas garantias adequadas ou forem aplicáveis derrogações em situações específicas. Caso os dados pessoais sejam transferidos da União para responsáveis pelo tratamento de dados, para subcontratantes ou para outros destinatários em países terceiros ou organizações internacionais, o nível de proteção das pessoas singulares assegurado na União pela presente diretiva deverá continuar a ser garantido, inclusive nos casos de posterior transferência de dados pessoais do país terceiro ou da organização internacional em causa para responsáveis pelo tratamento de dados, ou subcontratantes desse país terceiro ou de outro, ou para uma organização internacional.

(65) Caso sejam transferidos dados pessoais de um Estado-Membro para países terceiros ou organizações internacionais, essa transferência apenas deverá, em princípio, ser efetuada depois de o Estado-Membro de onde provêm os dados ter dado a sua autorização. O interesse de uma cooperação eficiente em matéria de aplicação da lei exige que, caso a natureza de uma ameaça à segurança pública de um Estado-Membro ou país terceiro ou aos interesses essenciais de um Estado-Membro seja tão iminente que impossibilite a obtenção de autorização prévia em tempo útil, a autoridade competente deva poder transferir os dados pessoais pertinentes para o país terceiro ou a organização internacional em causa sem essa autorização prévia. Os Estados-Membros deverão prever que sejam comunicadas aos países terceiros ou às organizações internacionais as condições específicas relativas à transferência. As transferências ulteriores de dados pessoais deverão ser submetidas a autorização prévia pela autoridade competente que realizou a transferência inicial. Ao decidir sobre um pedido de autorização para uma transferência ulterior, a autoridade competente que realizou a transferência inicial deverá ter devidamente em conta todos os fatores relevantes, designadamente a gravidade da infração penal, as condições específicas associadas e a finalidade para a qual os dados foram inicialmente transferidos, a natureza e as condições de execução da sanção penal e o nível de proteção de dados pessoais do país terceiro ou da organização internacional para os quais os dados pessoais são ulteriormente transferidos. A autoridade competente que realizou a transferência inicial poderá igualmente sujeitar a transferência ulterior a condições específicas. Tais condições específicas podem ser descritas, por exemplo, em códigos de tratamento.

(66) A Comissão poderá decidir, com efeitos no conjunto da União, que determinados países terceiros, um território ou um ou vários setores especificados num país terceiro ou numa organização internacional asseguram um nível adequado de proteção de dados, garantindo assim a segurança jurídica e a uniformidade a nível da União relativamente a países terceiros ou organizações internacionais que sejam considerados aptos a assegurar tal nível de proteção. Nesses casos, poderão ser feitas transferências de dados pessoais para esses países sem necessidade de qualquer autorização específica, exceto se outro Estado-Membro de onde provêm os dados tiver de dar a sua autorização à transferência.

(67) De acordo com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou de um setor específico num país terceiro, ter em consideração em que medida um determinado país respeita o primado do Estado de direito, o acesso à justiça, bem como as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. A adoção de uma decisão de adequação relativa a um território ou um setor específico num país terceiro deverá ter em conta critérios claros e objetivos, tais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro. Este deverá dar garantias de assegurar um nível adequado de proteção, essencialmente equivalente ao assegurado na União, em particular quando os dados são tratados num ou em vários setores específicos. Em especial, o país terceiro deverá garantir o controlo efetivo e independente da proteção dos dados e estabelecer mecanismos de cooperação com as autoridades s de proteção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial.

(68) Além dos compromissos internacionais assumidos pelo país terceiro ou pela organização internacional, a Comissão deverá também ter em conta as obrigações decorrentes da participação do país terceiro ou da organização internacional nos sistemas multilaterais ou regionais, em especial no que diz respeito à proteção dos dados pessoais, bem como o cumprimento de tais obrigações. Em especial, há que ter em conta a adesão do país terceiro em causa à Convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal, de 28 de janeiro de 1981, e respetivo Protocolo Adicional. A Comissão deverá consultar o Comité Europeu para a Proteção de Dados criado pelo Regulamento (UE) 2016/…[*] ("Comité") quando avalia o nível de proteção nos países terceiros ou organizações internacionais. A Comissão deverá ter igualmente em conta as decisões de adequação da Comissão pertinentes, adotadas em conformidade com o artigo 41.º do Regulamento (UE) 2016/…[*].

(69) A Comissão deverá controlar a eficácia das decisões sobre o nível de proteção assegurado num país terceiro, num território ou num setor específico de um país terceiro, ou numa organização internacional. Nas suas decisões de adequação, a Comissão deverá prever um processo de avaliação periódica da aplicação destas. A avaliação periódica deverá ser feita em consulta com o país terceiro ou a organização internacional em questão e ter em conta todos os desenvolvimentos pertinentes verificados no país terceiro ou organização internacional.

[*] JO: inserir o número do regulamento que consta no st 5419/16.

(70) A Comissão deverá igualmente poder reconhecer que um país terceiro, um território ou um setor específico de um país terceiro, ou uma organização internacional, deixou de assegurar um nível adequado de proteção de dados. Se for esse o caso, deverá ser proibida a transferência de dados pessoais para esse país terceiro ou organização internacional, a menos que sejam cumpridos os requisitos previstos na presente diretiva relativos às transferências sujeitas a garantias adequadas e às derrogações aplicáveis a situações específicas. É conveniente prever procedimentos de consulta entre a Comissão e esses países terceiros ou organizações internacionais. A Comissão deverá, em tempo útil, informar o país terceiro ou a organização internacional das razões de tal proibição e iniciar consultas com o país ou organização em causa a fim de corrigir a situação.

(71) As transferências não baseadas numa decisão de adequação só deverão ser autorizadas caso sejam apresentadas garantias adequadas num instrumento juridicamente vinculativo que garanta a proteção dos dados pessoais ou o responsável pelo tratamento tenha avaliado todas as circunstâncias inerentes à transferência de dados e, com base nessa avaliação, considere que existem garantias adequadas no que diz respeito à proteção de dados pessoais. Tais instrumentos juridicamente vinculativos poderão ser, por exemplo, acordos bilaterais juridicamente vinculativos que os Estados-Membros tenham celebrado e integrado no seu ordenamento jurídico e que possam ser executados pelos titulares de dados desses Estados-Membros, assegurando a observância dos requisitos relativos à proteção de dados e dos direitos dos titulares dos dados, incluindo o direito de recurso administrativo ou judicial. Ao avaliar todas as circunstâncias relativas à transferência de dados, o responsável pelo tratamento poderá ter em conta os acordos de cooperação que tenham sido celebrados entre a Europol ou a Eurojust e países terceiros e que permitam o intercâmbio de dados pessoais. O responsável pelo tratamento poderá ainda ter em conta que a transferência de dados pessoais ficará sujeita a obrigações de confidencialidade e ao princípio da especificidade, assegurando que os dados não sejam tratados para efeitos que não sejam os da transferência. Além disso, o responsável pelo tratamento deverá ter em conta que os dados pessoais não serão utilizados para requerer, aplicar ou executar uma pena de morte ou qualquer forma de tratamento cruel ou desumano. Embora essas condições possam ser consideradas garantias adequadas para a transferência de dados, o responsável pelo tratamento pode exigir garantias adicionais.

(72) Na falta de decisão de adequação ou de garantias adequadas, só poderão ser efetuadas transferências ou categorias de transferências em situações específicas, se necessário para: proteger os interesses vitais do titular dos dados ou de um terceiro ou salvaguardar os interesses legítimos do titular dos dados, desde que o direito do Estado-Membro que efetua a transferência dos dados assim o preveja; prevenir uma ameaça iminente e grave para a segurança pública de um Estado-Membro ou de um país terceiro; em determinados casos, para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública; em determinados casos, para efeitos de declaração, exercício ou defesa de um direito num processo judicial. Essas derrogações deverão ser interpretadas de forma restritiva e não permitir transferências frequentes, maciças e estruturais de dados pessoais nem transferências maciças de dados, devendo ser limitadas aos dados estritamente necessários. Tais transferências deverão ser documentadas e disponibilizadas, a pedido, à autoridade de controlo para verificar a licitude da transferência.

(73) As autoridades competentes dos Estados-Membros aplicam os acordos internacionais bilaterais ou multilaterais vigentes celebrados com países terceiros no domínio da cooperação judiciária em matéria penal e da cooperação policial com vista ao intercâmbio de informações relevantes que lhes permitam exercer as atribuições previstas na lei. Em princípio, esse intercâmbio é efetuado em cooperação com as autoridades competentes dos países terceiros em causa ou, pelo menos, com a cooperação dessas autoridades, e por vezes até na falta de um acordo internacional bilateral ou multilateral. Todavia, em determinados casos específicos, os procedimentos normais que requerem contactar essa autoridade do país terceiro podem revelar-se ineficazes ou desadequados, nomeadamente devido à impossibilidade de a transferência ser efetuada em tempo útil ou devido ao facto de essa autoridade do país terceiro não respeitar o Estado de direito ou as regras e normas internacionais no domínio dos direitos humanos, de tal modo que as autoridades competentes dos Estados-Membros poderão decidir transferir os dados pessoais diretamente para os destinatários estabelecidos em países terceiros. Poderá ser o caso se houver necessidade urgente de transferir dados pessoais para salvar a vida de uma pessoa que corra o risco de ser vítima de uma infração penal ou prevenir a prática iminente de um crime, incluindo o terrorismo. Mesmo que essa transferência entre autoridades competentes e destinatários estabelecidos em países terceiros só deva ter lugar em determinados casos específicos, a presente diretiva deverá prever condições para regular tais casos. Essas disposições não deverão ser consideradas derrogações aos acordos internacionais bilaterais ou multilaterais vigentes no domínio da cooperação judiciária em matéria penal e da cooperação policial. Essas regras deverão complementar a aplicação das demais regras da presente diretiva, especialmente as que dizem respeito à licitude do tratamento e as que estabelece o Capítulo V.

(74) Quando os dados pessoais atravessam fronteiras há um risco acrescido de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se proteger da utilização ilícita ou da divulgação dessas informações. Paralelamente, as autoridades de controlo podem ser incapazes de dar seguimento a reclamações ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras. Os seus esforços para colaborar no contexto transfronteiriço podem ser também prejudicados pela falta poderes para tomar medidas preventivas ou de reparação, bem como pela incoerência e insuficiência dos regimes jurídicos aplicáveis Por conseguinte, revela-se necessário promover uma cooperação mais estreita entre as autoridades de controlo da proteção de dados a fim de que possam efetuar o intercâmbio de informações com as suas homólogas internacionais.

(75) A criação de autoridades de controlo nos Estados-Membros, com total independência no exercício das suas atribuições, constitui um elemento essencial da proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais. As autoridades de controlo deverão fiscalizar a aplicação das disposições adotadas por força da presente diretiva e deverão contribuir para a sua aplicação coerente em toda a União, a fim de proteger as pessoas singulares relativamente ao tratamento dos seus dados pessoais. Para esse efeito, as autoridades de controlo deverão cooperar entre si e com a Comissão.

(76) Os Estados Membros podem confiar a uma autoridade de controlo já criada nos termos do Regulamento (UE) 2016/…[*] o exercício das atribuições das autoridades nacionais de controlo criadas por força da presente diretiva.

[*] JO: inserir o número do regulamento que consta no st 5419/16.

(77) Os Estados-Membros deverão poder criar várias autoridades de controlo de modo a refletir a sua estrutura constitucional, organizativa e administrativa. Deverão ser dados às autoridades de controlo os meios financeiros e humanos, as instalações e as infraestruturas necessárias ao exercício eficaz das suas atribuições, incluindo as relacionadas com a assistência e a cooperação mútuas com outras autoridades de controlo da União. As autoridades de controlo deverão ter orçamentos anuais públicos separados, que poderão estar integrados no orçamento geral do estado ou do orçamento nacional.

(78) As autoridades de controlo deverão ficar sujeitas a procedimentos de controlo ou fiscalização independentes no que diz respeito às suas despesas financeiras, desde que tal não afete a sua independência.

(79) As condições gerais aplicáveis aos membros da autoridade de controlo deverão ser definidas pelo direito do Estado-Membro e deverão prever, em especial, que os referidos membros sejam nomeados por procedimento transparente pelo Parlamento, pelo Governo nacional ou pelo Chefe de Estado do Estado-Membro, com base numa proposta do governo ou de um dos seus membros ou do parlamento ou da sua câmara competente, ou por um organismo independente incumbido da nomeação nos termos do direito do Estado-Membro. A fim de assegurar a independência da autoridade de controlo, os membros que a integram deverão atuar com integridade, abster-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não deverão exercer nenhuma ocupação, seja ou não remunerada, que com elas seja incompatível. A fim de assegurar a independência da autoridade de controlo, o pessoal deverá ser selecionado pela autoridade de controlo, eventualmente com a intervenção de um organismo independente incumbido nos termos do direito do Estado-Membro.

(80) Embora a presente diretiva se aplique também às atividades dos tribunais nacionais e outras autoridades judiciais, a competência das autoridades de controlo não deverá abranger o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional , a fim de assegurar a independência dos juízes no desempenho das suas funções jurisdicionais. Esta exceção deverá ser estritamente limitada às atividades judiciais relativas a processos judiciais, não se aplicando a outras atividades a que os juízes possam estar associados por força do direito do Estado-Membro. Os Estados-Membros podem também prever a possibilidade de a competência das autoridades de controlo não abranger o tratamento de dados pessoais efetuado por outras autoridades judiciais independentes no exercício da sua função jurisdicional, nomeadamente o Ministério Público. Em todo o caso, o cumprimento das regras da presente diretiva pelos tribunais e outras autoridades judiciais independentes deverá ficar sempre sujeito a uma fiscalização independente nos termos do artigo 8.º, n.º 3, da Carta.

(81) Cada autoridade de controlo deverá tratar as reclamações apresentadas por qualquer titular de dados e investigar o assunto ou transmiti-lo à autoridade de controlo competente. A investigação decorrente de uma reclamação deverá ser realizada, sob reserva de controlo jurisdicional, na medida adequada ao caso específico. A autoridade de controlo deverá informar o titular dos dados da evolução e do resultado da reclamação num prazo razoável. Se o caso exigir maior investigação ou a coordenação com outra autoridade de controlo, deverão ser fornecidas informações intermédias ao titular dos dados.

(82) A fim de assegurar o controlo eficaz, fiável e coerente da conformidade com a presente diretiva e da sua aplicação em toda a União e nos termos do TFUE, conforme interpretado pelo Tribunal de Justiça, as autoridades de controlo deverão ter, em cada Estado-Membro, as mesmas atribuições e poderes, incluindo poderes de investigação e de correção, bem como funções consultivas, que constituem meios necessários no exercício das suas atribuições. Os seus poderes não deverão, contudo, interferir com as regras específicas aplicáveis ao processo penal, nomeadamente à investigação e repressão de infração penais, nem com a independência do poder judicial. Sem prejuízo dos poderes das autoridades responsáveis pela aplicação da lei nos termos do direito do Estado-Membro, as autoridades de controlo deverão ainda dispor do poder de levar as violações à presente diretiva ao conhecimento das autoridades judiciais e de intentar processos judiciais. Os poderes das autoridades de controlo deverão ser exercidos em conformidade com as garantias processuais adequadas previstas no direito da União e dos Estados-Membros, com imparcialidade e equidade e num prazo razoável. Em particular, cada medida deverá ser adequada, necessária e proporcionada a fim de garantir a conformidade com a presente diretiva, tendo em conta as circunstâncias de cada caso concreto, respeitar o direito de qualquer pessoa a ser ouvida antes de a seu respeito ser tomada qualquer medida individual que a afete desfavoravelmente e evitar custos supérfluos e inconvenientes excessivos para a pessoa em causa. Os poderes de investigação em matéria de acesso às instalações deverão ser exercidos em conformidade com os requisitos específicos do direito do Estado-Membro, como, por exemplo, a obrigação de obter autorização judicial prévia. A adoção de uma decisão juridicamente vinculativa deverá ficar sujeita a controlo jurisdicional no Estado-Membro da autoridade de controlo que tenha adotado a decisão.

(83) As autoridades de controlo deverão prestar-se mutuamente assistência no exercício das suas atribuições, por forma a assegurar a execução e aplicação coerentes das disposições adotadas por força da presente diretiva.

(84) O Comité deverá contribuir para a aplicação coerente da presente diretiva em toda a União, nomeadamente aconselhando a Comissão e promovendo a cooperação das autoridades de controlo em toda a União.

(85) Os titulares de dados deverão ter direito a apresentar reclamação a uma autoridade de controlo única e a intentar uma ação judicial, nos termos do artigo 47.º da Carta, se considerarem que os direitos que lhes são conferidos por disposições adotadas por força da presente diretiva foram violados ou a autoridade de controlo não responder à reclamação, a recusar ou rejeitar, total ou parcialmente, ou não tomar as iniciativas necessárias para proteger os seus direitos. A investigação decorrente de uma reclamação deverá ser realizada, sob reserva de controlo jurisdicional, na medida adequada ao caso específico. A autoridade de controlo competente deverá informar o titular dos dados da evolução e do resultado da reclamação num prazo razoável. Se o caso exigir maior investigação ou a coordenação com outra autoridade de controlo, deverão ser fornecidas informações intermédias ao titular dos dados. As autoridades de controlo deverão tomar medidas para facilitar a apresentação de reclamações, como, por exemplo, fornecer formulários para apresentação de reclamações que possam também ser preenchidos eletronicamente, sem excluir outros meios de comunicação.

(86) Todas as pessoas, singulares ou coletivas, deverão ter direito a intentar uma ação judicial perante os tribunais nacionais competentes contra as decisões das autoridades de controlo que produzam efeitos jurídicos que lhes digam respeito. Tais decisões prendem-se, em especial, com o exercício de poderes de investigação, correção e autorização pelas autoridades de controlo ou com a recusa ou rejeição de reclamações. Porém, este direito não abrange outras medidas das autoridades de controlo que não sejam juridicamente vinculativas, como os pareceres emitidos ou o aconselhamento prestado pela autoridade de controlo. As ações contra as autoridades de controlo deverão ser instauradas nos tribunais do Estado-Membro em cujo território a autoridade de controlo esteja estabelecida e deverão ser conduzidas nos termos do direito desse Estado-Membro. Estes tribunais deverão ter jurisdição plena, incluindo o poder de analisar todas as questões de facto e de direito relevantes para o litígio.

(87) Se considerar que os direitos que lhe são conferidos pela presente diretiva foram violados, o titular dos dados deverá ter o direito de mandatar um organismo que vise proteger os direitos e interesses dos titulares de dados no que respeita à proteção dos seus dados pessoais, e que seja constituído ao abrigo do direito de um Estado-Membro, para apresentar reclamação em seu nome a uma autoridade de controlo e exercer o direito de intentar ação judicial. O direito de representação dos titulares dos dados não deverá prejudicar o direito processual do Estado-Membro, que poderá exigir que estes se façam obrigatoriamente representar perante os tribunais nacionais por um advogado, tal como previsto na Diretiva 77/249/CEE do Conselho[1].

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

(88) Os danos sofridos por uma pessoa em virtude de um tratamento em violação da presente diretiva deverão ser ressarcidos pelo responsável pelo tratamento dos dados ou por qualquer outra autoridade competente nos termos do direito do Estado-Membro. O conceito de "dano" deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça de uma forma que reflita plenamente os objetivos da presente diretiva. Tal não prejudica os pedidos de indemnização por danos provocados pela violação de outras regras constantes do direito da União ou dos Estados-Membros. Quando se faça referência a tratamentos ilícitos ou a tratamentos que violem disposições adotadas por força da presente diretiva, ficam igualmente abrangidos os tratamentos que violem os atos de execução adotados nos termos da presente diretiva. Os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido.

(89) Deverão ser aplicadas sanções às pessoas singulares ou às pessoas coletivas, de direito privado ou público, que violem a presente diretiva. Os Estados-Membros deverão assegurar que as sanções sejam efetivas, proporcionadas e dissuasivas e tomar todas as medidas necessárias à sua aplicação.

(90) A fim de assegurar condições uniformes para a execução da presente diretiva, deverão ser conferidas competências de execução à Comissão no que diz respeito ao nível de proteção adequado garantido por um país terceiro, um território ou um setor específico desse país terceiro, ou por uma organização internacional, e o formato e os procedimentos de assistência mútua, bem como as regras de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho[1].

(91) Deverá ser utilizado o procedimento de exame para a adoção de atos de execução sobre o nível de proteção adequado garantido por um país terceiro, um território ou um setor específico desse país terceiro, ou por uma organização internacional, o formato e os procedimentos de assistência mútua, bem como as regras de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité, atendendo a que se trata de atos de alcance geral.

(92) A Comissão deverá adotar atos de execução imediatamente aplicáveis quando imperativos urgentes assim o exijam, em casos devidamente fundamentados relacionados com um país terceiro, um território ou um setor específico desse país terceiro ou uma organização internacional que tenha deixado de assegurar um nível de proteção adequado.

[1] 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).

(93) Atendendo a que os objetivos da presente diretiva, a saber, proteger os direitos e liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção de dados pessoais, e assegurar o livre intercâmbio desses dados pelas autoridades competentes na União, não podem ser suficientemente alcançados pelos Estados-Membros, mas podem, devido à dimensão e aos efeitos da ação, ser mais bem alcançados ao nível da União, a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do TUE. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, a presente diretiva não excede o necessário para atingir esses objetivos.

(94) Não deverão ser afetadas as disposições específicas dos atos, adotados pela União no domínio da cooperação judiciária em matéria penal e da cooperação policial antes da data de adoção da presente diretiva, que regulem o tratamento de dados pessoais entre Estados-Membros ou o acesso das autoridades designadas dos Estados-Membros aos sistemas de informação criados nos termos dos Tratados, como, por exemplo, as disposições específicas relativas à proteção dos dados pessoais aplicadas por força da Decisão 2008/615/JAI do Conselho[1] ou o artigo 23.º da Convenção relativa ao Auxílio Judiciário Mútuo em Matéria Penal entre os Estados-Membros da União Europeia[2]. Dado que o artigo 8.º da Carta e o artigo 16.º do TFUE exigem que o direito fundamental à proteção de dados pessoais seja garantido de forma coerente em toda a União, a Comissão deverá examinar a situação quanto à relação entre a presente diretiva e os atos adotados anteriormente à data de adoção da presente diretiva que regulem o tratamento de dados pessoais entre Estados-Membros ou o acesso de autoridades designadas dos Estados-Membros a sistemas de informação criados por força dos Tratados, a fim de avaliar a necessidade de adaptar essas disposições específicas à presente diretiva. Sempre que apropriado, a Comissão deverá apresentar propostas para assegurar regras jurídicas coerentes relacionadas com o tratamento de dados pessoais.

---

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

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

(95) A fim de assegurar uma proteção global e coerente dos dados pessoais na União, os acordos internacionais celebrados pelos Estados-Membros antes de a presente diretiva entrar em vigor que sejam conformes com o direito da União aplicável antes de a presente diretiva entrar em vigor deverão continuar a vigorar até serem alterados, substituídos ou revogados.

(96) Os Estados-Membros deverão dispor de um prazo, não superior a dois anos, a contar da data de entrada em vigor da presente diretiva para a transpor. Os tratamentos de dados que se encontrem já em curso à data de entrada em vigor da presente diretiva deverão passar a cumprir as disposições da presente diretiva no prazo de dois anos após a data da respetiva entrada em vigor. Todavia, caso tal tratamento cumpra o disposto no direito da União aplicável antes da entrada em vigor da presente diretiva, os requisitos por ela estabelecidos no que respeita à consulta prévia da autoridade de controlo não deverão ser aplicáveis às operações de tratamento já em curso antes da entrada em vigor da presente diretiva, uma vez que, pela sua natureza, tais requisitos deverão ser cumpridos antes do início do tratamento. Caso os Estados-Membros utilizem o período de transposição mais longo, que termina setes anos a contar da data de entrada em vigor da presente diretiva, para cumprir as obrigações de registo cronológico no que respeita a sistemas de tratamento automatizado criados antes da data de entrada em vigor da presente diretiva, o responsável pelo tratamento, ou o subcontratante, deverá dispor de métodos eficazes para demonstrar a licitude do tratamento dos dados, permitir o autocontrolo e garantir a integridade e a segurança dos dados, tais como registos cronológicos ou outros.

(97) A presente diretiva não prejudica as disposições relativas à luta contra o abuso sexual, a exploração sexual de crianças e a pornografia infantil, previstas na Diretiva 2011/93/UE do Parlamento Europeu e do Conselho[1].

(98) Por conseguinte, a Decisão-Quadro 2008/977/JAI deverá ser revogada.

(99) Nos termos do artigo 6.º-A do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao TUE e ao TFUE, o Reino Unido e a Irlanda não ficam vinculados pelas regras estabelecidas na presente diretiva que digam respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relativas à aplicação da Parte III, Título V, Capítulos 4 ou 5, do TFUE, caso não estejam vinculados por regras que regulem formas de cooperação judiciária em matéria penal ou de cooperação policial no âmbito das quais devam ser observadas as disposições definidas com base no artigo 16.º do TFUE.

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

(100) Nos termos dos artigos 2.º e 2.º-A do Protocolo n.º 22 relativo à posição da Dinamarca, anexo ao TUE e ao TFUE, a Dinamarca não fica vinculada nem sujeita à aplicação das regras da presente diretiva que digam respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relativas à aplicação da Parte III, Título V, Capítulos 4 ou 5, do TFUE. Uma vez que a presente diretiva constitui um desenvolvimento do acervo de Schengen, por força do disposto na Parte III, Título V, do TFUE, cabe à Dinamarca decidir, nos termos do artigo 4.º do referido Protocolo, no prazo de seis meses a contar da data de adoção da presente diretiva, se procederá à transposição da presente diretiva para o seu direito nacional.

(101) No que diz respeito à Islândia e à Noruega, a presente diretiva constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do Acordo celebrado pelo Conselho da União Europeia e a República da Islândia e o Reino da Noruega relativo à associação destes Estados à execução, à aplicação e ao desenvolvimento do acervo de Schengen[1].

(102) No que diz respeito à Suíça, a presente diretiva constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do Acordo entre a União Europeia, a Comunidade Europeia e a Confederação Suíça relativo à associação da Confederação Suíça à execução, à aplicação e ao desenvolvimento do acervo de Schengen[2].

[1] JO L 176 de 10.7.1999, p. 36.
[2] JO L 53 de 27.2.2008, p. 52.

(103) No que diz respeito ao Liechtenstein, a presente diretiva constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do Protocolo entre a União Europeia, a Comunidade Europeia, a Confederação Suíça e o Principado do Liechtenstein relativo à adesão do Principado do Liechtenstein ao Acordo entre a União Europeia, a Comunidade Europeia e a Confederação Suíça relativo à associação da Confederação Suíça à execução, à aplicação e ao desenvolvimento do acervo de Schengen[1].

(104) A presente diretiva respeita os direitos fundamentais e observa os princípios reconhecidos na Carta, consagrados pelo TFUE, nomeadamente o direito ao respeito da vida privada e familiar, o direito à proteção dos dados pessoais e o direito à ação e a um tribunal imparcial. As restrições introduzidas em relação a estes direitos são conformes com o artigo 52.º, n.º 1, da Carta, uma vez que são necessárias para cumprir os objetivos de interesse geral reconhecidos pela União ou para satisfazer a necessidade de proteger os direitos e as liberdades de outrem.

(105) De acordo com a declaração política conjunta dos Estados-Membros e da Comissão, de 28 de setembro de 2011, sobre os documentos explicativos, os Estados-Membros assumiram o compromisso de fazer acompanhar a notificação das suas medidas de transposição, nos casos em que tal se justifique, de um ou mais documentos que expliquem a relação entre as componentes de uma diretiva e as partes correspondentes das disposições nacionais de transposição. Em relação à presente diretiva, o legislador considera que a transmissão desses documentos se justifica.

[1] JO L 160 de 18.6.2011, p. 21.

(106) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001 e emitiu parecer em 7 de março de 2012[1].

(107) A presente diretiva não obsta a que os Estados-Membros possam aplicar disposições respeitantes ao exercício dos direitos dos titulares de dados em matéria de informação, de acesso e de retificação ou apagamento dos dados pessoais e de limitação do tratamento no âmbito de uma ação penal, bem como eventuais restrições desses direitos, na legislação processual penal nacional,

ADOTARAM A PRESENTE DIRETIVA:

[1] JO C 192 de 30.6.2012, p. 7.

CAPÍTULO I
DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto e objetivos

1. A presente diretiva estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública.

2. Nos termos da presente diretiva, os Estados-Membros asseguram:

   a) A proteção dos direitos e das liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção dos dados pessoais; e

   b) Que o intercâmbio de dados pessoais entre autoridades competentes na União, caso seja previsto pelo direito da União ou do Estado-Membro, não seja limitado nem proibido por razões relacionadas com a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

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

Artigo 2.º

Âmbito de aplicação

1. A presente diretiva aplica-se ao tratamento de dados pessoais pelas autoridades competentes para os efeitos estabelecidos no artigo 1.º, n.º 1.

2. A presente diretiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento de dados pessoais contidos num ficheiro ou a ele destinados por meios não automatizados.

3. A presente diretiva não se aplica ao tratamento de dados pessoais:

   a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;

   b) Efetuado pelas instituições, organismos, serviços e agências da União.

Artigo 3.º

Definições

Para efeitos da presente diretiva, entende-se por:

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

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

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

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

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

6) "Ficheiro", um conjunto estruturado de dados pessoais acessíveis segundo critérios específicos, centralizado, descentralizado ou repartido de modo funcional ou geográfico;

7) "Autoridade competente":

a) Uma autoridade pública competente para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; ou

b) Qualquer outro organismo ou entidade designados pelo direito de um Estado-Membro para exercer a autoridade pública e os poderes públicos para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;

8) "Responsável pelo tratamento", a autoridade competente que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento dos dados pessoais; caso as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou pelo direito de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;

9) "Subcontratante", uma pessoa singular ou coletiva, uma autoridade pública, uma agência ou outro organismo que tratam dados pessoais por conta do responsável pelo tratamento;

10) "Destinatário", uma pessoa singular ou coletiva, uma autoridade pública, uma agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito de um Estado-Membro não são consideradas como destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento;

11) "Violação de dados pessoais", uma violação da segurança que provoca, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação não autorizada de dados pessoais transmitidos, conservados ou tratados de outro modo, ou o acesso não autorizado a esses dados;

12) "Dados genéticos", dados pessoais, relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular, que dão informações únicas sobre a sua fisiologia ou sobre a sua saúde e que resultam, designadamente, da análise de uma amostra biológica da pessoa singular em causa;

13) "Dados biométricos", dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a sua identificação única, tais como imagens faciais ou dados dactiloscópicos;

14) "Dados relativos à saúde", dados pessoais relativos à saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelam informações sobre o seu estado de saúde;

15) "Autoridade de controlo", uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 41.º;

16) "Organização internacional", uma organização e os organismos de direito internacional público por ela tutelados, ou outro organismo criado por um acordo celebrado entre dois ou mais países ou com base num acordo dessa natureza.

CAPÍTULO II
PRINCÍPIOS

Artigo 4.º

Princípios relativos ao tratamento de dados pessoais

1. Os Estados-Membros preveem que os dados pessoais sejam:

a) Objeto de um tratamento lícito e leal;

b) Recolhidos para finalidades determinadas, explícitas e legítimas, e não tratados de uma forma incompatível com essas finalidades;

c) Adequados, pertinentes e limitados ao mínimo necessário relativamente às finalidades para as quais são tratados;

d) Exatos e atualizados sempre que necessário; devem ser tomadas todas as medidas razoáveis para que os dados inexatos, tendo em conta as finalidades para as quais são tratados, sejam apagados ou retificados sem demora;

e) Conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados;

f) Tratados de uma forma que garanta a sua segurança adequada, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidentais, recorrendo a medidas técnicas ou organizativas adequadas;

2. É permitido o tratamento pelo mesmo ou por outro responsável pelo tratamento para as finalidades previstas no artigo 1.º, n.º 1, diferentes da finalidade para a qual os dados pessoais foram recolhidos, desde que:

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

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

3. O tratamento pelo mesmo ou por outro responsável pelo tratamento pode incluir o arquivo de interesse público e a utilização científica, estatística ou histórica dos dados para as finalidades previstas no artigo 1.º, n.º 1, sob reserva de garantias adequadas dos direitos e liberdades do titular dos dados.

4. O responsável pelo tratamento é responsável pelo cumprimento do disposto nos n.ºs 1, 2 e 3 e deve poder comprovar esse cumprimento.

Artigo 5.º

Prazos para a conservação e avaliação

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

Artigo 6.º

Distinção entre diferentes categorias de titulares de dados

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

a) Pessoas relativamente às quais existem motivos fundados para crer que cometeram ou estão prestes a cometer uma infração penal;

b) Pessoas condenadas por uma infração penal;

c) Vítimas de uma infração penal ou pessoas relativamente às quais certos factos levam a crer que possam vir a ser vítimas de uma infração penal; e

d) Terceiros envolvidos numa infração penal, tais como pessoas que possam ser chamadas a testemunhar em investigações penais relacionadas com infrações penais ou em processos penais subsequentes, pessoas que possam fornecer informações sobre infrações penais, ou contactos ou associados de uma das pessoas a que se referem as alíneas a) e b).

Artigo 7.º

Distinção entre dados pessoais e verificação da qualidade dos dados pessoais

1. Os Estados-Membros preveem que os dados pessoais baseados em factos sejam, na medida do possível, distinguidos dos dados pessoais baseados em apreciações pessoais.

2. Os Estados-Membros preveem que as autoridades competentes tomem todas as medidas razoáveis para assegurar que os dados pessoais inexatos, incompletos ou desatualizados não possam ser transmitidos nem disponibilizados. Para o efeito, as autoridades competentes verificam, na medida do possível, a qualidade dos dados pessoais antes de estes serem transmitidos ou disponibilizados. Em todas as transmissões de dados pessoais devem ser fornecidas, na medida do possível, as informações necessárias para que a autoridade competente que as recebe possa apreciar até que ponto os dados são exatos, completos e fiáveis, e estão atualizados.

3. Se se verificar que foram transmitidos dados inexatos ou que foram transmitidos dados pessoais de forma ilícita, o destinatário deve ser informado sem demora. Neste caso, os dados pessoais são retificados ou apagados, ou o tratamento é limitado nos termos do artigo 16.º.

Artigo 8.º

Licitude do tratamento

1. Os Estados-Membros preveem que o tratamento só seja lícito se e na medida em que for necessário para o exercício de uma atribuição pela autoridade competente para os efeitos previstos no artigo 1.º, n.º 1, e tiver por base o direito da União ou de um Estado-Membro.

2. O direito de um Estado-Membro que rege o tratamento no âmbito da presente diretiva especifica pelo menos os objetivos do tratamento, os dados pessoais a tratar e as finalidades do tratamento.

Artigo 9.º

Condições específicas do tratamento

1. Os dados pessoais recolhidos pelas autoridades competentes para os fins do artigo 1.º, n.º 1, não podem ser tratados para fins diferentes dos previstos no artigo 1.º, n.º 1, a não ser que esse tratamento seja autorizado pelo direito da União ou de um Estado-Membro. Caso os dados pessoais sejam tratados para esses outros fins, é aplicável o Regulamento (UE) 2016/…[*], salvo se tratamento for efetuado no âmbito de uma atividade não sujeita à aplicação do direito da União.

2. Caso o direito dos Estados-Membros confie às autoridades competentes o exercício de atribuições diferentes das exercidas para os fins do artigo 1.º, n.º 1, o Regulamento (UE) 2016/…[*] é aplicável ao tratamento para esses fins, inclusive para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, salvo se o tratamento for efetuado no âmbito de uma atividade não sujeita à aplicação do direito da União.

3. Caso o direito da União ou dos Estados-Membros aplicável à autoridade transmissora competente preveja condições específicas para o tratamento, os Estados-Membros preveem que a autoridade transmissora competente informe o destinatário dos dados pessoais dessas condições e da obrigação de as cumprir.

4. Os Estados-Membros preveem que a autoridade transmissora competente não aplique condições ao abrigo do n.º 3 a destinatários situados noutros Estados-Membros nem a agências, organismos e órgãos criados nos termos do Título V, Capítulos 4 e 5, do TFUE, diferentes das aplicáveis a transmissões de dados similares no Estado-Membro da autoridade transmissora competente.

[*] JO: inserir o número do regulamento que consta no st 5419/16.

Artigo 10.º

Tratamento de categorias especiais de dados pessoais

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

a) For autorizado pelo direito da União ou de um Estado-Membro;

b) Se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou

c) Estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados.

Artigo 11.º

Decisões individuais automatizadas

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

2. As decisões a que se refere o n.º 1 do presente artigo não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 8.º, a não ser que sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

3. Em conformidade com o direito da União, são proibidas as definições de perfis que conduzam à discriminação de pessoas singulares com base nas categorias especiais de dados pessoais a que se refere o artigo 10.º.

CAPÍTULO III
DIREITOS DO TITULAR DOS DADOS

Artigo 12.º

Comunicação e regras de exercício dos direitos dos titulares dos dados

1. Os Estados-Membros preveem que o responsável pelo tratamento tome todas as medidas razoáveis para fornecer ao titular dos dados as informações a que se refere o artigo 13.º e para efetuar as comunicações relativas aos artigos 11.º, 14.º a 18.º e 31.º a respeito do tratamento de uma forma concisa, inteligível e de fácil acesso, utilizando uma linguagem clara e simples. As informações são fornecidas pelos meios adequados, inclusive eletrónicos. Em regra geral, o responsável pelo tratamento fornece as informações na mesma forma que o pedido.

2. Os Estados-Membros preveem que o responsável pelo tratamento facilite o exercício dos direitos do titular dos dados nos termos dos artigos 11.º e 14.º a 18.º.

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

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

   a) Exigir o pagamento de uma taxa razoável, tendo em conta os custos administrativos da prestação das informações ou da comunicação ou da tomada das medidas solicitadas; ou

   b) Recusar dar seguimento ao pedido.

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

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

Artigo 13.º

Informações a facultar ou a fornecer ao titular dos dados

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

   a) A identidade e os contactos do responsável pelo tratamento;

b) Os contactos do encarregado da proteção de dados, se for caso disso;

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

d) O direito de apresentar reclamação à autoridade de controlo e de obter os contactos dessa autoridade;

e) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que dizem respeito ao titular, bem como a sua retificação ou o seu apagamento e a limitação do tratamento.

2. Para além das informações a que se refere o n.º 1, os Estados-Membros preveem por lei que o responsável pelo tratamento forneça ao titular dos dados, em determinados casos, as seguintes informações adicionais, a fim de lhe permitir exercer os seus direitos:

a) O fundamento jurídico do tratamento;

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

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

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

3. Os Estados-Membros podem adotar medidas legislativas que prevejam o adiamento, a limitação ou a não prestação aos titulares dos dados das informações a que se refere o n.º 2 se e enquanto tais medidas constituírem medidas necessárias e proporcionadas numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de:

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

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

c) Proteger a segurança pública;

d) Proteger a segurança nacional;

e) Proteger os direitos e as liberdades de terceiros.

4. Os Estados-Membros podem adotar medidas legislativas a fim de determinar as categorias de tratamento suscetíveis de ser abrangidas, total ou parcialmente, pelo âmbito do n.º 3, alíneas a) a e).

Artigo 14.º

Direito de acesso do titular dos dados aos seus dados pessoais

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

a) As finalidades e o fundamento jurídico do tratamento;

b) As categorias dos dados pessoais em causa;

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

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

e) A existência do direito de solicitar ao responsável pelo tratamento a retificação ou o apagamento dos dados pessoais ou a limitação do tratamento dos dados pessoais que dizem respeito ao titular dos dados;

f) O direito de apresentar reclamação à autoridade de controlo e de obter os contactos dessa autoridade;

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

Artigo 15.º

Limitações do direito de acesso

1. Os Estados-Membros podem adotar medidas legislativas para limitar, total ou parcialmente, o direito de acesso do titular dos dados, se e enquanto tal limitação, total ou parcial, constituir uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de:

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

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

c) Proteger a segurança pública;

d) Proteger a segurança nacional;

e) Proteger os direitos e as liberdades de terceiros.

2. Os Estados-Membros podem adotar medidas legislativas a fim de determinar as categorias de tratamento suscetíveis de ser abrangidas, total ou parcialmente, pelo âmbito do n.º 1, alíneas a) a e).

3. Nos casos a que se referem os n.ºs 1 e 2, os Estados-Membros preveem que o responsável pelo tratamento informe por escrito o titular dos dados, sem demora injustificada, de todos os casos de recusa ou limitação de acesso, e dos motivos da recusa ou da limitação. Essa informação pode ser omitida caso a sua prestação possa prejudicar uma das finalidades enunciadas no n.º 1. Os Estados-Membros preveem que o responsável pelo tratamento informe o titular dos dados do direito que lhe assiste de apresentar reclamação à autoridade de controlo ou de intentar uma ação judicial.

4. Os Estados-Membros preveem que o responsável pelo tratamento detalhe os motivos de facto ou de direito em que a sua decisão se baseou. Essa informação deve ser facultada às autoridades de controlo.

Artigo 16.º

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

1. Os Estados-Membros preveem que o titular dos dados tenha o direito de obter sem demora injustificada do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta a finalidade do tratamento, os Estados-Membros preveem que o titular dos dados tenha direito a que os seus dados pessoais incompletos sejam completados, inclusive por meio de declaração adicional.

2. Os Estados-Membros exigem que o responsável pelo tratamento apague os dados pessoais sem demora injustificada e preveem que o titular dos dados tenha o direito de obter sem demora injustificada do responsável pelo tratamento o apagamento dos dados pessoais que lhe digam respeito caso o tratamento infrinja as disposições adotadas nos termos dos artigos 4.º, 8.º ou 10.º, ou caso os dados pessoais tenham de ser apagados a fim de cumprir uma obrigação legal a que o responsável pelo tratamento esteja sujeito.

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

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

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

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

4. Os Estados-Membros preveem que o responsável pelo tratamento informe o titular dos dados, por escrito, de todos os casos de recusa da retificação ou do apagamento de dados pessoais ou da limitação do tratamento, e dos motivos da recusa. Os Estados-Membros podem adotar medidas legislativas que limitem, total ou parcialmente, a obrigação de fornecer essas informações, na medida em que tal limitação constitua uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de:

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

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

c) Proteger a segurança pública;

d) Proteger a segurança nacional;

e) Proteger os direitos e as liberdades de terceiros.

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

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

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

Artigo 17.º

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

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

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

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

Artigo 18.º

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

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

CAPÍTULO IV
RESPONSÁVEL PELO TRATAMENTO E SUBCONTRATANTE

SECÇÃO 1
OBRIGAÇÕES GERAIS

Artigo 19.º

Obrigações do responsável pelo tratamento

1. Os Estados-Membros preveem que o responsável pelo tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares, aplique as medidas técnicas e organizativas adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com a presente diretiva. Estas medidas são avaliadas e atualizadas, se necessário.

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

Artigo 20.º

Proteção de dados desde a conceção e por defeito

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

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

Artigo 21.º

Responsáveis conjuntos pelo tratamento

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

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

Artigo 22.º

Subcontratante

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

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

3. Os Estados-Membros preveem que o tratamento em subcontratação seja regulada por um contrato ou outro ato normativo sujeito ao direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento e que estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias de titulares de dados, as obrigações e os direitos do responsável pelo tratamento. Esse contrato ou outro ato normativo prevê, designadamente, que o subcontratante:

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

b) Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou se encontram sujeitas às obrigações legais de confidencialidade adequada;

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

d) Apaga todos os dados pessoais ou devolve-os ao responsável pelo tratamento, consoante a escolha deste, depois de concluir os serviços de tratamento de dados, e apaga as cópias existentes, a menos que a sua conservação seja exigida pelo direito da União ou do Estado-Membro;

e) Disponibiliza ao responsável pelo tratamento dos dados todas as informações necessárias para demonstrar o cumprimento do presente artigo;

f) Respeita as condições referidas nos n.ºs 2 e 3 na contratação de outro subcontratante.

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

5. Se, em violação da presente diretiva, um subcontratante determinar as finalidades e os meios do tratamento, esse mesmo subcontratante é considerado responsável pelo tratamento em relação ao referido tratamento.

Artigo 23.º

Tratamento sob a autoridade do responsável pelo tratamento ou do subcontratante

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

Artigo 24.º

Registos das atividades de tratamento

1. Os Estados-Membros preveem que os responsáveis pelo tratamento conservem um registo de todas as categorias de atividades de tratamento sob a sua responsabilidade. Desse registo deve constar :

   a) O nome e contactos do responsável pelo tratamento de dados e, se for caso disso, do responsável conjunto pelo tratamento de dados e do encarregado da proteção de dados;

   b) As finalidades do tratamento;

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

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

   e) Se for caso disso, a utilização da definição de perfis;

   f) Se for caso disso, as categorias de transferências de dados pessoais para um país terceiro ou uma organização internacional;

   g) Uma indicação da fundamento jurídico da operação de tratamento, incluindo transferências, a que os dados pessoais se destinam;

h) Se possível, os prazos fixados para o apagamento das diferentes categorias de dados pessoais;

i) Se possível, uma descrição geral das medidas técnicas e organizativas em matéria de segurança referidas no artigo 29.º, n.º 1.

2. Os Estados-Membros preveem que os subcontratantes conservem um registo de todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento, do qual constem:

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

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

c) Se for caso disso, as transferências de dados pessoais para um país terceiro ou uma organização internacional se o responsável pelo tratamento der instruções explícitas nesse sentido, incluindo a identificação desse país terceiro ou dessa organização internacional;

d) Se possível, uma descrição geral das medidas técnicas e organizativas em matéria de segurança referidas no artigo 29.º, n.º 1.

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

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

Artigo 25.º

Registo cronológico

1. Os Estados-Membros preveem que sejam conservados em sistemas de tratamento automatizado registos cronológicos pelo menos das seguintes operações de tratamento: recolha, alteração, consulta, divulgação – incluindo transferências –, interconexão e apagamento. Os registos cronológicos das operações de consulta e divulgação permitem determinar o motivo, a data e a hora dessas operações e, na medida do possível, a identificação da pessoa que consultou ou divulgou dados pessoais, e a identidade dos destinatários desses dados pessoais.

2. Os registos cronológicos são utilizados exclusivamente para efeitos de verificação da licitude do tratamento, autocontrolo e garantia da integridade e segurança dos dados pessoais, bem como para ações penais.

3. O responsável pelo tratamento e o subcontratante disponibilizam os registos cronológicos à autoridade de controlo, a pedido desta.

Artigo 26.º

Cooperação com a autoridade de controlo

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

Artigo 27.º

Avaliação de impacto sobre a proteção de dados

1. Caso um tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, seja suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares, os Estados-Membros preveem que o responsável efetue, antes de iniciar o tratamento, uma avaliação do impacto que as operações de tratamento previstas terão sobre a proteção dos dados pessoais.

2. A avaliação a que se refere o n.º1 inclui, pelo menos, uma descrição geral das operações de tratamento de dados previstas, uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados, as medidas previstas para fazer face a esses riscos, as garantias, medidas de segurança e mecanismos para assegurar a proteção dos dados pessoais e demonstrar a conformidade com a presente diretiva, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

Artigo 28.º

Consulta prévia à autoridade de controlo

1. Os Estados-Membros preveem que o responsável pelo tratamento ou o subcontratante consulte a autoridade de controlo antes de proceder ao tratamento de dados pessoais que farão parte de um novo ficheiro a criar caso:

   a) A avaliação de impacto sobre a proteção de dados prevista no artigo 27.º indique que o tratamento resultaria num elevado risco na ausência das medidas a tomar pelo responsável pelo tratamento para atenuar o risco; ou

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

2. Os Estados-Membros preveem que a autoridade de controlo seja consultada durante a elaboração de propostas de medidas legislativas a adotar por um parlamento nacional ou de medidas regulamentares baseadas nessas medidas legislativas, quando tais propostas estejam relacionadas com o tratamento.

3. Os Estados-Membros preveem que a autoridade de controlo possa estabelecer uma lista das operações de tratamento de dados sujeitas a consulta prévia nos termos do n.º 1.

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

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

SECÇÃO 2
SEGURANÇA DOS DADOS PESSOAIS

Artigo 29.º

Segurança do tratamento

1. Os Estados-Membros preveem que o responsável pelo tratamento e o subcontratante, , tendo em conta as técnicas mais avançadas, os custos da sua aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos de probabilidade e gravidade variáveis que este tratamento representa para os direitos e liberdades das pessoas singulares, apliquem medidas técnicas e organizativas adequadas a fim de assegurar um nível de segurança adequado ao risco, em especial no que respeita ao tratamento das categorias especiais de dados pessoais a que se refere o artigo 10.º.

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

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

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

   c) Impedir a introdução não autorizada de dados pessoais, bem como qualquer inspeção, alteração ou apagamento não autorizados de dados pessoais conservados (controlo da conservação);

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

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

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

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

h) Impedir que, durante as transferências de dados pessoais ou o transporte de suportes de dados, os dados pessoais possam ser lidos, copiados, alterados ou suprimidos sem autorização (controlo do transporte);

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

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

Artigo 30.º

Notificação de uma violação de dados pessoais à autoridade de controlo

1. Os Estados-Membros preveem que, em caso de violação de dados pessoais, o responsável pelo tratamento notifique desse facto a autoridade de controlo sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.

2. O subcontratante notifica o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais.

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

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

   b) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas informações adicionais;

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

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

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

5. Os Estados-Membros preveem que o responsável pelo tratamento documente qualquer violação de dados pessoais referida no n.º 1, compreendendo os factos relacionados com a violação de dados pessoais, os seus efeitos e as medidas de reparação adotadas. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo.

6. Os Estados-Membros preveem que, caso a violação de dados pessoais envolva dados pessoais que tenham sido transmitidos pelo ou ao responsável pelo tratamento de outro Estado-Membro, as informações referidas no n.º 3 sejam comunicadas sem demora injustificada ao responsável pelo tratamento deste último Estado-Membro.

Artigo 31.º

Comunicação de uma violação de dados pessoais ao titular dos dados

1. Os Estados-Membros preveem que, quando a violação dos dados pessoais for suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunique a violação de dados pessoais ao titular dos dados sem demora injustificada.

2. A comunicação ao titular dos dados referida no n.º 1 do presente artigo descreve numa linguagem clara e simples a natureza da violação dos dados pessoais e inclui, pelo menos, as informações e recomendações previstas no artigo 30.º, n.º 3, alíneas b), c) e d).

3. A comunicação ao titular dos dados referida no n.º 1 não é exigida se:

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

b) O responsável pelo tratamento de dados tiver tomado medidas subsequentes capazes de assegurar que a ocorrência de elevado risco para os direitos e liberdades dos titulares referida no n.º 1 deixou de ser provável; ou

c) Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.

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

5. A comunicação ao titular dos dados referida no n.º 1 do presente artigo pode ser adiada, limitada ou omitida sob reserva das condições e pelos motivos enunciados no artigo 13.º, n.º 3.

SECÇÃO 3
ENCARREGADO DA PROTEÇÃO DE DADOS

Artigo 32.º

Designação do encarregado da proteção de dados

1. Os Estados-Membros preveem que o responsável pelo tratamento designe um encarregado da proteção de dados. Os Estados-Membros podem isentar dessa obrigação os tribunais e outras autoridades judiciais independentes no exercício da sua função jurisdicional.

2. O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio da legislação e práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 34.º.

3. Pode ser designado um único encarregado da proteção de dados para várias autoridades competentes, tendo em conta a sua dimensão e estrutura organizativa.

4. Os Estados-Membros preveem que o responsável pelo tratamento dos dados publique os contactos do encarregado da proteção de dados e os comunique à autoridade de controlo.

Artigo 33.º

Cargo de encarregado da proteção de dados

1. Os Estados-Membros preveem que o responsável pelo tratamento assegure que o encarregado da proteção de dados seja envolvido, de forma adequada e em tempo útil, em todas as questões relacionadas com a proteção de dados pessoais.

2. O responsável pelo tratamento dos dados apoia o encarregado da proteção de dados no desempenho das funções a que se refere o artigo 34.º, fornecendo-lhe os recursos necessários para o efeito e para a manutenção dos seus conhecimentos, e dando-lhe acesso aos dados pessoais e às operações de tratamento.

Artigo 34.º

Funções do encarregado da proteção de dados

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

a) Informar e aconselhar o responsável pelo tratamento dos dados e os empregados que efetuem o tratamento quanto às obrigações que lhes incumbem por força da presente diretiva e a outras disposições da União ou dos Estados-Membros de proteção de dados;

b) Fiscalizar a conformidade com a presente diretiva, com outras disposições da União ou dos Estados-Membros de proteção de dados e com as políticas do responsável pelo tratamento de dados em matéria de proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados e as auditorias correspondentes;

c) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controlar a sua realização nos termos do artigo 27.º;

d) Cooperar com a autoridade de controlo;

e) Ponto de contacto para a autoridade de controlo em assuntos relacionados com o tratamento, incluindo a consulta prévia referida no artigo 28.º, e aconselhar esta autoridade, se for caso disso, sobre qualquer outro assunto.

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

Artigo 35.º

Princípios gerais das transferências de dados pessoais

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

   a) A transferência se necessária para a consecução das finalidades estabelecidas no artigo 1.º, n.º 1;

   b) Os dados pessoais serem transferidos para um responsável pelo tratamento no país terceiro ou na organização internacional que seja uma autoridade competente para as finalidades referidas no artigo 1.º, n.º 1;

   c) Caso os dados pessoais sejam transmitidos ou disponibilizados por outro Estado-Membro, esse Estado ter dado o seu consentimento prévio à transferência nos termos do seu direito nacional;

d) A Comissão ter adotado uma decisão de adequação nos termos do artigo 36.º ou, na falta dessa decisão de adequação , terem sido apresentadas ou existirem garantias adequadas nos termos do artigo 37.º, ou, na falta de decisão de adequação nos termos do artigo 36.º ou de garantias adequadas nos termos do artigo 37.º, se forem aplicáveis derrogações a situações específicas nos termos do artigo 38.º; e

e) No caso de uma transferência ulterior para um país terceiro ou uma organização internacional, a autoridade competente que realizou a transferência inicial, ou outra autoridade competente do mesmo Estado-Membro, autorizar a transferência ulterior após ter em conta todos os fatores pertinentes, incluindo a gravidade da infração penal, a finalidade para que os dados pessoais foram transferidos inicialmente e o nível de proteção dos dados pessoais no país terceiro ou na organização internacional para os quais os dados pessoais são ulteriormente transferidos.

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

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

Artigo 36.º

Transferências com base numa decisão de adequação

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

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

   a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação desta legislação, das regras de proteção de dados, das regras profissionais e das medidas de segurança relativas à proteção de dados, incluindo as regras para transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e meios efetivos de recurso administrativo e judicial para os titulares dos dados cujos dados pessoais sejam objeto de transferência;

b) A existência e o funcionamento efetivo de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e fazer cumprir as regras de proteção de dados e dotadas de poderes sancionatórios adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e por cooperar com as autoridades de controlo dos Estados-Membros; e

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

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

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

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

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

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

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

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

Artigo 37.º

Transferências sujeitas a garantias adequadas

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

   a) Tiverem sido apresentadas garantias adequadas no que diz respeito à proteção de dados pessoais mediante um instrumento juridicamente vinculativo; ou

   b) O responsável pelo tratamento de dados tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas r no que diz respeito à proteção desses dados.

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

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

Artigo 38.º

Derrogações aplicáveis a situações específicas

1. Na falta de uma decisão de adequação nos termos do artigo 36.º ou de garantias adequadas nos termos do artigo 37.º, os Estados-Membros preveem que só se possa efetuar uma transferência ou uma categoria de transferências de dados pessoais para um país terceiro ou uma organização internacional se a transferência for necessária:

   a) Para proteger os interesses vitais do titular dos dados ou de outra pessoa;

   b) Para salvaguardar os legítimos interesses do titular dos dados caso a legislação do Estado-Membro que transfere os dados pessoais o preveja;

   c) Para prevenir uma ameaça imediata e grave contra a segurança pública de um Estado-Membro ou de um país terceiro;

   d) Em determinados casos, para a consecução das finalidades estabelecidas no artigo 1.º, n.º 1; ou

   e) Num dado caso, para declarar, exercer ou defender num processo judicial um direito relacionado com as finalidades estabelecidas no artigo 1.º, n.º 1.

2. Os dados pessoais não são transferidos se a autoridade competente que procede à transferência determinar que, aquando da transferência referida no n.º 1, alíneas d) e e), os direitos e liberdades fundamentais do titular dos dados em causa primam sobre o interesse público.

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

Artigo 39.º

Transferência de dados pessoais para destinatários estabelecidos em países terceiros

1. Em derrogação do artigo 35.º, n.º 1, alínea b), e sem prejuízo de qualquer acordo internacional referido no n.º 2 do presente artigo, o direito da União ou dos Estados-Membros pode prever a possibilidade de, em determinados casos específicos, as autoridades competentes referidas no artigo 3.º, ponto 7), alínea a), transferirem dados pessoais diretamente para destinatários estabelecidos em países terceiros unicamente no caso de serem cumpridas as demais disposições da presente diretiva e preenchidas todas as seguintes condições:

   a) A transferência é estritamente necessária a uma função desempenhada pela autoridade competente que efetua a transferência e prevista pelo direito da União ou dos Estados-Membros tendo em vista a consecução das finalidades estabelecidas no artigo 1.º, n.º 1;

   b) A autoridade competente que efetua a transferência determina que nenhum direito ou liberdade fundamental do titular dos dados em causa prevalece sobre o interesse público que exige a transferência no caso em apreço;

   c) A autoridade competente que efetua a transferência considera que a transferência para uma autoridade que é competente para os efeitos referidos no artigo 1.º, n.º 1, no país terceiro se revela ineficaz ou desadequada, nomeadamente por não ser possível efetuá-la em tempo útil;

   d) A autoridade que é competente para os efeitos referidos no artigo 1.º, n.º 1, no país terceiro é informada sem demora injustificada, a menos que tal se revele ineficaz ou inadequado; e

e) A autoridade competente que efetua a transferência informa o destinatário da finalidade ou finalidades específicas para as quais o destinatário apenas pode tratar os dados pessoais, desde que o tratamento seja necessário.

2. Por "acordo internacional" a que se refere o n.º 1 entende-se um acordo internacional bilateral ou multilateral em vigor entre os Estados-Membros e países terceiros no domínio da cooperação judiciária em matéria penal e da cooperação policial.

3. A autoridade competente que efetua a transferência informa a autoridade de controlo sobre as transferências abrangidas pelo presente artigo.

4. As transferências efetuadas nos termos do n.º 1 devem ser documentadas.

Artigo 40.º

Cooperação internacional no domínio da proteção de dados pessoais

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

a) Estabelecer procedimentos internacionais de cooperação destinados a facilitar a aplicação efetiva da legislação em matéria de proteção de dados pessoais;

b) Prestar assistência mútua a nível internacional no domínio da aplicação da legislação de proteção de dados pessoais, nomeadamente através da notificação, transmissão das reclamações, assistência na investigação e intercâmbio de informações, sob reserva das garantias adequadas para a proteção dos dados pessoais e outros direitos e liberdades fundamentais;

c) Associar as partes interessadas aos debates e atividades que visem promover a cooperação internacional no âmbito da aplicação da legislação relativa à proteção de dados pessoais;

d) Promover o intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, inclusive sobre conflitos jurisdicionais com países terceiros.

CAPÍTULO VI
AUTORIDADES DE CONTROLO INDEPENDENTES

SECÇÃO 1
ESTATUTO INDEPENDENTE

Artigo 41.º

Autoridade de controlo

1. Cada Estado-Membro prevê que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação da presente diretiva, a fim de proteger os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União.

2. Cada autoridade de controlo contribui para a aplicação coerente da presente diretiva em toda a União. Para esse efeito, cooperam entre si e com a Comissão nos termos do Capítulo VII.

3. Os Estados-Membros podem prever que uma autoridade de controlo criada pelo Regulamento (UE) 2016/…* seja a autoridade de controlo a que se refere a presente diretiva e assuma as funções de autoridade de controlo a definir nos termos do n.º 1 do presente artigo.

4. Se for criada mais do que uma autoridade de controlo num Estado-Membro, o Estado-Membro em questão designa a autoridade de controlo que as representa as demais no Comité a que se refere o artigo 51.º.

Artigo 42.º

Independência

1. Os Estados-Membros preveem que cada autoridade de controlo aja com total independência no exercício das suas atribuições e dos poderes que lhe forem atribuídos nos termos da presente diretiva.

2. Os Estados-Membros preveem que os membros das autoridades de controlo, no desempenho das suas funções e no exercício dos poderes nos termos da presente diretiva, não estejam sujeitos a influências externas, diretas ou indiretas, e não solicitem nem recebam instruções de outrem.

3. Os membros das autoridades de controlo dos Estados-Membros abstêm-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não podem desempenhar qualquer atividade profissional incompatível, remunerada ou não.

* JO: inserir o número do regulamento que consta no st 5419/16.

4. Os Estados-Membros asseguram que as suas autoridades de controlo disponham dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários ao exercício eficaz das suas atribuições e dos seus poderes, designadamente no contexto da assistência mútua, da cooperação e da participação no Comité.

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

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

Artigo 43.º

Condições gerais aplicáveis aos membros da autoridade de controlo

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

   – pelo Parlamento,

   – pelo Governo,

   – pelo Chefe de Estado, ou

   – por um organismo independente incumbido da nomeação nos termos do direito do Estado-Membro.

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

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

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

Artigo 44.º

Regras aplicáveis à criação da autoridade de controlo

1. Cada Estado-Membro estabelece por lei:

   a) A criação da respetiva autoridade de controlo;

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

   c) As regras e procedimentos aplicáveis à nomeação dos membros da respetiva autoridade de controlo;

d) A duração do mandato dos membros da respetiva autoridade de controlo, que não será inferior a quatro anos, salvo no caso do primeiro mandato após … [*inserir data da entrada em vigor da presente diretiva]*, que pode ser mais curta caso seja necessário preservar a independência da autoridade de controlo através de um procedimento de nomeações escalonadas;

e) Se for caso disso, o número máximo, de mandatos dos membros da respetiva autoridade de controlo;

f) As condições que regem as obrigações dos membros e do pessoal da respetiva autoridade de controlo, a proibição das ações, funções e benefícios que com elas são incompatíveis durante o mandato e após o seu termo e as normas que regem a cessação da relação de trabalho.

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

SECÇÃO 2
COMPETÊNCIA, ATRIBUIÇÕES E PODERES

Artigo 45.º

Competência

1. Os Estados-Membros preveem que a respetiva autoridade de controlo seja competente para, no respetivo território, exercer as atribuições e os poderes que lhe são conferidos pela presente diretiva.

2. Os Estados-Membros preveem que a respetiva autoridade de controlo não seja responsável pela supervisão de operações de tratamento efetuadas pelos tribunais no exercício da sua função jurisdicional. Os Estados-Membros podem estabelecer que a respetiva autoridade de controlo não tenha competência para supervisionar operações de tratamento efetuadas por outras autoridades judiciais independentes no exercício da sua função jurisdicional

Artigo 46.º

Atribuições

1. Os Estados-Membros preveem que, no território respetivo, cada autoridade de controlo:

   a) Fiscalize e faça aplicar a presente diretiva e as suas medidas de execução;

   b) Promova a sensibilização e a compreensão do público relativamente aos riscos, regras, garantias e direitos associados ao tratamento;

c) Aconselhe, nos termos do direito do Estado-Membro, o Parlamento nacional, o Governo e outras instituições e organismos quanto às medidas legislativas e administrativas relacionadas com a proteção dos direitos e liberdades das pessoas singulares em matéria de tratamento;

d) Promova a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as obrigações que lhes incumbem nos termos da presente diretiva;

e) Se tal lhe for solicitado, preste informações a qualquer titular de dados sobre o exercício dos seus direitos nos termos da presente diretiva e, se adequado, coopere para esse efeito com as autoridades de controlo de outros Estados-Membros;

f) Trate de reclamações apresentadas pelos titulares de dados ou por um organismo, organização ou associação, nos termos do artigo 55.º, e investigue, na medida do necessário, o conteúdo da reclamação, informando o autor da reclamação do andamento e do resultado da investigação num prazo razoável, especialmente se forem necessárias operações de investigação ou de coordenação complementares com outra autoridade de controlo;

g) Verifique a licitude do tratamento nos termos do artigo 17.º e, num prazo razoável, informe o respetivo titular do resultado da verificação, conforme previsto no artigo 17.º, n.º 2, ou dos motivos que impediram a sua realização;

h) Coopere, nomeadamente partilhando informações, e preste assistência mútua a outras autoridades de controlo, tendo em vista assegurar a coerência da aplicação e da execução da presente diretiva;

i) Conduza investigações sobre a aplicação da presente diretiva, nomeadamente com base em informações recebidas de outra autoridade de controlo ou outra autoridade pública;

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

k) Preste aconselhamento sobre as operações de tratamento referidas no artigo 28.º;

l) Contribua para as atividades do Comité.

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

3. O exercício das atribuições de cada autoridade de controlo é gratuito para o titular dos dados e para o encarregado da proteção de dados.

4. Caso os pedidos sejam manifestamente infundados ou excessivos, particularmente devido ao seu caráter recorrente, a autoridade de controlo pode exigir o pagamento de uma taxa razoável, com base nos custos administrativos, ou indeferi-los. Cabe à autoridade de controlo demonstrar o caráter manifestamente infundado ou excessivo do pedido.

Artigo 47.º

Poderes

1. Cada Estado-Membro prevê, por lei, que a sua autoridade de controlo detenha poderes de investigação efetivos. Esses poderes incluem, pelo menos, o poder de obter do responsável pelo tratamento de dados e do subcontratante autorização de acesso a todos os dados pessoais objeto de tratamento e a todas as informações necessárias ao exercício das suas atribuições.

2. Cada Estado-Membro prevê, por lei, que a sua autoridade de controlo tenha poderes de correção efetivos, como, por exemplo:

   a) Advertir o responsável pelo tratamento de dados ou o subcontratante de que as operações de tratamento previstas são suscetíveis de violar as disposições adotadas por força da presente diretiva;

   b) Ordenar ao responsável pelo tratamento de dados ou ao subcontratante que, na medida do necessário, proceda por forma a que as operações de tratamento cumpram as disposições adotadas por força da presente diretiva, de determinada forma e num prazo determinado; em especial, ordenar a retificação ou apagamento dos dados pessoais ou a limitação tratamento nos termos do artigo 16.º;

   c) Impor uma limitação temporária ou definitiva, inclusive uma proibição, ao tratamento.

3. Cada Estado-Membro prevê, por lei, que a sua autoridade de controlo tenha poderes consultivos efetivos para aconselhar o responsável pelo tratamento de dados pelo procedimento de consulta prévia previsto no artigo 28.º e emitir, por iniciativa própria ou a pedido, pareceres dirigidos ao seu Parlamento nacional, ao seu Governo ou, nos termos do direito do Estado-Membro, a outras instituições e organismos, bem como ao público, sobre qualquer questão relacionada com a proteção de dados pessoais.

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

5. Cada Estado-Membro prevê, por lei, que a sua autoridade de controlo tenha o poder de apresentar as violações das disposições adotadas por força da presente diretiva ao conhecimento das autoridades judiciais e, se adequado, de intentar ou de outro modo intervir em processos judiciais, a fim de fazer aplicar as disposições adotadas por força da presente diretiva.

Artigo 48.º

Comunicação das violações

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

Artigo 49.º

Relatório de atividades

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

CAPÍTULO VII
COOPERAÇÃO

Artigo 50.º

Assistência mútua

1. Os Estados-Membros preveem que as suas autoridades de controlo prestem entre si informações relevantes e assistência mútua a fim de executar e aplicar a presente diretiva de forma coerente, e ponham em prática medidas para cooperar eficazmente entre si. A assistência mútua abrange, em especial, os pedidos de informação e as medidas de controlo, como os pedidos de consulta, inspeção e investigação.

2. Os Estados-Membros preveem que cada autoridade de controlo tome todas as medidas adequadas para responder aos pedidos de outra autoridade de controlo sem demora injustificada e, o mais tardar, um mês após a receção do pedido. Essas medidas podem incluir, particularmente, a transmissão de informações úteis sobre a condução de uma investigação.

3. Os pedidos de assistência inclui todas as informações necessárias, nomeadamente a finalidade e os motivos do pedido. As informações trocadas só são utilizadas para a finalidade para que tenham sido solicitadas.

4. A autoridade de controlo requerida não pode indeferir um pedido, salvo se:

   a) Não for competente em razão do objeto do pedido ou das medidas cuja execução lhe é solicitada; ou

   b) O deferimento do pedido viole a presente diretiva ou o direito da União ou do Estado-Membro ao qual a autoridade de controlo que recebe o pedido esteja sujeita.

5. A autoridade de controlo requerida informa a autoridade de controlo requerente dos resultados obtidos ou, consoante o caso, do andamento do pedido ou das medidas tomadas para lhe dar resposta. A autoridade de controlo requerida deve fundamentar a decisão de indeferir o pedido nos termos do n.º 4.

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

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

8. A Comissão pode especificar, por atos de execução, o formato e os procedimentos de assistência mútua referidos no presente artigo, bem como as regras de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 58.º, n.º 2.

Artigo 51.º

Atribuições do Comité

1. O Comité criado pelo Regulamento (UE) 2016/…*, exerce as seguintes atribuições no que diz respeito ao tratamento no âmbito de aplicação da presente diretiva:

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

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

c) Elaborar diretrizes dirigidas às autoridades de controlo em matéria de aplicação das medidas referidas no artigo 47.º, n.ºs 1 e 3;

* JO: inserir o número do regulamento que consta no st 5419/16.

d) Emitir diretrizes, recomendações e boas práticas em conformidade com a alínea b) do presente número, aplicáveis à determinação das violações de dados pessoais e da demora injustificada referidas no artigo 30.º, n.ºs 1 e 2, e às circunstâncias particulares em que um responsável pelo tratamento ou um subcontratante é obrigado a notificar a violação de dados pessoais;

e) Emitir diretrizes, recomendações e boas práticas em conformidade com a alínea b) do presente número, tendo como objeto as circunstâncias em que uma violação de dados pessoais é suscetível de resultar num risco elevado para os direitos e liberdades das pessoas singulares a que se refere o artigo 31.º, n.º 1;

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

g) Dar parecer à Comissão tendo em vista avaliar a adequação do nível de proteção num país terceiro ou organização internacional e também avaliar se um país terceiro, o território ou a organização internacional ou o setor específico deixou de garantir um nível de proteção adequado;

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

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

j) Promover o intercâmbio de conhecimentos e documentação sobre direito e práticas de proteção de dados com autoridades de controlo de todo o mundo.

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

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

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

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

CAPÍTULO VIII
VIAS DE RECURSO, RESPONSABILIDADE E SANÇÕES

Artigo 52.º

Direito de apresentar reclamação a uma autoridade de controlo

1. Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, os Estados-Membros preveem que todos os titulares de dados têm o direito de apresentar reclamação a uma autoridade de controlo única, se o titular dos dados considerar que o tratamento dos dados pessoais que lhe diz respeito viola as disposições adotadas por força da presente diretiva.

2. Os Estados-Membros preveem que, se a reclamação não for apresentada à autoridade de controlo competente nos termos do artigo 45.º, n.º 1, a autoridade de controlo a que é apresentada a transmita, sem demora injustificada, à autoridade de controlo competente. O titular dos dados é informado dessa transmissão.

3. Os Estados-Membros preveem que a autoridade de controlo à qual a reclamação é apresentada preste assistência complementar a pedido do titular dos dados.

4. O titular dos dados é informado pela autoridade de controlo competente do andamento e do resultado da reclamação apresentada, nomeadamente da possibilidade de intentar ação judicial nos termos do artigo 53.º.

Artigo 53.º

Direito de intentar ação judicial contra uma autoridade de controlo

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

2. Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, todos os titulares de dados têm o direito de intentar ação judicial se a autoridade de controlo competente nos termos do artigo 45.º, n.º 1, não atender à reclamação ou não informar o titular dos dados, no prazo de três meses, do andamento ou do resultado da reclamação apresentada nos termos do artigo 52.º.

3. Os Estados-Membros preveem que os recursos contra uma autoridade de controlo sejam interpostos nos tribunais do Estado-Membro em cujo território essa autoridade se encontre estabelecida.

Artigo 54.º

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

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

Artigo 55.º

Representação dos titulares dos dados

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

Artigo 56.º

Direito de indemnização

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

Artigo 57.º

Sanções

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

CAPÍTULO IX
ATOS DE EXECUÇÃO

Artigo 58.º

Procedimento de comité

1. A Comissão é assistida pelo comité criado pelo artigo 93.º do Regulamento (UE) 2016/…[*]. Esse comité é um comité na aceção do Regulamento (UE) n.º 182/2011.

2. Caso se remeta para o presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

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

[*] JO: inserir o número do regulamento que consta no st 5419/16.

CAPÍTULO X
DISPOSIÇÕES FINAIS

Artigo 59.º

Revogação da Decisão-Quadro 2008/977/JAI

1. A Decisão-Quadro 2008/977/JAI é revogada com efeitos a partir de … [*dois anos a contar da data de entrada em vigor da presente diretiva*].

2. As remissões para a decisão revogada a que se refere o n.º 1 entendem-se como sendo feitas para a presente diretiva.

Artigo 60.º

Atos jurídicos da União em vigor

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

Artigo 61.º

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

Os acordos internacionais que impliquem a transferência de dados pessoais para países terceiros ou organizações internacionais, que foram celebrados pelos Estados-Membros antes de … [*data de entrada em vigor da presente diretiva*],e que, nos termos do direito da União, são aplicáveis antes de … [*data de entrada em vigor da presente diretiva*]*,* continuam a vigorar até serem alterados, substituídos ou revogados.

Artigo 62.º

Relatórios da Comissão

1. Até … [*seis anos após a entrada em vigor da presente diretiva*] e posteriormente de quatro em quatro anos, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e a revisão da presente diretiva. Os relatórios devem ser públicos.

2. No âmbito das avaliações e revisões a que se refere o n.º 1, a Comissão examina, em particular, a aplicação e o funcionamento do Capítulo VII sobre a transferência de dados pessoais para países terceiros ou organizações internacionais, em especial no que diz respeito às decisões adotadas nos termos do artigo 36.º, n.º 3, e do artigo 39.º.

3. Para os efeitos dos n.ºs 1 e 2, a Comissão pode solicitar informações aos Estados-Membros e às autoridades de controlo.

4. Ao proceder às avaliações e revisões a que se referem os n.ºs 1 e 2, a Comissão tem em consideração as posições e conclusões a que tenham chegado o Parlamento Europeu, o Conselho e outros organismos e fontes pertinentes.

5. Se necessário, a Comissão apresenta propostas adequadas com vista à alteração da presente diretiva atendendo, em especial, à evolução das tecnologias da informação e aos progressos da sociedade da informação e à harmonização de outros instrumentos jurídicos.

6. Até … [*três anos após a entrada em vigor da presente diretiva*], a Comissão reexamina outros atos jurídicos adotados pela União que regulam o tratamento pelas autoridades competentes para efeitos do artigo 1.º, n.º 1, designadamente os referidos no artigo 60.º, a fim de avaliar a necessidade de os harmonizar com a presente diretiva e apresenta, se for caso disso, as propostas necessárias à alteração desses atos de forma a assegurar uma abordagem coerente da proteção de dados pessoais no âmbito da presente diretiva.

Artigo 63.º

Transposição

1. Os Estados-Membros adotam e publicam, até … [*data/dois anos após a data de entrada em vigor da presente diretiva*], as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva. Comunicam imediatamente à Comissão o texto dessas disposições. Os Estados-Membros aplicam as referidas disposições a partir de … [*data/dois anos após a data de entrada em vigor da presente diretiva*].

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

2. Em derrogação do n.º 1, um Estado-Membro pode estabelecer que, excecionalmente, quando o esforço envolvido for desproporcionado, os sistemas de tratamento automatizado estabelecidos antes de ... [*data de entrada em vigor da presente diretiva*] seja tornado conforme com o artigo 25.º, n.º 1, até … [*7 anos a contar da data de entrada em vigor da presente diretiva*].

3. Em derrogação dos n.ºs 1 e 2 do presente artigo, um Estado-Membro pode, em circunstâncias excecionais, tornar um sistema de tratamento automatizado, referido no n.º 2 do presente artigo, conforme com o artigo 25.º, n.º 1, num prazo fixado após o período a que se refere o n.º 2 do presente artigo, caso, de outra forma, sejam causadas graves dificuldades ao funcionamento desse sistema de tratamento automatizado. O Estado-Membro em causa notifica a Comissão dos motivos para essas graves dificuldades e dos motivos para o prazo especificado em que tornará esse particular sistema de tratamento automatizado conforme com o artigo 25.º, n.º 1. O prazo fixado não pode, em caso algum, ir além de … [*10 anos após a data de entrada em vigor da presente diretiva*].

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

Artigo 64.º

Entrada em vigor

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

Artigo 65.º

Destinatários

Os destinatários da presente diretiva são os Estados-Membros.

Feito em …, em

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