COMISSÃO EUROPEIA

Bruxelas, 25.1.2012
COM(2012) 10 final

2012/0010 (COD)

Proposta de

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 e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados

[…]

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

A presente exposição de motivos apresenta mais em pormenor o novo quadro jurídico proposto para a proteção dos dados pessoais na União Europeia como consta da Comunicação COM (2012) 9 final. Este novo quadro jurídico consiste em duas propostas legislativas:

– uma proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral de proteção de dados), e

– uma proposta de 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 e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados.

A presente exposição de motivos diz respeito à segunda proposta legislativa.

O instrumento principal da atual legislação da UE em matéria de proteção de dados pessoais, a Diretiva 95/46/CE[1], foi adotada em 1995 com dois objetivos em vista: proteger o direito fundamental à proteção de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros. Foi completada por vários instrumentos contendo regras específicas de proteção dos dados pessoais no âmbito da cooperação policial e judiciária em matéria penal[2] (antigo terceiro pilar), nomeadamente a Decisão-Quadro 2008/977/JAI[3].

O Conselho Europeu convidou a Comissão a avaliar o funcionamento dos instrumentos da UE relativos à proteção de dados e a apresentar, se necessário, iniciativas adicionais, legislativas e não legislativas[4]. Na sua resolução sobre o Programa de Estocolmo, o Parlamento Europeu[5] acolheu favoravelmente a proposta de um regime global de proteção de dados na União e, designadamente, solicitou a revisão da decisão-quadro. No seu Plano de Ação de aplicação do Programa de Estocolmo[6], a Comissão insistiu sobre a necessidade de assegurar uma aplicação coerente do direito fundamental à proteção de dados pessoais no contexto de todas as políticas da União. O Plano de Ação sublinhou que «*numa sociedade globalizada, caracterizada por uma evolução tecnológica rápida em que o intercâmbio de informações não conhece fronteiras, é particularmente importante respeitar a esfera privada dos cidadãos. A União deve assegurar que o direito fundamental à proteção de dados é aplicado de forma sistemática. É necessário reforçar a posição da UE em matéria de proteção dos dados*

---

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 Ver a lista completa no Anexo 3 da avaliação de impacto [SEC(2012) 72].

3 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 (a seguir designada «decisão-quadro»).

4 «O Programa de Estocolmo - Uma Europa aberta e segura que sirva e proteja os cidadãos», JO C 115 de 4.5.2010, p. 1.

5 Ver a Resolução do Parlamento Europeu, de 25 de novembro de 2009, relativa à Comunicação da Comissão ao Parlamento Europeu e ao Conselho – Um espaço de liberdade, segurança e justiça ao serviço dos cidadãos – Programa de Estocolmo (P7_TA (2009)0090).

6 COM(2010) 171 final.

pessoais no contexto de todas as políticas da União Europeia, incluindo nos domínios da aplicação da lei e da prevenção da criminalidade, bem como nas nossas relações internacionais».

Na sua Comunicação intitulada «Uma abordagem global da proteção de dados pessoais na União Europeia»[7], a Comissão concluiu que a UE carece de uma política mais ampla e coerente relativa ao direito fundamental à proteção dos dados pessoais.

A Decisão-Quadro 2008/977/JAI tem um âmbito de aplicação limitado, uma vez que apenas se aplica ao tratamento transfronteiriço de dados, excluindo as atividades de tratamento realizadas pelas autoridades policiais e judiciárias a nível meramente nacional. Este fator é suscetível de criar dificuldades às autoridades policiais e a outras autoridades competentes no domínio da cooperação judiciária em matéria penal e da cooperação policial. Estas autoridades nem sempre conseguem distinguir facilmente o tratamento meramente nacional do tratamento transfronteiriço, nem prever se determinados dados pessoais poderão vir a ser objeto de um intercâmbio transfronteiriço numa fase ulterior (ver ponto 2 infra). Além disso, por força da sua natureza e conteúdo, a decisão-quadro deixa uma ampla margem de manobra aos Estados-Membros na transposição das suas disposições para o direito nacional. Por outro lado, a decisão-quadro não prevê qualquer mecanismo ou grupo consultivo análogo ao Grupo de Trabalho do artigo 29.º, que dê apoio a uma interpretação comum das suas disposições, nem qualquer competência de execução a favor da Comissão para assegurar uma abordagem comum na sua execução.

O artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE), estabelece o princípio de que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Além disso, com o artigo 16.º, n.° 2, do TFUE, o Tratado de Lisboa introduziu uma base jurídica específica para a adoção de regras em matéria de proteção de dados pessoais, que se aplica igualmente à cooperação judiciária em matéria penal e à cooperação policial. O artigo 8.º da Carta dos Direitos Fundamentais da UE consagra a proteção de dados pessoais como um direito fundamental. O artigo 16.º do TFUE exige que o legislador estabeleça regras relativas à proteção das pessoas singulares no que respeita ao tratamento de dados pessoais também nos domínios da cooperação judiciária em matéria penal e da cooperação policial, abrangendo o tratamento de dados pessoais quer a nível transfronteiriço quer a nível nacional. Isto permitirá proteger os direitos e as liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção de dados pessoais, garantindo simultaneamente o intercâmbio de dados pessoais para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, o que contribuirá para facilitar a cooperação a nível da luta contra a criminalidade na Europa.

Devido à natureza específica do domínio da cooperação policial e judiciária em matéria penal, foi reconhecido na Declaração 21[8], anexada ao TFUE, que poderão ser necessárias disposições específicas sobre a proteção de dados pessoais e sobre a livre circulação desses dados, nos domínios da cooperação judiciária em matéria penal e da cooperação policial, com base no artigo 16.º do TFUE.

---

7 Comissão Europeia, Comunicação sobre «Uma abordagem global da proteção de dados pessoais na União Europeia», COM(2010) 609 final de 4 de novembro de 2010.

8 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, de 13.12.2007).

2. RESULTADOS DAS CONSULTAS DAS PARTES INTERESSADAS E DA AVALIAÇÃO DE IMPACTO

A presente iniciativa é o resultado de consultas exaustivas a todas as principais partes interessadas sobre a oportunidade de rever o quadro jurídico atual da proteção de dados pessoais, que incluiu duas fases de consulta pública:

– De 9 de julho a 31 de dezembro de 2009, a «*consulta sobre o quadro jurídico aplicável ao direito fundamental à proteção dos dados pessoais*». A Comissão recebeu 168 respostas, 127 das quais de pessoas singulares, de organizações e de associações, e 12 de autoridades públicas. Os contributos não confidenciais podem ser consultados no sítio *web* da Comissão[9].

– De 4 de novembro de 2010 a 15 de janeiro de 2011, a «consulta sobre a abordagem global da Comissão em matéria de proteção de dados pessoais na União Europeia». A Comissão recebeu 305 respostas, 54 das quais provenientes de cidadãos, 31 de autoridades públicas e 220 de organizações privadas, nomeadamente associações empresariais e organizações não governamentais. Os contributos não confidenciais poderão ser consultados no sítio *web* da Comissão[10].

Uma vez que essas consultas incidiram essencialmente sobre a revisão da Diretiva 95/46/CE, foram organizadas consultas dirigidas especialmente aos responsáveis pela aplicação lei; em particular, foi realizada uma sessão de trabalho em 29 de junho de 2010, com as autoridades dos Estados-Membros sobre a aplicação das regras de proteção de dados pessoais às entidades públicas, incluindo no domínio da cooperação policial e judiciária em matéria penal. Além disso, em 2 de fevereiro de 2011, a Comissão reuniu autoridades dos Estados-Membros numa sessão de trabalho com vista a debater a execução da Decisão-Quadro 2008/977/JAI e, mais em geral, questões de proteção de dados no domínio da cooperação policial e judiciária em matéria penal.

Os cidadãos da União foram consultados através de um inquérito do Eurobarómetro realizado entre novembro e dezembro de 2010[11]. Foi igualmente lançado um conjunto de estudos[12]. O Grupo de Trabalho do artigo 29.º[13] emitiu vários pareceres e contributos úteis dirigidos à Comissão[14]. A Autoridade Europeia para a Proteção de Dados emitiu também um parecer

---

9 http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

10 http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm.

11 Eurobarómetro Especial (EB) 359, *Data Protection and Electronic Identity in the EU* (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf..

12 Ver o estudo sobre os benefícios económicos das tecnologias de proteção da privacidade ou o estudo comparativo sobre as abordagens diferentes relativamente a novos desafios em matéria de privacidade, em espacial à luz dos desenvolvimentos tecnológicos, janeiro de 2010. (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf).

13 O Grupo de Trabalho do artigo 29.º foi criado em 1996 (por força do artigo 29.º da Diretiva). Tem natureza consultiva e é composto por representantes das autoridades nacionais de controlo em matéria de proteção de dados, da Autoridade Europeia para a Proteção de Dados (AEPD) e da Comissão. Para mais informações sobre as suas atividades, consultar http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

14 Consultar, em especial, os seguintes pareceres: relativo ao «Futuro da Privacidade» (2009, WP 168); relativo aos conceitos de «responsável pelo tratamento» e «subcontratante» (1/2010, WP 169); relativo a publicidade comportamental em linha (2/2010, WP 171); relativo ao princípio da responsabilidade (3/2010, WP 173); relativo à legislação aplicável (8/2010, WP 179); e relativo ao consentimento (15/2011, WP 187). A pedido da Comissão, adotou também os três documentos seguintes sobre,

exaustivo relativo às questões suscitadas na Comunicação da Comissão de novembro de 2010[15].

O Parlamento Europeu aprovou, através da sua resolução de 6 de julho de 2011, um relatório que apoiava a abordagem da Comissão quanto à reforma do quadro legislativo de proteção de dados[16]. O Conselho da União Europeia adotou, em 24 de fevereiro de 2011, conclusões que apoiam em grande medida a intenção da Comissão de reformar o quadro da proteção de dados e aprova muitos dos elementos da sua abordagem. O Comité Económico e Social Europeu declarou-se igualmente favorável a uma revisão adequada da Diretiva 95/46/CE[17], apoiando o objetivo geral da Comissão no sentido de assegurar uma aplicação mais coerente das regras europeias de proteção de dados em todos os Estados-Membros.

Em consonância com a sua política «Legislar melhor», a Comissão realizou uma avaliação de impacto das diferentes opções estratégicas[18]. A avaliação de impacto baseou-se nos três objetivos de melhorar a dimensão «mercado interno» da proteção de dados, tornar o exercício do direito à proteção de dados pelas pessoas singulares mais eficaz e criar um quadro global e coerente que abranja todos os domínios de competência da União, incluindo a cooperação policial e judiciária em matéria penal. No que diz respeito ao último objetivo em especial, foram examinadas duas opções: a primeira opção consistia em alargar simplesmente o alcance das regras de proteção de dados a esse domínio e colmatar as lacunas e outras questões suscitadas pela decisão-quadro, enquanto a segunda opção, mais completa, consistia em adotar regras muito normativas e estritas que implicariam, aliás, a alteração imediata de todos os instrumentos abrangidos pelo «antigo terceiro pilar». Uma terceira opção, «minimalista», baseada em grande medida em comunicações interpretativas e medidas de apoio, tais como programas de financiamento e ferramentas técnicas, com uma intervenção legislativa mínima, não foi considerada adequada para resolver os problemas registados neste domínio em relação à proteção de dados.

Em conformidade com a metodologia estabelecida pela Comissão, cada opção foi avaliada, com a ajuda de um grupo diretor interserviços, quanto à sua eficácia para atingir os objetivos fixados, ao impacto económico sobre as partes interessadas (incluindo sobre o orçamento das instituições da UE), bem como ao impacto e efeitos sobre os direitos fundamentais. Não foi avaliado o impacto ambiental.

Essa análise do impacto global permitiu desenvolver a opção preferida que é parte integrante da presente proposta. Segundo a avaliação de impacto, a aplicação dessa opção deve permitir reforçar a proteção dos dados neste domínio, nomeadamente através da inclusão do tratamento de dados nacional, bem como aumentar a segurança jurídica para as autoridades competentes nos domínios da cooperação judiciária em matéria penal e da cooperação policial.

---

notificações, dados sensíveis e execução prática do artigo 28.º, n.º 6, da Diretiva 95/46/CE. Estes documentos podem ser consultados em: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm.

15 Disponível no sítio web da AEPD: http://www.edps.europa.eu/EDPSWEB/.

16 Resolução do PE, de 6 de julho de 2011, relativa a uma abordagem global sobre a proteção dos dados pessoais na União Europeia (2011/2025(INI), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&language=EN&ring=A7-2011-0244 (relator: DPE Axel Voss (PPE/DE).

17 CESE 999/2011.

18 SEC(2012) 72.

O comité das avaliações de impacto emitiu um parecer relativo ao projeto de avaliação de impacto em 9 de setembro de 2011, na sequência do qual foram introduzidas as seguintes alterações:

– foram clarificados os objetivos do quadro jurídico atual (em que medida foram ou não atingidos), bem como os objetivos da reforma prevista;

– foram acrescentados elementos factuais e explicações/esclarecimentos adicionais na secção sobre a definição dos problemas.

A Comissão preparou também um relatório sobre a execução da Decisão-Quadro 2008/977/JAI, com base no artigo 29.º, n.º 2, que deve ser adotado no quadro do presente pacote de medidas sobre a proteção de dados[19]. As conclusões desse relatório, que tiveram por base os contributos dos Estados-Membros, foram igualmente integradas na preparação da avaliação de impacto.

3. ELEMENTOS JURÍDICOS DA PROPOSTA

3.1. Base jurídica

A presente proposta baseia-se no artigo 16.º, .° 2, do TFUE, que constitui a nova base jurídica específica, introduzida pelo Tratado de Lisboa, para a adoção de regras em matéria de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União, bem como pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do direito da União, e de regras relativas à livre circulação desses dados.

A proposta visa assegurar um nível coerente e elevado de proteção de dados neste domínio, favorecendo deste modo a confiança mútua entre as autoridades policiais e judiciárias dos diferentes Estados-Membros e facilitando a livre circulação dos dados e a cooperação entre as referidas autoridades.

3.2. Subsidiariedade e proporcionalidade

Segundo o princípio da subsidiariedade (artigo 5.º, n.º 3, do TUE), devem ser adotadas medidas a nível da União apenas se e na medida em que os objetivos previstos não possam ser suficientemente alcançados pelos Estados-Membros, podendo, contudo, ser mais bem alcançados a nível da União devido à dimensão ou aos efeitos da ação proposta. Atendendo aos problemas acima mencionados, a análise da subsidiariedade indica a necessidade de uma ação a nível da UE nos domínios policial e da justiça penal pelas seguintes razões:

– o direito à proteção de dados pessoais, consagrado no artigo 8.º da Carta dos Direitos Fundamentais, e no artigo 16.°, n.° 1, do TFUE, exige o mesmo nível de proteção dos dados no conjunto da União. Requer o mesmo nível de proteção para os dados trocados e tratados a nível nacional;

– torna-se cada vez mais necessário que as autoridades de aplicação da lei nos Estados-Membros possam tratar e trocar os dados mais rapidamente, a fim de prevenir e

[19] COM(2012) 12.

lutar contra a criminalidade transnacional e o terrorismo. Neste contexto, regras claras e coerentes em matéria de proteção de dados a nível da UE contribuirão para desenvolver a cooperação entre as referidas autoridades;

– além disso, existem desafios práticos que se colocam à correta aplicação da legislação sobre a proteção de dados e a necessidade de cooperação entre os Estados-Membros e as suas autoridades competentes, que deve ser organizada a nível da UE de forma a assegurar a uniformidade de aplicação do direito da União. Em certas situações, a UE está também melhor posicionada para assegurar, de forma eficaz e coerente, o mesmo nível de proteção às pessoas singulares quando os seus dados pessoais são transferidos para países terceiros;

– os Estados-Membros não podem, por si só, reduzir os problemas na situação atual, particularmente os que se devem à fragmentação das legislações nacionais. Assim, existe uma necessidade especial de criação de um quadro harmonizado e coerente que permita uma transferência fácil dos dados pessoais para além das fronteiras nacionais a nível da UE, assegurando simultaneamente a proteção efetiva de todas as pessoas singulares no conjunto da União;

– as ações legislativas propostas a nível da UE têm melhores probabilidades de serem eficazes do que ações similares dos Estados-Membros devido à natureza e à dimensão dos problemas, que não se restringem a um ou vários Estados-Membros.

O princípio da proporcionalidade exige que qualquer intervenção seja específica e não exceda o necessário para alcançar os objetivos definidos. Este princípio orientou a preparação da presente proposta legislativa, desde a identificação e a avaliação das diferentes opções até à sua redação.

Uma diretiva é, portanto, o instrumento mais adequado para assegurar uma harmonização a nível da UE neste domínio, deixando aos Estados-Membros a flexibilidade necessária na execução dessas regras e princípios, bem como das suas derrogações a nível nacional. Tendo em conta a complexidade das regras nacionais atuais relativas à proteção de dados pessoais tratados no domínio da cooperação policial e da cooperação judiciária em matéria penal, bem como do objetivo de harmonização global dessas regras por via de uma diretiva, a Comissão solicitará aos Estados-Membros que lhe forneçam os documentos explicativos sobre a relação entre os elementos da diretiva e as partes correspondentes dos instrumentos nacionais de transposição, a fim de poder cumprir a missão de que está investida de acompanhamento da transposição da presente diretiva.

3.3. Resumo dos aspetos relativos aos direitos fundamentais

O direito à proteção dos dados pessoais está consagrado no artigo 8.º da Carta dos Direitos Fundamentais da UE e no artigo 16.º do TFUE, bem como no artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH). Conforme sublinhado pelo Tribunal de Justiça da UE[20], o direito à proteção dos dados pessoais não é absoluto, mas deve ser considerado em relação à sua função na sociedade[21]. A proteção de dados está profundamente relacionada

[20] Tribunal de Justiça da UE, acórdão de 9.11.2010 nos processos apensos C-92/09 e C-93/09, Volker e Markus Schecke, Coletânia 2010, p. I-0000.

[21] Nos termos do artigo 52.º, n.º 1, da Carta, podem ser impostas restrições ao exercício do direito à proteção de dados, desde que as restrições sejam estipuladas por lei, respeitem a essência do direito e das liberdades e, sem prejuízo do princípio da proporcionalidade, sejam necessárias e cumpram

com o respeito pela vida privada e familiar, protegido pelo artigo 7.º da Carta. Tal encontra-se refletido no artigo 1.º, n.º 1, da Diretiva 95/46/CE, que prevê que os Estados-Membros devem assegurar os direitos e liberdades fundamentais das pessoas singulares e, em especial, o direito à privacidade no que diz respeito ao tratamento de dados pessoais.

Os outros direitos fundamentais consagrados na Carta suscetíveis de serem afetados são, entre outros, a proibição de discriminação em razão da raça, origem étnica, características genéticas, religião ou convicções, opiniões políticas ou outras, deficiência ou orientação sexual (artigo 21.º), os direitos da criança (artigo 24.º) e o direito à ação e a um tribunal imparcial (artigo 47.º).

3.4. Explicação pormenorizada da proposta

3.4.1. CAPÍTULO I – DISPOSIÇÕES GERAIS

O artigo 1.º define o objeto da diretiva, ou seja, o estabelecimento de regras relativas ao tratamento de dados pessoais para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e enuncia os dois objetivos da diretiva, ou seja, proteger os direitos e as liberdades fundamentais das pessoas singulares e, em especial, os seus direitos à proteção dos dados pessoais, assegurando simultaneamente um elevado nível de segurança pública, bem como assegurar o intercâmbio de dados pessoais entre as autoridades competentes a nível da União.

O artigo 2.º define o âmbito de aplicação da diretiva, que não está limitado ao tratamento de dados transfronteiriço, mas que se aplica ao conjunto das atividades de tratamento efetuadas pelas «autoridades competentes» (definidas no artigo 3.º, n.º 14) para efeitos da diretiva. A diretiva não se aplica ao tratamento no contexto de uma atividade não abrangida pelo âmbito de aplicação do direito da União, nem ao tratamento de dados pelas instituições, órgãos, organismos, e agências da União Europeia, abrangido pelo Regulamento (CE) n.° 45/2001 e outra legislação específica.

O artigo 3.º define os termos utilizados na diretiva. Embora algumas definições tenham sido transpostas da Diretiva 95/46/CE e da Decisão-Quadro 2008/977/JAI, outras foram alteradas ou completadas por elementos suplementares, ou são novas. As novas definições são a «violação de dados pessoais», «dados genéticos» e «dados biométricos», «autoridades competentes» [esta última definição tem por base o artigo 87.º do TFUE e o artigo 2.º, alínea h), da Decisão-Quadro 2008/977/JAI] e «criança», definição baseada na Convenção das Nações Unidas sobre os Direitos da Criança[22].

3.4.2. CAPÍTULO II – PRINCÍPIOS

O artigo 4.º enuncia os princípios que regulam o tratamento de dados pessoais, refletindo o artigo 6.º da Diretiva 95/46/CE e o artigo 3.º da Decisão-Quadro 2008/977/JAI, adaptando estes princípios ao contexto particular da presente diretiva.

---

genuinamente objetivos de interesse geral reconhecidos pela União Europeia ou a necessidade de assegurar os direitos e liberdades de terceiros.

[22] A que se refere também o artigo 2.º, alínea a), da Diretiva 2011/92/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.

O artigo 5.º exige que os Estados-Membros estabeleçam na medida do possível, uma distinção entre dados pessoais de diferentes categorias de titulares de dados. Trata-se de uma disposição nova, que não consta da Diretiva 95/46/CE nem da Decisão-Quadro 2008/977/JAI, mas que a Comissão tinha inserido na sua proposta inicial de decisão-quadro[23]. Inspira-se na Recomendação n.° R (87)15 do Conselho da Europa. Já existem regras semelhantes para a Europol[24] e a Eurojust[25].

O artigo 6.º, relativo aos diferentes níveis de exatidão e de fiabilidade dos dados pessoais, reflete o princípio 3.2 da Recomendação n.º R (87)15 do Conselho da Europa. Existem regras semelhantes para a Europol[26], igualmente incluídas na proposta da Comissão da decisão-quadro.

O artigo 7.º enuncia os motivos que fundamentam o tratamento lícito quando necessário para a execução de uma missão por uma autoridade competente ao abrigo do direito nacional, para o respeito de uma obrigação legal à qual esteja sujeito o responsável pelo tratamento, para assegurar os interesses vitais do titular de dados ou de um terceiro, ou para evitar uma ameaça grave e imediata para a segurança pública. Os outros motivos que fundamentam o tratamento lícito, referidos no artigo 7.º da Diretiva 95/46/CE, não são pertinentes para efeitos do tratamento de dados em matéria policial e penal.

O artigo 8.º estabelece a proibição geral de tratamento de categorias especiais de dados pessoais e as exceções a esta regra geral, com base no artigo 8.º da Diretiva 95/46/CE, acrescentando os dados genéticos, em conformidade com a jurisprudência do Tribunal de Europeu dos Direitos do Homem (TEDH)[27].

O artigo 9.º estabelece uma proibição de medidas exclusivamente baseadas no tratamento automatizado de dados pessoais, salvo se estiver autorizado por lei que preveja as garantias adequadas, na aceção do artigo 7.º da Decisão-Quadro 2008/977/JAI.

3.4.3. CAPÍTULO III - DIREITOS DO TITULAR DOS DADOS

O artigo 10.º introduz a obrigação de os Estados-Membros assegurarem informações de fácil acesso e compreensão, que se inspira especialmente no princípio 10 da Resolução de Madrid sobre as regras internacionais em matéria de proteção de dados pessoais e da vida privada[28], e imporem aos responsáveis pelo tratamento de dados que prevejam procedimentos e mecanismos que facilitem o exercício dos direitos pelos titulares de dados. Tal inclui a obrigação de prever o exercício, em princípio gratuito, desses direitos.

O artigo 11.º enuncia a obrigação que incumbe aos Estados-Membros de assegurar a informação do titular de dados. Estas obrigações têm por base os artigos 10.º e 11.º da Diretiva 95/46/CE, sem artigos separados que especifiquem se as informações são ou não recolhidas junto do titular de dados, alargando assim as informações a fornecer. Este artigo prevê igualmente exceções à obrigação de informações sempre que estas são necessárias e

---

23 COM (2005) 475 final

24 Artigo 14.º da Decisão 2009/371/JAI da Europol.

25 Artigo 15.º da Decisão 2009/426/JAI da Eurojust.

26 Artigo 14.º da Decisão 2009/371/JAI da Europol.

27 Acórdão do TEDH de 4.12.2008, S. e Marper/UK (pedidos n.os 30562/04 e 30566/04).

28 Adotada pela Conferência internacional dos comissários para a proteção de dados e da vida privada em 5.11.2009.

proporcionadas numa sociedade democrática para o exercício das funções das autoridades competentes (com base no artigo 13.º da Diretiva 95/46/CE e no artigo 17.º da Decisão-Quadro 2008/977/JAI).

O artigo 12.° prevê a obrigação de os Estados-Membros assegurarem o direito de acesso aos dados pessoais do titular desses dados. Retoma o disposto no artigo 12.º, alínea a), da Diretiva 95/46/CE, e acrescenta novos elementos, tais como a obrigação de informar os titulares dos dados (sobre o período de conservação, o direito de retificação, de apagamento ou de solicitar a limitação do tratamento, bem como de apresentar uma queixa).

O artigo 13.º prevê, inspirado no artigo 17.º, n.os 2 e 3, da Decisão-Quadro 2008/977/JAI, que os Estados-Membros podem adotar medidas legislativas que restrinjam o direito de acesso se a natureza específica do tratamento de dados nos domínios policial e judiciário assim o exigirem, bem como informar o titular de dados sobre a limitação de acesso.

O artigo 14.º introduz a regra segundo a qual, nos casos em que o acesso direto seja limitado, o titular dos dados deve ser informado sobre a possibilidade de acesso indireto por intermédio da autoridade de controlo, que deve exercer esse direito por conta da referida pessoa e tem a obrigação de a informar sobre o resultado das suas verificações.

O artigo 15.º sobre o direito de retificação, retoma o disposto no artigo 12.º, alínea b), da Diretiva 95/46/CE e, no que diz respeito às obrigações impostas em caso de recusa, o disposto no artigo 18.º, n.º 1, da Decisão-Quadro 2008/977/JAI.

O artigo 16.º sobre o direito de apagamento, retoma o disposto no artigo 12.º, alínea b), da Diretiva 95/46/CE, e, no que diz respeito às obrigações impostas em caso de recusa, o disposto no artigo 18.º, n.º 1, da Decisão-Quadro 2008/977/JAI. Integra igualmente o direito à marcação dos dados em determinados casos, evitando o termo ambíguo «bloqueio», utilizado no artigo 12.º, alínea b), da Diretiva 95/46/CE e no artigo 18.º, n.º 1, da Decisão-Quadro 2008/977/JAI.

O artigo 17.º sobre a retificação, o apagamento e a limitação do tratamento em processos judiciais, fornece uma clarificação com base no artigo 4.º, n.º 4, da Decisão-Quadro 2008/977/JAI.

3.4.4. CAPÍTULO IV – RESPONSÁVEL PELO TRATAMENTO E SUBCONTRATANTE

3.4.4.1. SECÇÃO 1 OBRIGAÇÕES GERAIS

O artigo 18.º descreve as obrigações que incumbem ao responsável pelo tratamento para se conformar com a presente diretiva e assegurar a sua observância, incluindo através da adoção de regras internas e mecanismos para esse efeito.

O artigo 19.º estabelece que os Estados-Membros devem assegurar que o responsável pelo tratamento respeite as obrigações decorrentes dos princípios de proteção de dados desde a conceção e de proteção de dados por defeito.

O artigo 20.º relativo aos responsáveis conjuntos pelo tratamento, clarifica o estatuto destes últimos no que diz respeito às suas relações internas.

O artigo 21.º clarifica a função e as obrigações dos subcontratantes, retomando parcialmente o artigo 17.º, n.º 2, da Diretiva 95/46/CE, e acrescentando novos elementos, designadamente o

facto de um subcontratante que efetue o tratamento de dados de uma forma diferente da prevista nas instruções do responsável pelo tratamento dever ser considerado corresponsável pelo tratamento.

O artigo 22.º sobre o tratamento efetuado sob a autoridade do responsável pelo tratamento ou do subcontratante, retoma o disposto no artigo 16.º da Diretiva 95/46/CE.

O artigo 23.º introduz a obrigação para os responsáveis pelo tratamento e subcontratantes de manterem documentação relativa a todos os sistemas e procedimentos de tratamento sob a sua responsabilidade.

O artigo 24.º diz respeito à conservação de registos, em linha com o artigo 10.º, n.º 1, da Decisão-Quadro 2008/977, fornecendo, no entanto, clarificações adicionais.

O artigo 25.º clarifica as obrigações que incumbem ao responsável pelo tratamento e ao subcontratante relativamente à cooperação com a autoridade de controlo.

O artigo 26.º, inspirado no artigo 23.º da Decisão-Quadro 2008/977/JAI, visa os casos em que é obrigatória a consulta da autoridade de controlo previamente ao tratamento.

3.4.4.2. SECÇÃO 2 SEGURANÇA DOS DADOS

O artigo 27.º sobre a segurança do tratamento, é baseado no atual artigo 17.º, n.º 1, da Diretiva 95/46/CE, relativo à segurança do tratamento, e no artigo 22.º da Decisão-Quadro 2008/977/JAI, alargando aos subcontratantes as obrigações daí decorrentes, independentemente do contrato que celebraram com o responsável pelo tratamento.

Os artigos 28.º e 29.º introduzem uma obrigação de notificação das violações de dados pessoais, inspirada na notificação das violações de dados pessoais prevista no artigo 4.º, n.º 3, da Diretiva 2002/58/CE (relativa à privacidade e às comunicações eletrónicas), clarificando e distinguindo, por um lado, a obrigação de notificação à autoridade de controlo (artigo 28.º) e, por outro, a obrigação de informação, em determinadas circunstâncias, do titular dos dados (artigo 29.º). O artigo 29.º prevê igualmente derrogações com base nos motivos enumerados no artigo 11.º, n.º 4.

3.4.4.3. SECÇÃO 3 DELEGADO PARA A PROTEÇÃO DE DADOS

O artigo 30.º introduz a obrigação, que incumbe ao responsável pelo tratamento, de designar um delegado para a proteção de dados encarregado das atribuições enumeradas no artigo 32.º. Sempre que várias autoridades competentes atuem sob o controlo de uma autoridade central, que funciona como responsável pelo tratamento, deve incumbir pelo menos esta autoridade central designar o referido delegado. O artigo 18.º, n.º 2, da Diretiva 95/46/CE, prevê a possibilidade de os Estados-Membros introduzirem esse requisito em vez da obrigação de notificação geral imposta pela referida diretiva.

O artigo 31.º define a função do delegado para a proteção de dados.

O artigo 32.º prevê as atribuições do delegado para a proteção de dados.

3.4.5. *CAPÍTULO V – TRANSFERÊNCIA DE DADOS PESSOAIS PARA PAÍSES TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS*

O artigo 33.º enuncia os princípios gerais aplicáveis às transferências de dados para países terceiros ou organizações internacionais no domínio da cooperação policial e da cooperação judiciária em matéria penal, incluindo as transferências ulteriores. Clarifica que as transferências para países terceiros só podem ocorrer se forem necessárias para a prevenção, investigação, deteção e repressão de infrações penais ou a execução de sanções penais.

O artigo 34.º autoriza as transferências para países terceiros em relação aos quais a Comissão tiver adotado uma decisão sobre o nível de proteção adequado por força do Regulamento .../.../201X, ou decorrentes especificamente do domínio da cooperação policial e da cooperação judiciária em matéria penal ou, na falta de tal decisão, se existirem as garantias adequadas. Enquanto não tiver sido adotada uma decisão que declare o nível de proteção adequado, a diretiva garante que as transferências possam prosseguir com base em garantias adequadas e derrogações. Estabelece, além disso, os critérios de avaliação, por parte da Comissão, de um nível adequado ou inadequado de proteção, e inclui expressamente o primado do estado de direito, o direito de recurso judicial e um controlo independente. O artigo prevê igualmente a possibilidade de a Comissão avaliar o nível de proteção assegurado por um território ou um setor de tratamento num país terceiro. Estabelece que uma decisão geral relativa ao nível de proteção adequado, adotada segundo os procedimentos previstos no artigo 38.º do regulamento geral de proteção de dados, é aplicável nos limites da presente diretiva. Pode ser igualmente adotada pela Comissão uma decisão sobre o nível de proteção adequado para efeitos exclusivos da presente diretiva.

O artigo 35.º define as garantias adequadas que, na a falta de uma decisão da Comissão sobre o nível de proteção adequado, são exigidas antes de qualquer transferência internacional. Essas garantias podem ser apresentadas através de um instrumento juridicamente vinculativo, como um acordo internacional. O responsável pelo tratamento pode igualmente, com base numa avaliação das circunstâncias inerentes à transferência, concluir pela existência de tais garantias.

O artigo 36.º define as derrogações autorizadas para a transferência de dados, com base no artigo 26.º da Diretiva 95/46/CE e no artigo 13.º da Decisão-Quadro 2008/977/JAI.

O artigo 37.º obriga os Estados-Membros a preverem que o responsável pelo tratamento informe o destinatário de quaisquer restrições de tratamento e tome todas as medidas razoáveis para assegurar o cumprimento dessas restrições pelos destinatários de dados pessoais no país terceiro ou na organização internacional.

O artigo 38.º prevê expressamente a elaboração de mecanismos de cooperação internacionais no domínio da proteção de dados pessoais entre a Comissão e as autoridades de controlo dos países terceiros, nomeadamente os que se considera oferecerem um nível de proteção adequado, tendo em conta a Recomendação da OCDE, relativa à cooperação transfronteiriça na aplicação de legislações de proteção da privacidade, de 12 de junho de 2007.

CAPÍTULO VI – AUTORIDADES NACIONAIS DE CONTROLO

3.4.5.1. SECÇÃO 1 ESTATUTO INDEPENDENTE

O artigo 39.º obriga os Estados-Membros a criarem autoridades de controlo, nos termos do artigo 28.º, n.º 1, da Diretiva 95/46/CE, e do artigo 25.º da Decisão-Quadro 2008/977/JAI, e alargarem a missão dessas autoridades a fim de contribuírem para a aplicação coerente da diretiva no conjunto da União, que poderá ser a autoridade de controlo criada por força do regulamento geral de proteção de dados.

O artigo 40.º clarifica as condições que garantem a independência das autoridades de controlo, em aplicação da jurisprudência do Tribunal de Justiça da UE[29], e inspirando-se igualmente no artigo 44.º do Regulamento (CE) n.º 45/2001[30].

O artigo 41.º prevê as condições gerais para os membros das autoridades de controlo, em aplicação da jurisprudência relevante[31], baseando-se também no artigo 42.º, n.ºs 2 a 6, do Regulamento (CE) 45/2001.

O artigo 42.º define as regras relativas à criação da autoridade de controlo, incluindo as aplicáveis aos seus membros, que os Estados-Membros devem estabelecer por via legislativa.

O artigo 43.º sobre o sigilo profissional dos membros e do pessoal da autoridade de controlo, retoma as disposições do artigo 28.º, n.º 7, da Diretiva 95/46/CE, e do artigo 25.º, n.º 4, da Decisão-Quadro 2008/977/JAI.

3.4.5.2. SECÇÃO 2 FUNÇÕES E PODERES

O artigo 44.º, baseado no artigo 28.º, n.º 6, da Diretiva 95/46/CE, e no artigo 25.º, n.º 1, da Decisão-Quadro 2008/977/JAI, define a competência das autoridades de controlo. Os tribunais, quando atuam na qualidade de poder judiciário, são dispensados da fiscalização pelas autoridades de controlo, mas não de aplicarem as regras materiais relativas à proteção de dados.

O artigo 45.º prevê a obrigação de os Estados-Membros definirem as funções da autoridade de controlo, que consistem nomeadamente em receber e examinar queixas, bem como promover a sensibilização do público sobre os riscos, regras, garantias e direitos existentes. Uma função própria às autoridades de controlo no contexto da presente diretiva consiste, sempre que o acesso direto aos dados seja recusado ou limitado, em exercer o direito de acesso por conta dos titulares de dados e em verificar a licitude do tratamento desses dados.

O artigo 46.º, baseado no artigo 28.º, n.º 3, da Diretiva 95/46/CE, e no artigo 25.º, n.ºs 2 e 3 da Decisão-Quadro 2008/977/JAI, enuncia os poderes da autoridade de controlo. O artigo 47.º estabelece a obrigação para as autoridades de controlo de elaborarem relatórios de atividades anuais, com base no artigo 28.º, n.º 5, da Diretiva 95/46/CE.

---

29 Tribunal de Justiça da União Europeia, acórdão de 9 de março de 2010 no processo C-518/07, Comissão/Alemanha (Coletânea 2010, p. I-1885).

30 Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares relativamente ao tratamento de dados pessoais pelas instituições e organismos comunitários e sobre a livre circulação desses dados; JO L 8 de 12.1.2001, p. 1.

31 Cit. nota de pé de página 27.

3.4.6. CAPÍTULO VII – COOPERAÇÃO

O artigo 48.º introduz regras em matéria de assistência mútua obrigatória, enquanto o artigo 28.º, n.º 6, segundo parágrafo, da Diretiva 95/46/CE, previa uma mera obrigação geral de cooperação, sem outra especificação.

O artigo 49.º prevê que o Comité Europeu para a Proteção de Dados, criado pelo regulamento geral de proteção de dados, exerce as suas atribuições também no contexto dos tratamentos abrangidos pelo âmbito de aplicação da presente diretiva. Tendo em vista um apoio suplementar, a Comissão solicitará o parecer dos representantes das autoridades dos Estados-Membros competentes em matéria de prevenção, investigação, deteção e repressão de infrações penais, bem como dos representantes da Europol e da Eurojust, através de um grupo de peritos, sobre os aspetos relacionados com a aplicação da lei no domínio da proteção de dados.

3.4.7. CAPÍTULO VIII – VIAS DE RECURSO, RESPONSABILIDADE E SANÇÕES

O artigo 50.º prevê o direito de qualquer titular de dados apresentar uma queixa a uma autoridade de controlo, com base no artigo 28.º, n.º 4, da Diretiva 95/46/CE, e visa qualquer infração à diretiva relacionada com o queixoso. Especifica também os organismos, organizações ou associações que podem apresentar uma queixa em nome do titular dos dados ou, em caso de violação de dados pessoais, independentemente da eventual queixa apresentada por um titular de dados.

O artigo 51.º diz respeito ao direito ao recurso aos tribunais contra uma autoridade de controlo. Tem por base a disposição geral do artigo 28.º, n.º 3, da Diretiva 95/46/CE, e prevê especificamente que o titular dos dados pode intentar uma ação em tribunal a fim de obrigar a autoridade de controlo a dar seguimento a uma queixa.

O artigo 52.º refere-se ao direito a ação judicial contra um responsável pelo tratamento ou subcontratante, com base no artigo 22.º da Diretiva 95/46/CE e no artigo 20.º da Decisão-Quadro 2008/977/JAI.

O artigo 53.º introduz regras comuns para os procedimentos judiciais, incluindo o direito conferido a organismos, organizações ou associações de representar os titulares de dados nos tribunais, e o direito de as autoridades de controlo intervirem em processos judiciais. A obrigação que incumbe aos Estados-Membros de assegurarem processos judiciais rápidos é inspirada no artigo 18.º, n.º 1, da Diretiva 2000/31/CE relativa ao comércio eletrónico[32].

O artigo 54.º obriga os Estados-Membros a preverem um direito de indemnização. Tem por base o artigo 23.º da Diretiva 95/46/CE, e o artigo 19.º, n.º 1, da Decisão-Quadro 2008/977/JAI, alargando esse direito aos danos causados pelos subcontratantes e clarificando a responsabilidade dos responsáveis conjuntos pelo tratamento e dos subcontratantes que asseguram conjuntamente o tratamento.

O artigo 55.º obriga os Estados-Membros a estabelecer regras sobre sanções, a sancionar infrações à diretiva e a assegurar a sua aplicação.

---

[32] Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva relativa ao comércio eletrónico»); JO L 178 de 17.7.2000, p. 1.

3.4.8. CAPÍTULO IX - ATOS DELEGADOS E ATOS DE EXECUÇÃO

O artigo 56.º contém as disposições-tipo aplicáveis ao exercício da delegação, nos termos do artigo 290.º do TFUE. Este último permite ao legislador delegar na Comissão o poder de adotar atos não legislativos de aplicação geral para completar ou alterar determinados elementos não essenciais de um ato legislativo (atos quase-legislativos).

O artigo 57.º contém a disposição relativa ao procedimento de comité necessário para conferir competências de execução à Comissão nos casos em que, em conformidade com o artigo 291.º do TFUE, são necessárias condições uniformes para a execução de atos juridicamente vinculativos da União. Aplica-se o procedimento de exame.

3.4.9. CAPÍTULO X - DISPOSIÇÕES FINAIS

O artigo 58.º revoga a Decisão-Quadro 2008/977/JAI.

O artigo 59.º estabelece que as disposições específicas no que respeita ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, que figuram nos atos da União que regulam o tratamento de dados pessoais ou o acesso aos sistemas de informação abrangidos pelo âmbito de aplicação da diretiva, e foram adotados antes da adoção da presente diretiva, não serão afetados.

O artigo 60.º clarifica a relação da presente diretiva com acordos internacionais concluídos anteriormente pelos Estados-Membros no domínio da cooperação judiciária em matéria penal e da cooperação policial.

O artigo 61.º estabelece a obrigação de a Comissão avaliar e redigir um relatório sobre a execução da diretiva, a fim de apreciar a necessidade de a harmonizar com disposições específicas anteriormente adotadas, enunciadas no artigo 59.º da presente diretiva.

O artigo 62.º estabelece a obrigação de os Estados-Membros transporem a diretiva para o seu direito nacional e notificarem à Comissão as disposições adotadas por força da diretiva.

O artigo 63.º fixa a data de entrada em vigor da diretiva.

O artigo 64.º estabelece os destinatários da presente diretiva.

4. INCIDÊNCIA ORÇAMENTAL

A ficha financeira legislativa que acompanha a proposta de regulamento geral de proteção de dados cobre as incidências orçamentais do regulamento e da presente diretiva.

2012/0010 (COD)

Proposta de

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 e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados

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,

Após consulta da Autoridade Europeia para a Proteção de Dados[33],

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

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

(2) O tratamento dos dados pessoais é concebido para servir as pessoas; os princípios e as regras em matéria de proteção das pessoas singulares no que respeita ao tratamento dos seus dados pessoais devem 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. O tratamento dos dados deve 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 registaram um espetacular aumento. As novas tecnologias permitem às autoridades competentes utilizar dados pessoais numa escala sem precedentes no exercício das suas atividades.

[33] JO C , , p. .

(4) Esta evolução exige uma maior facilidade na livre circulação de dados entre as autoridades competentes a nível da União e na sua transferência para países terceiros e organizações internacionais, assegurando paralelamente um elevado nível de proteção dos dados pessoais. Este contexto obriga ao estabelecimento na União de um quadro de proteção de dados sólido e mais coerente, apoiado por uma aplicação rigorosa das regras.

(5) A 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[34], é aplicável a todas as atividades de tratamento de dados pessoais realizadas nos Estados-Membros, nos setores público e privado. Não se aplica, porém, 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, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal[35], 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 os Estados-Membros.

(7) É crucial assegurar um nível elevado e coerente de proteção dos dados pessoais das pessoas singulares e facilitar o intercâmbio de dados pessoais entre as autoridades competentes dos Estados-Membros, a fim de assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação policial. Para tal, o nível de proteção dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, tem de ser equivalente em todos os Estados-Membros. A proteção efetiva dos dados pessoais na União exige não só reforçar os direitos dos titulares de dados e as obrigações dos responsáveis pelo tratamento de dados pessoais, mas também 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 Tratado sobre o Funcionamento da União Europeia prevê que o Parlamento Europeu e o Conselho estabeleçam as 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) Com base nessa orientação, o Regulamento UE …../2012 do Parlamento Europeu e do Conselho, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral de proteção de dados), estabelece regras gerais visando proteger as pessoas singulares relativamente ao tratamento de dados pessoais e assegurar a livre circulação de dados pessoais na União.

---

34 JO L 281 de 23.11.1995, p. 31.

35 JO L 350 de 30.12.2008, p. 60.

(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 a livre circulação desses dados, nos domínios da cooperação judiciária em matéria penal e da cooperação policial, com base no artigo 16.º do Tratado sobre o Funcionamento da União Europeia.

(11) Por conseguinte, uma diretiva distinta deve permitir responder à natureza específica destes domínios e estabelecer 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 e repressão de infrações penais ou de execução de sanções penais.

(12) A fim de assegurar o mesmo nível de proteção para as pessoas singulares através de direitos juridicamente protegidos no conjunto da União e evitar que as divergências constituam um obstáculo ao intercâmbio de dados pessoais entre as autoridades competentes, a diretiva prevê regras harmonizadas para a proteção e a livre circulação de dados pessoais nos domínios da cooperação judiciária em matéria penal e da cooperação policial.

(13) A presente diretiva permite tomar em consideração o princípio do direito de acesso público aos documentos oficiais aquando da aplicação das suas disposições.

(14) A proteção conferida pela presente diretiva diz respeito a pessoas singulares, independentemente da sua nacionalidade ou lugar de residência, relativamente ao tratamento de dados pessoais.

(15) A proteção das pessoas singulares deve ser neutra em termos tecnológicos e independente das técnicas utilizadas, sob a pena de criar um sério risco de ser contornada. Deve aplicar-se ao tratamento de dados pessoais por meios automatizados e manuais se os dados estiverem contidos ou forem destinados a serem conservados num sistema de ficheiros. As pastas ou conjuntos de pastas, bem como as suas capas, que não estejam estruturadas de acordo com critérios específicos, não se incluem no âmbito de aplicação da presente diretiva. A presente diretiva não se aplica ao tratamento de dados pessoais efetuado no exercício de atividades não sujeitas à aplicação do direito da União, nomeadamente as relativas à segurança nacional, nem aos dados tratados pelas instituições, organismos, serviços e agências da União, designadamente a Europol ou a Eurojust.

(16) Os princípios da proteção de dados devem aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios suscetíveis de serem razoavelmente utilizados, quer pelo responsável pelo tratamento dos dados quer por qualquer outra pessoa, para identificar a referida pessoa. Os princípios da proteção de dados não se aplicam a dados tornados de tal forma anónimos que o titular dos dados já não possa ser identificado.

(17) Os dados pessoais relativos à saúde devem incluir, em especial, todos os dados relativos ao estado de saúde de um titular de dados, informações sobre a inscrição da

pessoa singular para a prestação de serviços de saúde, informações sobre pagamentos ou elegibilidade para cuidados de saúde; um número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; quaisquer informações sobre a pessoa recolhidas no decurso de uma prestação de serviços de saúde; informações obtidas a partir de testes ou exames de uma parte do corpo ou de uma substância corporal, incluindo amostras biológicas; identificação de uma pessoa enquanto prestador de cuidados de saúde ao doente; ou quaisquer informações sobre, por exemplo, uma doença, deficiência, risco de doença, historial clínico, tratamento clínico ou estado físico ou biomédico atual do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um aparelho médico ou um teste de diagnóstico *in vitro*.

(18) Qualquer tratamento de dados pessoais deve ser efetuado de forma lícita, leal e transparente para com as pessoas em causa. Em especial, as finalidades específicas do tratamento devem ser explícitas.

(19) Para efeitos de prevenção, investigação e repressão de infrações penais, é necessário que as autoridades competentes conservem e tratem os dados pessoais, recolhidos no contexto da prevenção, investigação, deteção e repressão de infrações penais específicas, e para além desse contexto, a fim de obter uma melhor compreensão dos fenómenos criminais e das tendências que os caracterizam, recolher informação específica sobre as redes criminosas organizadas e estabelecer ligações entre as diferentes infrações detetadas.

(20) Os dados pessoais não devem ser tratados para fins incompatíveis com a finalidade para a qual foram recolhidos. Os dados pessoais tratados devem ser adequados, pertinentes e não excessivos para as finalidades do tratamento. Devem ser adotadas todas as medidas razoáveis para assegurar que os dados pessoais inexatos são retificados ou apagados.

(21) É conveniente aplicar o princípio da exatidão dos dados tendo em conta a natureza e a finalidade do tratamento em causa. Em especial no caso de processos judiciais, as declarações que contêm dados pessoais são baseadas em perceções pessoais subjetivas e nem sempre são verificáveis. Este princípio não deve, portanto aplicar-se à exatidão da própria declaração, mas simplesmente ao facto de tal declaração ter sido feita.

(22) Na interpretação e aplicação dos princípios gerais relacionados com o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais, ou de execução de sanções penais, deve atender-se às especificidades do setor, incluindo os objetivos específicos prosseguidos.

(23) 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 uma distinção o mais clara possível 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.

(24) Na medida do possível, os dados pessoais devem ser distinguidos em função do seu grau de precisão e de fiabilidade. Os factos devem ser distinguidos de apreciações

pessoais, a fim de assegurar simultaneamente a proteção das pessoas singulares e a qualidade e a fiabilidade da informação tratada pelas autoridades competentes.

(25) Para ser lícito, o tratamento de dados pessoais tem de ser necessário para o respeito de uma obrigação legal à qual o responsável pelo tratamento esteja sujeito, bem como para a execução de uma missão de interesse público por uma autoridade competente prevista na lei, ou para a proteção dos interesses vitais do titular dos dados ou de outra pessoa, ou para a prevenção de uma ameaça grave e imediata para a segurança pública.

(26) Os dados pessoais que sejam, devido à sua natureza, especialmente sensíveis do ponto de vista dos direitos fundamentais ou da privacidade, designadamente os dados genéticos, merecem proteção específica. Estes dados não devem ser objeto de tratamento, salvo se essa operação for especificamente autorizada por uma lei que preveja medidas adequadas de proteção dos interesses legítimos do titular dos dados, ou se for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa, ou se estiver relacionado com dados que tenham sido manifestamente tornados públicos pelo titular dos dados.

(27) Qualquer pessoa singular deve ter o direito a não estar sujeita a uma medida baseada exclusivamente no tratamento automatizado, se este produzir efeitos negativos na esfera jurídica dessa pessoa, salvo se autorizada por lei e subordinada a medidas adequadas que garantam os interesses legítimos do titular de dados.

(28) A fim de permitir aos titulares de dados exercer os seus direitos, quaisquer informações que lhe sejam dirigidas devem ser de fácil acesso e compreensão e, nomeadamente, formuladas em termos claros e simples.

(29) Devem ser previstas modalidades para facilitar o exercício pelo titular de dados dos direitos conferidos pela presente diretiva, incluindo mecanismos para solicitar, a título gratuito, em especial o acesso aos dados, a sua retificação e apagamento. O responsável pelo tratamento deve ser obrigado a responder aos pedidos do titular de dados sem demora injustificada.

(30) Os princípios de tratamento leal e transparente exigem que o titular dos dados seja informado, em especial, da existência da operação de tratamento de dados e das suas finalidades, do período de conservação dos dados, da existência do direito de acesso, retificação ou apagamento, bem como do seu direito de apresentar uma queixa. Sempre que os dados forem recolhidos junto do titular dos dados, este deve ser também informado da obrigatoriedade de fornecer esses dados e das respetivas consequências, caso não os faculte.

(31) As informações sobre o tratamento de dados pessoais devem ser fornecidas ao titular dos dados no momento da sua recolha ou, se a recolha não foi obtida junto da pessoa em causa, no momento do seu registo ou num prazo razoável após a sua recolha, dependendo das circunstâncias do caso.

(32) Qualquer pessoa deve ter o direito de acesso aos dados recolhidos sobre si e de exercer facilmente este direito, a fim de conhecer e verificar a licitude do tratamento. Por conseguinte, cada titular de dados deve ter o direito de conhecer e ser informado, em especial, das finalidades a que se destinam os dados tratados, da duração da sua conservação, bem como da identidade dos destinatários, incluindo em países terceiros.

Os titulares de dados devem poder obter uma cópia dos seus dados pessoais objeto de tratamento.

(33) Os Estados-Membros devem ser autorizados a adotar medidas legislativas visando atrasar ou limitar a informação dos titulares de dados ou o acesso aos dados pessoais que lhes digam respeito, ou a não fornecer essas informações ou esse acesso, desde que tal limitação, parcial ou total, represente uma medida necessária e proporcional numa sociedade democrática, tendo devidamente em conta os interesses legítimos do titular de dados, a fim de evitar que tal constitua um obstáculo para os inquéritos, investigações e procedimentos oficiais ou legais, para evitar prejudicar a prevenção, investigação, deteção e repressão de infrações penais ou a execução de sanções penais, para proteger a segurança pública ou a segurança nacional ou proteger o titular de dados ou os direitos e as liberdades de terceiros.

(34) Qualquer recusa ou restrição do acesso deve ser comunicada por escrito ao titular dos dados, indicando simultaneamente os motivos factuais ou jurídicos que fundamentam a decisão adotada.

(35) Sempre que os Estados-Membros tiverem adotado medidas legislativas para limitar total ou parcialmente o direito de acesso, o titular de dados deve ter o direito de solicitar à autoridade nacional de controlo competente que verifique a licitude do tratamento. O titular de dados deve ser informado desse direito. Quando o direito de acesso for exercido pela autoridade de controlo em nome do titular de dados, a autoridade de controlo deve pelo menos informar o interessado de que foram realizadas todas as verificações necessárias e do resultado relativamente à licitude do tratamento em questão.

(36) Qualquer pessoa deve ter o direito a que os dados que lhe digam respeito sejam retificados e o «direito a ser esquecido», quando o tratamento não for conforme com os princípios gerais enunciados na presente diretiva. Sempre que os dados pessoais forem tratados no âmbito de uma investigação criminal ou de um processo penal, o direito à informação, o direito de acesso, de retificação e de apagamento, bem como o direito de limitação do tratamento, podem ser exercidos em conformidade com as regras nacionais aplicáveis aos processos judiciais.

(37) Deve ser definida uma responsabilidade global do responsável pelo tratamento por qualquer tratamento de dados pessoais que ele próprio realize ou que seja realizado por sua conta. Em especial, o responsável pelo tratamento deve assegurar a conformidade das operações de tratamento de dados com o disposto na presente diretiva.

(38) A proteção dos direitos e liberdades dos titulares de dados relativamente ao tratamento dos seus dados pessoais exige a adotada de medidas técnicas e organizativas adequadas, a fim de assegurar o cumprimento dos requisitos da presente diretiva. A fim de assegurar a conformidade com a presente diretiva, o responsável pelo tratamento deve adotar regras internas e aplicar medidas apropriadas conformes, em especial, com os princípios de proteção de dados desde a conceção e de proteção de dados por defeito.

(39) A proteção dos direitos e liberdades dos titulares de dados, bem como a responsabilidade dos responsáveis pelo tratamento e dos subcontratantes, exige uma clara repartição das responsabilidades nos termos da presente diretiva, nomeadamente

quando o responsável pelo tratamento determina as finalidades, as condições e os meios do tratamento conjuntamente com outros responsáveis, ou quando uma operação de tratamento de dados é efetuada por conta de um responsável pelo tratamento.

(40) A fim de comprovar a observância da presente diretiva, o responsável pelo tratamento ou o subcontratante deve documentar cada operação de tratamento de dados. Cada responsável pelo tratamento e subcontratante deve ser obrigado a cooperar com a autoridade de controlo e a disponibilizar essa documentação, quando tal lhe for solicitado, para que possa servir ao controlo dessas operações de tratamento.

(41) A fim de assegurar a proteção efetiva dos direitos e liberdades dos titulares de dados através de ações preventivas, o responsável pelo tratamento ou o subcontratante deve, em determinados casos, consultar a autoridade de controlo previamente à operação de tratamento.

(42) A violação de dados pessoais pode, se não forem adotadas medidas adequadas e oportunas, causar danos, nomeadamente à reputação da pessoa singular em causa. Assim, logo que o responsável pelo tratamento tenha conhecimento da ocorrência de uma violação, deve comunicá-la à autoridade nacional competente. As pessoas singulares cujos dados pessoais possam ter sido afetados negativamente por tal violação, devem ser avisadas sem demora injustificada, para que possam adotar as precauções necessárias. Deve considerar-se que uma violação afeta negativamente os dados pessoais ou a privacidade de um titular de dados sempre que daí possa resultar, por exemplo, roubo ou usurpação de identidade, danos físicos, humilhações ou danos significativos contra a reputação, consecutivos ao tratamento de dados pessoais.

(43) Ao estabelecer regras pormenorizadas relativamente ao formato e aos procedimentos aplicáveis à notificação das violações de dados pessoais, deve ter-se devidamente em conta as circunstâncias da violação, nomeadamente a existência ou não de proteção dos dados pessoais através de medidas técnicas de proteção adequadas para reduzir eficazmente a probabilidade de utilização abusiva. Além disso, tais regras e procedimentos devem ter em conta os legítimos interesses das autoridades de aplicação da lei nos casos em que uma divulgação precoce de informações possa dificultar desnecessariamente a investigação das circunstâncias de uma violação.

(44) O responsável pelo tratamento, ou o subcontratante, deve designar uma pessoa para o ajudar a controlar a conformidade das disposições adotadas por força da presente diretiva. Um delegado para a proteção de dados pode ser designado conjuntamente por diversas entidades da autoridade competente. Os delegados para a proteção de dados devem estar em condições de desempenhar as suas funções e atribuições de forma efetiva e com total independência.

(45) Os Estados-Membros devem assegurar que uma transferência para um país terceiro só possa ser realizada se for necessária para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou para a execução de sanções penais, e se o responsável pelo tratamento no país terceiro ou na organização internacional for uma autoridade competente na aceção da presente diretiva. Uma transferência pode realizar-se nos casos em que a Comissão tiver decidido que o país terceiro, ou a organização internacional em questão, garante um nível de proteção adequado, ou se tiverem sido apresentadas garantias adequadas.

(46) A Comissão pode decidir, com efeitos no conjunto da União, que determinados países terceiros, um território ou um setor de tratamento de dados de um país terceiro, ou uma organização internacional, asseguram um nível de proteção de dados adequado, garantindo assim a segurança jurídica e a uniformidade a nível da União relativamente a países terceiros ou organizações internacionais que sejam consideradas aptas a assegurar tal nível de proteção. Nestes casos, podem realizar-se transferências de dados pessoais para esses países sem que para tal seja necessário qualquer outra autorização.

(47) Em consonância com os valores fundamentais sobre os quais assenta a União, particularmente a proteção dos direitos humanos, a Comissão deve ter em consideração em que medida esse país respeita o primado do Estado de direito, garante o acesso à justiça e observa as regras e normas internacionais no domínio dos direitos humanos.

(48) A Comissão deve igualmente poder reconhecer que um país terceiro, ou um território ou um setor de tratamento de um país terceiro, ou uma organização internacional, não assegura um nível de proteção adequado de dados. Se for esse no caso, deve ser proibida a transferência de dados pessoais para esse país terceiro, salvo se tiver por base um acordo internacional, garantias adequadas ou uma derrogação. É conveniente prever procedimentos de consulta entre a Comissão e o país terceiro ou a organização internacional. Todavia, tal decisão da Comissão não prejudica a possibilidade de realizar transferências com base em garantias adequadas ou numa derrogação prevista na diretiva.

(49) As transferências que não se basearem numa decisão sobre o nível adequado da proteção só devem ser autorizadas se forem apresentadas garantias apropriadas num instrumento juridicamente vinculativo que garanta a proteção dos dados pessoais, ou se o responsável pelo tratamento ou o subcontratante tiver avaliado todas as circunstâncias inerentes à transferência de dados ou ao conjunto de operações de transferências de dados e, com base nessa avaliação, considerar existirem garantias adequadas relativamente à proteção de dados pessoais. Caso não existam fundamentos para a autorização de transferência, devem ser permitidas derrogações se forem necessárias para proteger os interesses vitais do titular de dados ou de um terceiro, ou para assegurar os interesses legítimos dessa pessoa, desde que a legislação do Estado-Membro que efetua a transferência dos dados assim o preveja, ou se for essencial para a prevenção de uma ameaça imediata e grave para a segurança pública de um Estado-Membro ou de um país terceiro ou, em certos casos, para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, ou em casos especiais, tendo em vista a declaração, o exercício ou a defesa de um direito num processo judicial.

(50) Sempre que os dados pessoais atravessam fronteiras há um risco acrescido de que as pessoas singulares não possam exercer o seu direito 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 apreciar as queixas ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras. Os seus esforços para colaborar no contexto transfronteiriço podem ser também restringidos por competências insuficientes ou regimes jurídicos incoerentes. Por conseguinte, é necessário promover uma cooperação mais estreita entre as autoridades de controlo da proteção de dados a fim de que possam efetuar o

intercâmbio de informações e realizar investigações com as suas homólogas internacionais.

(51) A criação de autoridades de controlo nos Estados-Membros, que exerçam as suas funções com total independência, constitui um elemento essencial da proteção das pessoas singulares no que respeita ao tratamento dos seus dados pessoais. As autoridades de controlo devem supervisionar a aplicação das disposições da presente diretiva e contribuir para a sua aplicação coerente no conjunto da União, a fim de proteger as pessoas singulares relativamente ao tratamento dos seus dados pessoais. Para esse efeito, as autoridades de controlo devem cooperar entre si e com a Comissão.

(52) Os Estados Membros podem confiar a uma autoridade de controlo já criada nos Estados-Membros nos termos do Regulamento (UE) .../2012 a responsabilidade pelas funções a desempenhar pelas autoridades nacionais de controlo a instituir por força da presente diretiva.

(53) Deve ser permitido aos Estados-Membros criarem várias autoridades de controlo de modo a refletir a sua estrutura constitucional, organizacional e administrativa. É conveniente que cada autoridade de controlo disponha dos recursos financeiros e humanos adequados, bem como de instalações e infraestruturas, necessários a um exercício eficaz das suas funções, incluindo as relacionadas com a assistência e a cooperação mútuas com outras autoridades de controlo a nível da União.

(54) As condições gerais aplicáveis aos membros da autoridade de controlo devem ser definidas por lei em cada Estado-Membro e devem prever, em especial, que esses membros são nomeados pelo parlamento ou pelo governo nacional, e incluir disposições sobre a qualificação e as funções desses membros.

(55) Embora a presente diretiva se aplique também às atividades dos tribunais nacionais, a competência das autoridades de controlo não abrange o tratamento de dados pessoais quando os tribunais atuam no âmbito dessas funções, a fim de assegurar a independência dos juízes no exercício das suas funções jurisdicionais. Todavia, esta exceção deve ser estritamente limitada às atividades meramente judiciais relativas a processos em tribunal e não ser aplicável a outras atividades a que os juízes possam estar associados por força do direito nacional.

(56) A fim de assegurar o controlo e a aplicação coerentes da presente diretiva no conjunto da União, as autoridades de controlo devem ter, em cada Estado-Membro, os mesmos deveres e poderes efetivos, incluindo os poderes de investigação, de intervenção juridicamente vinculativa, de deliberação e de sanção, particularmente em caso de queixas apresentadas por pessoas singulares, bem como o poder de intervir em processos judiciais.

(57) Cada autoridade de controlo deve receber as queixas apresentadas por qualquer titular de dados e investigar a matéria. A investigação decorrente de uma queixa deve ser realizada, embora sujeita a revisão judicial, na medida adequada ao caso específico. A autoridade de controlo deve informar a pessoa em causa da evolução e do resultado da queixa num prazo razoável. Se o caso exigir uma investigação mais aprofundada ou a coordenação com outra autoridade de controlo, devem ser fornecidas informações intercalares ao titular dos dados.

(58) As autoridades de controlo devem prestar-se mutuamente assistência no desempenho das suas funções, por forma a assegurar a execução e aplicação coerentes das disposições adotadas em conformidade com a presente diretiva.

(59) O Comité Europeu para a Proteção de Dados, instituído pelo Regulamento (UE) .../2012, deve contribuir para a aplicação coerente da presente diretiva no conjunto da União, nomeadamente no aconselhamento da Comissão e na promoção da cooperação das autoridades de controlo na União.

(60) Qualquer titular de dados deve ter o direito de apresentar uma queixa à autoridade de controlo em qualquer Estado-Membro e dispor do direito de recurso aos tribunais se considerar que os direitos que lhe confere a presente diretiva não são respeitados, se a autoridade de controlo não responder à queixa, ou não agir conforme necessário para proteger os direitos da pessoa em causa.

(61) Qualquer organismo, organização ou associação que vise proteger os direitos e interesses dos titulares de dados no que respeita à proteção dos dados que lhe digam respeito, e seja constituído(a) ao abrigo do direito de um Estado-Membro, deve ter o direito de apresentar aos tribunais queixa junto de uma autoridade de controlo ou de exercer o direito de recurso aos tribunais em nome das pessoas em causa, mediante mandato nesse sentido, ou de apresentar, independentemente da queixa apresentada pela pessoa em causa, uma queixa em seu próprio nome, sempre que considere ter ocorrido uma violação de dados pessoais.

(62) Qualquer pessoa, singular ou coletiva, deve ter o direito de ação judicial contra as decisões que lhes digam respeito emitidas por uma autoridade de controlo. As ações contra uma autoridade de controlo devem ser intentadas nos tribunais do Estado-Membro no território do qual se encontra estabelecida a autoridade de controlo.

(63) Os Estados-Membros devem assegurar que as ações judiciais, para serem eficazes, permitam a adoção rápida de medidas visando a reparação ou a prevenção de uma violação prevista na presente diretiva.

(64) Qualquer dano de que uma pessoa possa ser vítima em resultado de um tratamento ilícito deve ser ressarcido pelo responsável pelo tratamento, ou pelo subcontratante, que no entanto pode ser exonerado da sua responsabilidade se provar que o facto causador do dano não lhe é imputável, nomeadamente se provar que o dano é imputável à pessoa em causa ou em caso de força maior.

(65) Devem ser aplicadas sanções a qualquer pessoa singular ou coletiva, regida pelo direito privado ou público, que não respeite o disposto na presente diretiva. Os Estados-Membros devem assegurar que as sanções sejam efetivas, proporcionadas e dissuasivas, e tomar todas as medidas necessárias à sua aplicação.

(66) Por forma a cumprir os objetivos da presente diretiva, nomeadamente proteger os direitos e liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção dos dados pessoais, e assegurar a livre circulação desses dados pelas autoridades competentes na União, o poder de adotar atos em conformidade com o artigo 290.º do Tratado sobre o Funcionamento da União Europeia deve ser delegado à Comissão. Em especial, devem ser adotados atos delegados em relação à notificação

de violações de dados pessoais à autoridade controlo. É especialmente importante que a Comissão proceda a consultas adequadas ao longo dos seus trabalhos preparatórios, incluindo a nível de peritos. A Comissão, aquando da preparação e elaboração dos atos delegados, deve assegurar uma transmissão simultânea, em tempo útil e em devida forma, dos documentos relevantes ao Parlamento Europeu e ao Conselho.

(67) Por forma a assegurar condições uniformes para a execução da presente diretiva no que respeita à documentação mantida pelos responsáveis pelo tratamento e subcontratantes, à segurança do tratamento, designadamente em relação às normas de codificação, à notificação de uma violação de dados pessoais à autoridade de controlo, e ao nível de proteção adequado assegurado por um país terceiro, um território ou um setor dentro desse país terceiro, ou uma organização internacional, devem ser conferidas competências de execução à Comissão. Essas competências devem ser exercidas em conformidade com o 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[36].

(68) O procedimento de exame deve ser utilizado para a adoção de medidas relativas à documentação mantida pelos responsáveis pelo tratamento e subcontratantes, à segurança do tratamento, à notificação de uma violação de dados pessoais à autoridade de controlo, e ao nível de proteção adequado garantido por um país terceiro, um território ou um setor dentro desse país terceiro, ou uma organização internacional, uma vez que esses atos são de âmbito geral.

(69) A Comissão deve adotar atos de execução imediatamente aplicáveis quando, em casos devidamente fundamentados relacionados com um país terceiro, um território ou um setor de tratamento de dados nesse país terceiro, ou uma organização internacional, que não assegure um nível de proteção adequado, imperativos urgentes assim o exijam.

(70) Dado que os objetivos da presente diretiva, nomeadamente proteger os direitos e liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção de dados pessoais, e assegurar o livre intercâmbio desses dados pelas autoridades competentes na União Europeia, não podem ser suficientemente realizados pelos Estados-Membros e podem pois, em razão da dimensão e dos efeitos da ação, ser melhor realizados a nível da União, esta última pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, a presente diretiva não excede o necessário para atingir esse objetivo.

(71) A Decisão-Quadro 2008/977/JAI é revogada pela presente diretiva.

(72) As disposições específicas no que respeita ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção, repressão de infrações penais ou de execução de sanções penais, mencionadas nos atos da União adotados 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

---

[36] JO L 55 de 28.2.2011, p. 13.

Estados-Membros aos sistemas de informação criados nos termos de Tratados, mantêm-se inalteradas. A Comissão deverá examinar a situação quanto à relação entre a presente diretiva e os atos adotados anteriormente à 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 harmonização dessas disposições específicas com a presente diretiva.

(73) A fim de assegurar uma proteção global e coerente dos dados pessoais na União, os acordos internacionais celebrados pelos Estados-Membros anteriormente à entrada em vigor da presente diretiva devem ser alterados em conformidade com a presente diretiva.

(74) A presente diretiva não prejudica as disposições relativas à luta contra o abuso sexual e a exploração sexual de crianças, bem como a pornografia infantil, previstas na Diretiva 2011/92/UE do Parlamento Europeu e do Conselho de 13 de dezembro de 2011[37].

(75) Nos termos do artigo 6.º-A do Protocolo relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, o Reino Unido e a Irlanda não ficam vinculados pelas regras estabelecidas na presente diretiva sempre que o Reino Unido e a Irlanda 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 Tratado sobre o Funcionamento da União Europeia.

(76) Nos termos dos artigos 2.º e 2.º-A do Protocolo relativo à posição da Dinamarca, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Dinamarca não fica vinculada nem sujeita à aplicação da pela presente diretiva. Uma vez que da presente diretiva desenvolve o acervo de Schengen, por força do disposto no Título V, Parte III, do Tratado sobre o Funcionamento da União Europeia, a Dinamarca decidirá, 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 diretiva para o seu direito nacional.

(77) 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 entre o Conselho da União Europeia e a República da Islândia e o Reino da Noruega, relativo à associação desses Estados à execução, à aplicação e ao desenvolvimento do acervo de Schengen[38].

(78) 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[39].

---

37 JO L 335 de 17.12.2011, p. 1.
38 JO L 176 de 10.7.1999, p. 36.
39 JO L 53 de 27.2.2008, p. 52.

(79) No que diz respeito ao Liechtenstein, o presente regulamento 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, aplicação e ao desenvolvimento do acervo de Schengen[40].

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

(81) Em conformidade com a Declaração Política Conjunta dos Estados-Membros e da Comissão sobre os documentos explicativos, de 28 de setembro de 2011, os Estados-Membros assumiram o compromisso de fazer acompanhar, nos casos em que tal se justifique, a notificação das suas medidas de transposição de um ou mais documentos explicando a relação entre os componentes da diretiva e as partes correspondentes dos instrumentos de transposição nacional. Em relação à presente diretiva, o legislador considera que a transmissão desses documentos se justifica.

(82) 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, acesso, retificação, apagamento e limitação do tratamento dos seus dados pessoais no âmbito de procedimentos penais, bem como eventuais restrições desses direitos, na legislação processual penal nacional,

ADOTARAM A PRESENTE DIRETIVA:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Artigo 1.º
Objeto e objetivos

1. A presente diretiva estabelece as regras relativas à proteção das pessoas quanto ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção, repressão de infrações penais ou de execução de sanções penais.

2. Em conformidade com a presente diretiva, os Estados-Membros devem assegurar:

[40] JO L 160 de 18.6.2011, p. 19.

(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 pelas autoridades competentes da União não seja restringido nem proibido por razões relacionadas com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais.

Artigo 2.º
Âmbito de aplicação

1. A presente diretiva aplica-se ao tratamento de dados pessoais pelas autoridades competentes para os efeitos referidos 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 por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados.

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, nomeadamente no que se refere à segurança nacional;

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

Artigo 3.º
Definições

Para efeitos da presente diretiva, entende-se por:

(1) «Titular de dados», uma pessoa singular identificada ou identificável, direta ou indiretamente, por meios com razoável probabilidade de serem utilizados pelo responsável pelo tratamento ou por qualquer outra pessoa singular ou coletiva, nomeadamente por referência a um número de identificação, a dados de localização, a um identificador em linha ou a um ou mais elementos específicos próprios à sua identidade física, fisiológica, genética, psíquica, económica, cultural ou social;

(2) «Dados pessoais», qualquer informação relativa a um titular de dados;

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

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

(5) «Ficheiro», qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;

(6) «Responsável pelo tratamento», a autoridade pública competente que, por si ou em conjunto, determina as finalidades, as condições e os meios de tratamento de dados pessoais; sempre que as finalidades, as condições e os meios de tratamento sejam determinados pelo direito da União ou pela legislação dos Estados Membros, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser indicados pelo direito da União ou pela legislação de um Estado-Membro;

(7) «Subcontratante», a pessoa singular ou coletiva, a autoridade pública, serviço ou qualquer outro organismo que trata dados pessoais por conta do responsável pelo tratamento;

(8) «Destinatário», a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que receba comunicações de dados pessoais;

(9) «Violação de dados pessoais», uma violação da segurança que provoca, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação, ou o acesso, não autorizados, de dados pessoais transmitidos, conservados ou tratados de outro modo;

(10) «Dados genéticos», todos os dados, independentemente do tipo, relacionados com as características de uma pessoa singular que são hereditárias ou adquiridas numa fase precoce do seu desenvolvimento pré-natal;

(11) «Dados biométricos», quaisquer dados relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam a sua identificação única, nomeadamente imagens faciais ou dados dactiloscópicos;

(12) «Dados relativos à saúde», quaisquer informações relacionadas com a saúde física ou psíquica de uma pessoa singular, ou com a prestação de serviços de saúde a essa pessoa;

(13) «Criança», qualquer pessoa com menos de 18 anos;

(14) «Autoridades competentes», qualquer autoridade pública competente para efeitos de prevenção, investigação, deteção e repressão de infrações penais, ou de execução de sanções penais;

(15) «Autoridade de controlo», a autoridade pública instituída por um Estado-Membro nos termos do artigo 39.º.

CAPÍTULO II
PRINCÍPIOS

Artigo 4.º
Princípios relativos ao tratamento de dados pessoais

Os Estados-Membros devem prever que os dados pessoais serão:

(a) Objeto de um tratamento leal e lícito;

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

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

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

(e) Conservados de forma a permitir a identificação dos titulares de dados apenas durante o período necessário para a prossecução das finalidades para que são tratados;

(f) Tratados sob a autoridade e responsabilidade do responsável pelo tratamento, que deve assegurar a conformidade com as disposições adotadas por força da presente diretiva.

Artigo 5.º
Distinção entre diferentes categorias de titulares de dados

1. Os Estados-Membros devem prever que o responsável pelo tratamento estabeleça, 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 existam motivos fundados para crer que cometeram ou vão 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 podem vir a ser vítimas de uma infração penal;

(d) Terceiros envolvidos numa infração penal, designadamente pessoas suscetíveis de serem chamadas a testemunhar em investigações penais relacionadas com a infrações penais, ou em processos penais subsequentes, ou uma pessoa que possa fornecer informações sobre infrações penais, ou um contacto ou associado de uma das pessoas mencionadas nas alíneas a) e b); e

(e) Pessoas não abrangidas por qualquer das categorias acima referidas.

Artigo 6.º
Níveis diferentes de exatidão e de fiabilidade de dados pessoais

1. Os Estados-Membros devem assegurar que seja estabelecida uma distinção, na medida do possível, entre as diferentes categorias de dados pessoais objeto de tratamento, em função do seu nível de precisão e de fiabilidade.

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

Artigo 7.º
Licitude do tratamento

Os Estados-Membros devem prever que o tratamento de dados pessoais só é lícito se e na medida em que for necessário para:

(a) O exercício de uma função pela autoridade competente, por força da legislação, tendo em vista as finalidades enunciadas no artigo 1.º, n.º 1; ou

(b) O respeito de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; ou

(c) A proteção dos interesses vitais do titular de dados ou de um terceiro; ou

(d) A prevenção de uma ameaça grave e imediata para a segurança pública.

Artigo 8.º
Tratamento de categorias especiais de dados pessoais

1. Os Estados-Membros devem proibir o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados genéticos ou dados relativos à saúde ou à situação médica ou à orientação sexual.

2. O n.º 1 não se aplica sempre que:

   (a) O tratamento for autorizado por uma legislação que preveja garantias adequadas; ou

   (b) O tratamento for necessário para a proteção dos interesses vitais do titular de dados ou de um terceiro; ou

   (c) O tratamento estiver relacionado com dados manifestamente tornados públicos pelo seu titular.

Artigo 9.º

Medidas baseadas na definição de perfis e no tratamento automatizado

1. Os Estados-Membros devem prever a proibição de medidas que produzam efeitos adversos na esfera jurídica do titular de dados ou que o afetem de modo significativo e que se baseiem unicamente no tratamento automatizado de dados pessoais destinado a avaliar determinados aspetos próprios dessa pessoa, salvo se forem autorizadas por uma lei que preveja igualmente medidas destinadas a assegurar os interesses legítimos do titular de dados.

2. O tratamento automatizado dos dados pessoais destinado a avaliar determinados aspetos pessoais próprios ao titular de dados não se deve basear exclusivamente nas categorias especiais de dados pessoais referidas no artigo 8.º.

CAPÍTULO III

DIREITOS DO TITULAR DOS DADOS

Artigo 10.º

Modalidades de exercício dos direitos do titular dos dados

1. Os Estados-Membros devem prever que o responsável pelo tratamento adote todas as medidas razoáveis a fim de aplicar regras internas transparentes e facilmente acessíveis no que diz respeito ao tratamento de dados pessoais, tendo em vista o exercício dos direitos pelos titulares de dados.

2. Os Estados-Membros devem prever que o responsável pelo tratamento faculte todas as informações e comunicações relativas ao tratamento de dados pessoais ao titular de dados de uma forma inteligível e numa linguagem clara e simples.

3. Os Estados-Membros devem prever que o responsável pelo tratamento adote todas as medidas razoáveis para estabelecer os procedimentos de informação referidos no artigo 11.º e os procedimentos para o exercício dos direitos pelos titulares de dados referidos nos artigos 12.º a 17.º.

4. Os Estados-Membros devem prever que o responsável pelo tratamento informe, sem demora injustificada, o titular de dados do seguimento dado ao seu pedido.

5. Os Estados-Membros devem prever que as informações e eventuais medidas adotadas pelo responsável pelo tratamento na sequência de um pedido previsto nos n.os 3 e 4 sejam gratuitas. Sempre que os pedidos sejam abusivos, particularmente devido ao seu caráter repetitivo, ou à dimensão ou volume do pedido, o responsável pelo tratamento pode exigir o pagamento de uma taxa pela prestação de informações ou adoção da medida solicitada, ou pode abster-se de a adotar. Neste caso, incumbe ao responsável pelo tratamento provar o caráter abusivo do pedido.

Artigo 11.º
Informação do titular dos dados

1. Sempre que os dados pessoais de uma pessoa forem recolhidos, os Estados-Membros devem assegurar que o responsável pelo tratamento adote todas as medidas adequadas para fornecer ao titular dos dados pelo menos as seguintes informações:

   (a) Identidade e contactos do responsável pelo tratamento e do delegado para a proteção de dados;

   (b) Finalidades do tratamento a que os dados pessoais se destinam;

   (c) Período de conservação dos dados pessoais;

   (d) Existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, e a sua retificação ou apagamento, ou a limitação do seu tratamento;

   (e) Direito de apresentar uma queixa à autoridade de controlo referida no artigo 39.º, e de obter os contactos desta autoridade;

   (f) Destinatários ou categorias de destinatários dos dados pessoais, incluindo nos países terceiros ou a nível das organizações internacionais;

   (g) Quaisquer outras informações, na medida em que sejam necessárias para assegurar à pessoa em causa um tratamento leal, tendo em conta as circunstâncias específicas em que os dados pessoais são tratados.

2. Sempre que os dados pessoais tiverem sido recolhidos junto do titular de dados, o responsável pelo tratamento deve informá-lo, para além da informação referida no n.º 1, do caráter obrigatório ou facultativo de fornecer os dados pessoais, bem como das eventuais consequências de não fornecer esses dados.

3. O responsável pelo tratamento deve comunicar as informações referidas no n.º 1:

   (a) No momento da recolha dos dados pessoais junto do titular de dados; ou

   (b) Sempre que os dados não forem recolhidos junto do titular de dados, no momento do seu registo ou num prazo razoável após a recolha dos dados, tendo em conta as circunstâncias específicas em que os dados foram tratados.

4. Os Estados-Membros podem adotar medidas legislativas prevendo o adiamento, a limitação da prestação das informações, ou a sua não prestação, aos titulares de dados na medida e enquanto tal limitação, parcial ou total, constitua uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os interesses legítimos do titular de dados:

   (a) Para evitar que constituam um entrave a inquéritos, investigações, ou procedimentos oficiais ou judiciais;

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

(c) Para proteger a segurança pública;

(d) Para proteger a segurança nacional;

(e) Para proteger os direitos e as liberdades de outrem.

5. Os Estados-Membros podem determinar categorias de tratamento de dados suscetíveis de serem objeto, na sua integralidade em parte, das derrogações previstas no n.º 4.

Artigo 12.º
Direito de acesso do titular dos dados

1. Os Estados-Membros devem prever o direito de o titular de dados poder obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento. Sempre que esses dados pessoais forem objeto de tratamento, o responsável pelo tratamento deve fornecer as seguintes informações:

(a) Finalidades do tratamento;

(b) Categorias de dados pessoais envolvidos;

(c) Destinatários ou categorias de destinatários a quem os dados pessoais foram divulgados, em especial quando os destinatários estão estabelecidos em países terceiros;

(d) Período de conservação dos dados pessoais;

(e) A existência do direito de solicitar à autoridade de controlo a retificação, o apagamento ou a limitação do tratamento dos dados pessoais do titular de dados;

(f) O direito de apresentar uma queixa à autoridade de controlo e de obter os contactos desta autoridade;

(g) Comunicação dos dados pessoais em fase de tratamento e quaisquer informações disponíveis sobre a origem desses dados.

2. Os Estados-Membros devem prever o direito do titular de dados de obter do responsável pelo tratamento uma cópia dos dados pessoais em fase de tratamento.

Artigo 13.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 de dados, na medida em que tal limitação total ou parcial constitua uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os interesses legítimos do titular de dados:

(a) Para evitar que constituam um entrave a inquéritos, investigações, ou procedimentos oficiais ou judiciais;

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

(c) Para proteger a segurança pública;

(d) Para proteger a segurança nacional;

(e) Para proteger os direitos e as liberdades de outrem.

2. Os Estados-Membros podem, por via legislativa, determinar categorias de tratamento de dados suscetíveis de ser objeto, no todo ou em parte, das derrogações previstas no n.º 1.

3. Nos casos previstos nos n.os 1 e 2, os Estados-Membros devem prever que em caso de recusa ou de limitação do acesso aos dados, o responsável pelo tratamento informe o titular de dados, por escrito, dos motivos da recusa e das possibilidades de apresentar uma queixa à autoridade de controlo e de intentar uma ação judicial. Os motivos de facto ou de direito em que se baseia a decisão podem ser omitidos sempre que a sua comunicação seja suscetível de prejudicar um dos objetivos enunciados no n.º 1.

4. Os Estados-Membros devem assegurar que o responsável pelo tratamento documente os fundamentos para não comunicar os motivos de facto ou de direito em que baseou a decisão.

Artigo 14.º
Modalidades de exercício do direito de acesso

1. Os Estados-Membros devem prever o direito de o titular de dados solicitar à autoridade de controlo, em especial nos casos referidos no artigo 13.º, a verificação da licitude do tratamento.

2. O Estado-Membro deve prever que o responsável pelo tratamento informe o titular de dados do seu direito de solicitar a intervenção da autoridade de controlo por força do n.º 1.

3. Sempre que o direito a que se refere o n.º 1 for exercido, a autoridade de controlo deve informar o titular de dados, pelo menos, de que foram realizadas todas as verificações necessárias que incumbem à referida autoridade e do resultado quanto à licitude do tratamento em causa.

Artigo 15.º
Direito de retificação

1. Os Estados-Membros devem prever o direito de o titular de dados obter do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. O titular de dados tem o direito de obter, nomeadamente através de uma declaração retificativa, que os seus dados pessoais incompletos sejam completados.

2. Os Estados-Membros devem prever que, em caso de recusa de ratificação dos dados, o responsável pelo tratamento informe o titular de dados, por escrito, dos motivos da recusa e das possibilidades de apresentar uma queixa à autoridade de controlo e de intentar uma ação judicial.

Artigo 16.º
Direito de apagamento

1. Os Estados-Membros devem prever o direito de o titular de dados obter do responsável pelo tratamento o apagamento dos dados pessoais que lhe digam respeito sempre que o tratamento não seja conforme com as disposições adotadas nos termos do artigo 4.º, alínea a) a e), e dos artigos 7.º e 8.º, da presente diretiva.

2. O responsável pelo tratamento deve efetuar esse apagamento sem demora.

3. Em vez de proceder ao apagamento, o responsável pelo tratamento deve marcar os dados pessoais sempre que:

   (a) A sua exatidão for contestada pelo titular dos dados, durante um período que permita ao responsável pelo tratamento verificar a exatidão dos dados;

   (b) Os dados pessoais devam ser conservados para efeitos de prova;

   (c) O titular dos dados se opuser ao seu apagamento e solicitar, em contrapartida, a limitação da sua utilização;

4. Os Estados-Membros devem prever que o responsável pelo tratamento informe o titular de dados, por escrito, de qualquer recusa de apagamento ou de marcação dos dados tratados, dos motivos de recusa e das possibilidades de apresentar uma queixa à autoridade de controlo e de intentar uma ação judicial.

Artigo 17.º
Direitos do titular dos dados no âmbito de investigações e ações penais

Os Estados-Membros podem prever, sempre que dados pessoais constem de uma decisão ou de um registo criminal objeto de tratamento no âmbito de uma investigação ou ação penal, que os direitos de informação, acesso, retificação, apagamento e limitação do tratamento, previstos nos artigos 11.º a 16.º, sejam exercidos em conformidade com as regras processuais penais nacionais.

CAPÍTULO IV
RESPONSÁVEL PELO TRATAMENTO E SUBCONTRATANTE

SECÇÃO 1
OBRIGAÇÕES GERAIS

Artigo 18.º
Obrigações do responsável pelo tratamento

1. Os Estados-Membros devem prever que o responsável pelo tratamento adote regras internas e execute as medidas adequadas para assegurar que o tratamento dos dados pessoais é realizado no respeito das disposições adotadas em conformidade com a presente diretiva.

2. As medidas referidas no n.º 1 devem incluir, nomeadamente:

   (a) Conservar a documentação, nos termos do artigo 23.º;

   (b) Respeitar a obrigação de consulta prévia, nos termos do artigo 26.º;

   (c) Aplicar os requisitos de segurança previstos no artigo 27.º;

   (d) Designar um delegado para a proteção de dados, nos termos do artigo 30.º.

3. O responsável pelo tratamento deve aplicar mecanismos de verificação da eficácia das medidas referidas no n.º 1. Sob reserva da sua proporcionalidade, essa verificação deve ser realizada por auditores independentes internos ou externos.

Artigo 19.º
Proteção de dados desde a conceção e por defeito

1. Os Estados-Membros devem prever que, tendo em conta as técnicas mais recentes e os custos associados à sua aplicação, o responsável pelo tratamento aplique as medidas e procedimentos técnicos e organizativos adequados, a fim de que o tratamento respeite as disposições adotadas em conformidade com a presente diretiva e garanta a proteção dos direitos do titular de dados.

2. O responsável pelo tratamento deve aplicar mecanismos que garantam, por defeito, que apenas são tratados os dados pessoais necessários para as finalidades do tratamento.

Artigo 20.º
Responsáveis conjuntos pelo tratamento

Os Estados-Membros devem prever, sempre que um responsável pelo tratamento definir, em conjunto com outros, as finalidades, as condições e os meios do tratamento de dados pessoais, os responsáveis conjuntos pelo tratamento devem definir, por acordo, as respetivas obrigações, a fim de respeitarem as disposições adotadas em conformidade com a presente

diretiva, nomeadamente no que diz respeito aos procedimentos e mecanismos que regulam o exercício de direitos do titular de dados.

Artigo 21.º
Subcontratante

1. Os Estados-Membros devem prever que o responsável pelo tratamento, em caso de tratamento por sua conta, escolha um subcontratante que apresente garantias suficientes de execução das medidas e procedimentos técnicos e organizativos apropriados, de forma a que esse tratamento respeite as disposições adotadas em conformidade com a presente diretiva e garanta a proteção dos direitos do titular de dados.

2. Os Estados-Membros devem prever que a realização de operações de tratamento por um subcontratante sejam reguladas por um ato jurídico que vincule o subcontratante ao responsável pelo tratamento e que preveja, nomeadamente, que o subcontratante atue apenas mediante instruções do responsável pelo tratamento, em especial quando a transferência de dados pessoais utilizados for proibida.

3. Se um subcontratante proceder ao tratamento de dados pessoais de forma diferente da que foi definida nas instruções do responsável pelo tratamento, o subcontratante é considerado responsável pelo tratamento em relação ao referido tratamento, ficando sujeito às disposições aplicáveis aos responsáveis conjuntos pelo tratamento previstas no artigo 20.º.

Artigo 22.º
Tratamento sob a autoridade do responsável pelo tratamento e do subcontratante

Os Estados-Membros devem prever que o subcontratante, bem como qualquer pessoa, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, que tenha acesso a dados pessoais, só pode efetuar o seu tratamento mediante instruções do responsável pelo tratamento ou se exigido pela legislação da União ou de um Estado-Membro.

Artigo 23.º
Documentação

1. Os Estados-Membros devem prever que cada responsável pelo tratamento e cada subcontratante, mantenha a documentação de todos os sistemas e procedimentos de tratamento sob a sua responsabilidade.

2. Essa documentação deve consistir, pelo menos, nas seguintes informações:

   (a) Nome e contactos do responsável pelo tratamento, ou de qualquer responsável conjunto pelo tratamento ou subcontratante;

   (b) Finalidades do tratamento;

   (c) Destinatários ou categorias de destinatários dos dados pessoais;

(d) Transferências de dados para um país terceiro ou uma organização internacional, incluindo o nome desse país terceiro ou dessa organização internacional.

3. O responsável pelo tratamento e o subcontratante devem disponibilizar a documentação existente à autoridade de controlo, quando por esta solicitado.

Artigo 24.º
Conservação de registos das operações de tratamento

1. Os Estados-Membros devem assegurar que são conservados registos de, pelo menos, as seguintes operações: recolha, alteração, consulta, comunicação, interconexão ou apagamento. Os registos das operações de consulta e de comunicação indicarão, em especial, a finalidade, a data e hora dessas operações e, na medida do possível, a identificação da pessoa que consultou ou comunicou dados pessoais.

2. Os registos só podem ser utilizados para efeitos de verificação da licitude do tratamento de dados, de autocontrolo e de garantia da integridade e segurança dos dados.

Artigo 25.º
Cooperação com a autoridade de controlo

1. Os Estados-Membros devem prever que o responsável pelo tratamento e o subcontratante cooperem, mediante pedido, com a autoridade de controlo no exercício das suas funções, comunicando nomeadamente todas as informações de que esta necessite para esse efeito.

2. Sempre que autoridade de controlo exerça os poderes que lhe são conferidos por força do artigo 46.º, alíneas a) e b), o responsável pelo tratamento e o subcontratante devem responder à autoridade de controlo num prazo razoável a fixar por esta última. A resposta deve incluir uma descrição das medidas adotadas e dos resultados obtidos, tendo em conta as observações formuladas pela autoridade de controlo.

Artigo 26.º
Consulta prévia da autoridade de controlo

1. Os Estados-Membros devem assegurar que o responsável pelo tratamento ou o subcontratante consulta a autoridade de controlo antes de proceder ao tratamento de dados pessoais que farão parte de um novo ficheiro a criar, sempre que:

(a) O tratamento visar categorias especiais de dados referidas no artigo 8.º;

(b) Devido à utilização, em especial, de novos mecanismos, tecnologias ou procedimentos, o tipo de tratamento apresente riscos específicos para os direitos e liberdades fundamentais e, em particular, para a proteção de dados pessoais do seu titular.

2. Os Estados-Membros podem prever que a autoridade de controlo estabeleça uma lista das operações de tratamento de dados sujeitas a consulta prévia nos termos do n.º 1.

SECÇÃO 2
SEGURANÇA DOS DADOS

Artigo 27.º
Segurança do tratamento

1. Os Estados-Membros devem prever que o responsável pelo tratamento e o subcontratante apliquem as medidas técnicas e organizativas necessárias para assegurar um nível de segurança adaptado aos riscos que o tratamento representa e à natureza dos dados pessoais a proteger, atendendo às técnicas mais recentes e aos custos resultantes da sua aplicação.

2. No que respeita ao tratamento automatizado de dados, cada Estado-Membro deve prever que o responsável pelo tratamento ou o subcontratante, na sequência de uma avaliação de riscos, aplique medidas destinadas a:

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

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

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

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

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

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

   (g) Assegurar que possa ser verificado e estabelecido *a posteriori* quais foram os dados pessoais introduzidos nos sistemas de tratamento automatizado de dados, 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 possam ser lidos, copiados, alterados ou suprimidos de forma não autorizada (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).

3. A Comissão pode adotar, se necessário, atos de execução a fim de especificar os requisitos previstos nos n.os 1 e 2 aplicáveis às várias situações, particularmente normas de cifragem. Esses atos de execução são adotados em conformidade com o procedimento de exame previsto no artigo 57.º, n.º 2.

Artigo 28.º

Notificação da violação de dados pessoais à autoridade de controlo

1. Os Estados-Membros devem prever 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, o mais tardar 24 horas após ter tido conhecimento da mesma. Caso a notificação seja transmitida após esse prazo, o responsável pelo tratamento deve apresentar uma justificação à autoridade de controlo, a pedido desta.

2. O subcontratante deve alertar e informar o responsável pelo tratamento imediatamente após ter conhecimento de uma violação de dados pessoais.

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

(a) Descrever a natureza de violação dos dados pessoais, incluindo as categorias e o número de titulares de dados afetados, bem como as categorias e o número de registos de dados em causa;

(b) Comunicar a identidade e os contactos do delegado para a proteção de dados referido no artigo 30.°, ou de outro ponto de contacto onde possam ser obtidas informações adicionais;

(c) Recomendar medidas destinadas a atenuar os eventuais efeitos adversos da violação de dados pessoais;

(d) Descrever as consequências eventuais da violação de dados pessoais;

(e) Descrever as medidas propostas ou adotadas pelo responsável pelo tratamento para remediar a violação de dados pessoais.

4. Os Estados-Membros devem prever que o responsável pelo tratamento conserve documentação sobre qualquer violação de dados pessoais, incluindo os factos relacionados com a mesma, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controlo verificar o respeito do disposto no presente artigo. A documentação deve incluir apenas as informações necessárias para esse efeito.

5. São conferidas competências à Comissão para adotar atos delegados nos termos do artigo 56.º, a fim de especificar mais concretamente os critérios e requisitos aplicáveis à determinação da violação de dados referida nos n.os 1 e 2, e às circunstâncias particulares em que um responsável pelo tratamento e um subcontratante são obrigados a notificar a violação de dados pessoais.

6. A Comissão pode definir um formato normalizado para essa notificação à autoridade de controlo, os procedimentos aplicáveis ao requisito de notificação, bem como o formulário e as modalidades para a documentação referida no n.º 4, incluindo os prazos para o apagamento das informações aí contidas. Os atos de execução correspondentes são adotados em conformidade com o procedimento de exame referido no artigo 57.º, n.º 2.

Artigo 29.º
Comunicação de uma violação de dados pessoais ao titular dos dados

1. Os Estados-Membros devem prever que, sempre que a violação de dados pessoais for suscetível de afetar negativamente a proteção dos dados pessoais ou a privacidade do titular dos dados, o responsável pelo tratamento, após a notificação a que se refere o artigo 28.º, comunica a violação de dados pessoais à pessoa em causa sem demora injustificada.

2. A comunicação ao titular dos dados referida no n.º 1 deve descrever a natureza da violação dos dados pessoais e incluir, pelo menos, as informações e recomendações previstas no artigo 28.º, n.º 3, alíneas b) e c).

3. A comunicação de uma violação de dados pessoais ao seu titular não deve ser exigida se o responsável pelo tratamento demonstrar cabalmente, a contento da autoridade competente, que adotou as medidas de proteção tecnológica adequadas e que estas foram aplicadas aos dados a que a violação diz respeito. Essas medidas de proteção tecnológica devem tornar os dados incompreensíveis para qualquer pessoa que não esteja autorizada a aceder a esses dados.

4. A comunicação ao titular dos dados pode ser adiada, limitada ou omitida pelos motivos referidos no artigo 11.º, n.º 4.

SECÇÃO 3
DELEGADO PARA A PROTEÇÃO DE DADOS

Artigo 30.º
Designação do delegado para a proteção de dados

1. Os Estados-Membros devem prever que o responsável pelo tratamento ou o subcontratante designem um delegado para a proteção de dados.

2. O delegado para a proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio da legislação e das práticas a nível da proteção de dados, e na sua capacidade para cumprir as funções referidas no artigo 32.º.

3. O delegado para a proteção de dados pode ser designado para várias entidades, tendo em conta a estrutura organizativa da autoridade competente.

Artigo 31.º
Função do delegado para a proteção de dados

1. Os Estados-Membros devem prever que o responsável pelo tratamento ou o subcontratante assegure que o delegado para a proteção de dados seja associado, de forma adequada e em tempo útil, a todas as matérias relacionadas com a proteção de dados pessoais.

2. O responsável pelo tratamento ou o subcontratante deve assegurar que o delegado para a proteção de dados dispõe dos meios para desempenhar as suas funções e atribuições referidas no artigo 32.º, de forma eficaz e independente, e que não recebe quaisquer instruções relativas ao exercício da sua função.

Artigo 32.º
Atribuições do delegado para a proteção de dados

Os Estados-Membros devem prever que o responsável pelo tratamento ou o subcontratante confie ao delegado para a proteção de dados, pelo menos, as seguintes atribuições:

(a) Informar e aconselhar o responsável pelo tratamento ou o subcontratante sobre as suas obrigações em aplicação das disposições adotadas em conformidade com a presente diretiva, e conservar documentação sobre esta atividade e as respostas recebidas;

(b) Controlar a execução e a aplicação das regras internas em matéria de proteção de dados, incluindo a repartição das responsabilidades, a formação do pessoal que participa nas operações de tratamento e nas auditorias correspondentes;

(c) Controlar a execução e a aplicação das disposições adotadas em conformidade com a presente diretiva, em especial quanto aos requisitos relacionados com a proteção de dados desde a conceção, a proteção de dados por defeito e a segurança de dados, bem como às informações dos titulares dos dados e exame dos pedidos para exercer os seus direitos ao abrigo das disposições adotadas em conformidade com a presente diretiva;

(d) Assegurar que a documentação referida no artigo 23.º é conservada;

(e) Acompanhar a documentação, a notificação e a comunicação relativas a violações de dados pessoais, nos termos dos artigos 28.º e 29.º;

(f) Verificar se os pedidos de consulta prévia foram apresentados à autoridade de controlo, caso esta seja necessária nos termos do artigo 26.º;

(g) Acompanhar a resposta aos pedidos da autoridade de controlo e, no âmbito da competência do delegado para a proteção de dados, cooperar com a autoridade de controlo, a pedido desta ou por iniciativa do próprio delegado para a proteção de dados;

(h) Atuar como ponto de contacto para a autoridade de controlo sobre assuntos relacionados com o tratamento, e consultar esta autoridade, se for caso disso, por sua própria iniciativa.

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

Artigo 33.º
Princípios gerais das transferências de dados pessoais

Os Estados-Membros devem prever que qualquer transferência, pelas autoridades competentes, de dados pessoais objeto de tratamento ou que se destinem a ser tratadas após a sua transferência para um país terceiro, ou para uma organização internacional, incluindo uma transferência ulterior para outro país terceiro ou outra organização internacional, só pode ser efetuada se:

(a) A transferência for necessária para fins de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais; e

(b) As condições estabelecidas no presente capítulo forem cumpridas pelo responsável pelo tratamento e pelo subcontratante.

Artigo 34.º
Transferências acompanhadas de uma decisão de adequação

1. Os Estados-Membros devem prever que uma transferência de dados pessoais para um país terceiro ou uma organização internacional pode ser efetuada sempre que a Comissão tiver declarado, mediante decisão, em conformidade com o artigo 41.º do Regulamento (UE) …./2012, ou em conformidade com o n.º 3 deste artigo, que o país terceiro, um território ou um setor de tratamento nesse país terceiro, ou a organização internacional em causa, garante um nível de proteção adequado. Essa transferência não exige qualquer autorização suplementar.

2. Na falta de uma decisão adotada por força do artigo 41.º do Regulamento (UE) …./2012, a Comissão deve avaliar a adequação do nível de proteção tendo em conta os seguintes elementos:

(a) O primado do Estado de direito, a legislação relevante em vigor, geral ou setorial, incluindo no que respeita à segurança pública, à defesa, à segurança nacional e ao direito penal, e às medidas de segurança que são respeitadas nesse país ou por essa organização internacional, bem como a existência de direitos efetivos e oponíveis, incluindo vias de recurso administrativo e judicial para os titulares de dados, nomeadamente para as pessoas residentes na União 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 na organização internacional em causa, responsáveis por assegurar o respeito das regras de proteção de dados, assistir e

aconselhar o titular de dados no exercício dos seus direitos, e cooperar com as autoridades de controlo da União e dos Estados-Membros; e

(c) Os compromissos internacionais assumidos pelo país terceiro ou a organização internacional.

3. A Comissão pode decidir, nos limites da presente diretiva, que um país terceiro, um território, ou um setor de tratamento dentro desse país terceiro, ou uma organização internacional, garante um nível de proteção adequado na aceção do n.º 2. Os atos de execução correspondentes são adotados em conformidade com o procedimento de exame referido no artigo 57.º, n.º 2.

4. O ato de execução deve especificar o âmbito de aplicação geográfico e setorial e, se for caso disso, identificar a autoridade de controlo referida no n.º 2, alínea b).

5. A Comissão pode decidir, nos limites da presente diretiva, que um país terceiro, um território ou um setor de tratamento nesse país terceiro, ou uma organização internacional, não assegura um nível de proteção adequado na aceção do n.º 2, em especial nos casos em que a legislação relevante, quer de caráter geral ou setorial, em vigor no país terceiro ou na organização internacional, não assegura direitos efetivos e oponíveis, incluindo vias de recurso administrativo e judicial para os titulares de dados, nomeadamente para as pessoas residentes no território da União cujos dados pessoais sejam objeto de transferência. Os atos de execução correspondentes são adotados em conformidade com o procedimento de exame referido no artigo 57.º, n.º 2, ou, em casos de extrema urgência para as pessoas singulares no que se refere ao seu direito de proteção de dados pessoais, em conformidade com o procedimento referido no artigo 57.º, n.º 3.

6. Os Estados-Membros devem assegurar que, sempre que a Comissão adote uma decisão por força do n.º 5, segundo a qual qualquer transferência de dados pessoais para o país terceiro, um território ou um setor de tratamento nesse país terceiro, ou organização internacional em causa é proibida, tal decisão não prejudique transferências efetuadas nos termos do artigo 35.º, n.º 1, ou em conformidade com o artigo 36.º. Em momento oportuno, a Comissão deve encetar negociações com o país terceiro ou a organização internacional com vista a remediar a situação resultante da decisão adotada nos termos do n.º 5.

7. A Comissão publica no *Jornal Oficial da União Europeia* uma lista dos países terceiros, territórios e setores de tratamento num país terceiro e de organizações internacionais relativamente aos quais tenha declarado, mediante decisão, que asseguram ou não um nível de proteção adequado.

8. A Comissão deve acompanhar a aplicação dos atos de execução referidos nos n.ºs 3 e 5.

Artigo 35.º
Transferências mediante garantias adequadas

1. Sempre que a Comissão não tenha tomado qualquer decisão nos termos do artigo 34.º, os Estados-Membros devem prever que uma transferência de dados pessoais para um país terceiro uma organização internacional só pode ser efetuada:

(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 ou o subcontratante tiver avaliado todas as circunstâncias inerentes à operação de transferência de dados pessoais e concluir existirem garantias adequadas relativamente à proteção de dados pessoais.

1. A decisão de transferência nos termos do n.º 1, alínea b), deve ser adotada por pessoal devidamente autorizado. Qualquer transferência desse tipo deve fundamentada mediante documentação, que deve ser disponibilizada à autoridade de controlo, se solicitada.

Artigo 36.º
Derrogações

Em derrogação aos artigos 34.º e 35.º, os Estados-Membros devem prever que uma transferência de dados pessoais para um país terceiro ou uma organização internacional só pode ser efetuada:

(a) Se for necessária para proteger os interesses vitais do titular dos dados ou de outra pessoa; ou

(b) Se for necessária para proteger os interesses legítimos do titular dos dados sempre que a legislação do Estado-Membro que transfere os dados pessoais o preveja; ou

(c) Se for essencial para a prevenção de uma ameaça imediata e grave contra a segurança pública de um Estado-Membro ou de um país terceiro; ou

(d) Se for necessária em casos particulares para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais; ou

(e) Se for necessária em casos particulares tendo em vista a confirmação, exercício ou defesa de um direito no âmbito de um processo judicial relacionado com a prevenção, investigação, deteção ou repressão de uma infração penal específica ou a execução de uma sanção penal específica.

Artigo 37.º
Condições específicas aplicáveis à transferência de dados pessoais

Os Estados-Membros devem prever que o responsável pelo tratamento informe o destinatário dos dados pessoais de qualquer limitação do tratamento e que adote todas as medidas razoáveis a fim de assegurar que tais limitações sejam respeitadas.

Artigo 38.º

Cooperação internacional no domínio da proteção de dados pessoais

1. Em relação a países terceiros e a organizações internacionais, a Comissão e os Estados-Membros devem adotar as medidas necessárias para:

   (a) Elaborar mecanismos de cooperação internacionais eficazes visando facilitar a aplicação da legislação relativa à proteção de dados pessoais;

   (b) Prestar assistência mútua a nível internacional no domínio da aplicação da legislação de proteção de dados pessoais, incluindo através da notificação, transmissão das queixas, 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 relevantes nas discussões e atividades com vista à promoção da cooperação internacional na 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.

2. Para efeitos da aplicação do n.º 1, a Comissão deve adotar as medidas necessárias para intensificar as relações com os países terceiros ou as organizações internacionais e, em especial, as suas autoridades de controlo, sempre que a Comissão tiver declarado, mediante decisão, que asseguram um nível de proteção adequado na aceção do artigo 34.º, n.º 3.

CAPÍTULO VI
AUTORIDADES DE CONTROLO INDEPENDENTES

SECÇÃO 1
ESTATUTO INDEPENDENTE

Artigo 39.º

Autoridade de controlo

1. Cada Estado-Membro deve prever que uma ou mais autoridades públicas sejam responsáveis pela fiscalização da aplicação das disposições adotadas nos termos da presente diretiva e por contribuir para a sua aplicação coerente no conjunto da União, a fim de proteger os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento dos seus dados pessoais e facilitar a livre circulação desses dados na União. Para esse efeito, as autoridades de controlo devem cooperar entre si e com a Comissão.

2. Os Estados-Membros podem prever que a autoridade de controlo instituída nos Estados-Membros em conformidade com o Regulamento (EU)…./2012 assuma as funções de autoridade de controlo a definir nos termos do n.º 1 do presente artigo.

3. Sempre que um Estado-Membro institui várias autoridades de controlo, deve designar aquela que funciona como ponto de contacto único tendo em vista uma participação efetiva dessas autoridades no Comité Europeu para a Proteção de Dados.

Artigo 40.º
Independência

1. Os Estados-Membros devem assegurar que a autoridade de controlo exerça com total independência as funções e poderes que lhe forem atribuídos.

2. Cada Estado-Membro deve prever que os membros da autoridade de controlo, no exercício das suas funções, não solicitam nem recebem instruções de outrem.

3. Os membros da autoridade de controlo devem abster-se de praticar qualquer ato incompatível com as suas funções e, durante o seu mandato, não podem desempenhar qualquer atividade profissional, remunerada ou não.

4. Após cessarem as suas funções, os membros da autoridade de controlo devem agir com integridade e discrição relativamente à aceitação de determinadas funções e benefícios.

5. Cada Estado-Membro deve assegurar que a autoridade de controlo dispõe de recursos humanos, técnicos e financeiros apropriados, bem como de instalações e infraestruturas, necessários à execução eficaz das suas funções e poderes, incluindo os executados no contexto da assistência mútua, cooperação e participação ativa no Comité Europeu para a Proteção de Dados.

6 Cada Estado-Membro deve assegurar que a autoridade de controlo dispõe do seu próprio pessoal, que é designado pelo diretor da autoridade de controlo e está sujeito às suas ordens.

7. Os Estados-Membros devem assegurar que a autoridade de controlo fica sujeita a um controlo financeiro que não afete a sua independência. Os Estados-Membros garantem que a autoridade de controlo disponha de orçamentos anuais próprios. Os orçamentos serão objeto de publicação.

Artigo 41.º
Condições gerais aplicáveis aos membros da autoridade de controlo

1. Os Estados-Membros devem prever que os membros da autoridade de controlo sejam nomeados pelos respetivos parlamentos ou governos.

2. Os membros são escolhidos de entre pessoas que ofereçam todas as garantias de independência e cuja experiência e conhecimentos técnicos necessários para o exercício das suas funções seja comprovada.

3. As funções de um membro cessam findo o termo do seu mandato, demissão ou destituição, nos termos do n.º 5.

4. Um membro pode ser declarado demissionário ou privado do seu direito à pensão ou a outros benefícios equivalentes por decisão de um tribunal nacional competente se deixar de preencher os requisitos necessários ao exercício das suas funções ou tiver cometido uma falta grave.

5. Um membro cujo mandato termine ou que se demita deve continuar a exercer as suas funções até à nomeação de um novo membro.

Artigo 42.º
Regras relativas à constituição da autoridade de controlo

Cada Estado-Membro deve prever, por via legislativa:

(a) A constituição e o estatuto da autoridade de controlo, nos termos dos artigos 39.º e 40.º;

(b) As qualificações, a experiência e as competências para o exercício das funções de membro da autoridade de controlo;

(c) As regras e os procedimentos para a nomeação dos membros da autoridade de controlo, bem como as regras relativas a ações ou atividades profissionais incompatíveis com a função;

(d) A duração do mandato dos membros da autoridade de controlo, que não pode ser inferior a quatro anos, salvo no que se refere ao primeiro mandato após a entrada em vigor da presente diretiva, que pode ter uma duração mais curta;

(e) O caráter renovável ou não do mandato dos membros da autoridade de controlo;

(f) O estatuto e as condições comuns que regulam as funções dos membros e do pessoal da autoridade de controlo;

(g) As regras e os procedimentos relativos à cessação das funções dos membros da autoridade de controlo, incluindo quando deixem de preencher os requisitos necessários ao exercício das suas funções ou se tiverem cometido uma falta grave.

Artigo 43.º
Sigilo profissional

Os Estados-Membros devem prever que os membros e o pessoal da autoridade de controlo ficam sujeitos, durante o respetivo mandato e após a sua cessação, à obrigação de sigilo profissional quanto a quaisquer informações confidenciais a que tenham tido acesso no desempenho das suas funções oficiais.

SECÇÃO 2
FUNÇÕES E PODERES

Artigo 44.º
Competência

1. Os Estados-Membros devem prever que cada autoridade de controlo exerce, no território do seu Estado-Membro, os poderes que lhe são conferidos em conformidade com a presente diretiva.

2. Os Estados-Membros devem prever que a autoridade de controlo não tem competência para controlar operações de tratamento efetuadas por tribunais que atuem no exercício da sua função jurisdicional.

Artigo 45.º
Funções

1. Os Estados-Membros devem prever que incumbe à autoridade de controlo:

   (a) Controlar e assegurar a aplicação das disposições adotadas em conformidade com a presente diretiva e das suas medidas de execução;

   (b) Receber as queixas apresentadas por qualquer titular de dados ou por uma associação que o represente nos termos do artigo 50.º, examinar a matéria, na medida do necessário, e informar a pessoa em causa ou a associação do andamento e do resultado da queixa num prazo razoável, em especial se forem necessárias operações de investigação ou de coordenação complementares com outra autoridade de controlo;

   (c) Verificar a licitude do tratamento dos dados nos termos do artigo 14.º, e informar o titular de dados num período razoável do resultado da verificação ou dos motivos que impediram a sua realização;

   (d) Prestar assistência mútua a outras autoridades de controlo e assegurar a coerência da aplicação e execução das disposições adotadas nos termos da presente diretiva;

   (e) Conduzir investigações, por sua própria iniciativa ou com base numa queixa ou a pedido de outra autoridade de controlo, e informar o titular dos dados, num prazo razoável, do resultado das operações de investigação;

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

   (g) Ser consultada pelas instituições e organismos do Estado-Membro quanto a medidas legislativas e administrativas relacionadas com a proteção dos direitos e liberdades no que diz respeito ao tratamento de dados pessoais;

(h) Ser consultada sobre as operações de tratamento nos termos do artigo 26.º;

(i) Participar nas atividades do Comité Europeu para a Proteção de Dados.

2. Cada autoridade de controlo deve promover a sensibilização do público sobre os riscos, regras, garantias, e direitos associados ao tratamento de dados pessoais. As atividades especificamente dedicadas às crianças devem ser objeto de uma atenção especial.

3. A autoridade de controlo deve, a pedido, aconselhar qualquer titular de dados sobre o exercício dos seus direitos decorrentes da presente diretiva e, se for caso disso, coopera com as autoridades de controlo de outros Estados-Membros para esse efeito.

4. No que respeita às queixas referidas no n.º 1, alínea b), a autoridade de controlo deve fornecer um formulário de queixa, que possa ser preenchido eletronicamente, sem excluir outros meios de comunicação.

5. Os Estados-Membros devem prever que o desempenho das funções da autoridade de controlo é gratuito para o titular dos dados.

6. Sempre que os pedidos sejam manifestamente abusivos, particularmente devido ao seu caráter repetitivo, a autoridade de controlo pode exigir o pagamento de uma taxa, ou não adotar as medidas solicitadas pelo titular dos dados. Incumbe à autoridade de controlo o ónus de provar o caráter manifestamente abusivo do pedido.

Artigo 46.º
Poderes

Os Estados-Membros devem prever que cada autoridade de controlo esteja habilitada a exercer os seguintes poderes:

(a) Poder de investigação, nomeadamente aceder aos dados objeto de tratamento e recolher todas as informações necessárias ao desempenho das suas funções de controlo;

(b) Poder efetivo de intervenção, nomeadamente emitir pareceres previamente ao tratamento de dados e assegurar a publicação adequada desses pareceres, ordenar a limitação, o apagamento ou a destruição dos dados, proibir temporária ou definitivamente um tratamento, dirigir uma advertência ou uma admoestação ao responsável pelo tratamento ou remeter a questão para os parlamentos nacionais ou para outras instituições políticas;

(c) Poder de intervir em processos judiciais em caso de violação das disposições nacionais adotadas em aplicação da presente diretiva ou de levar essa violação ao conhecimento das autoridades judiciais.

Artigo 47.º
Relatório de atividades

Os Estados-Membros devem prever que cada autoridade de controlo elabore um relatório anual de atividades. O relatório é disponibilizado à Comissão e ao Comité Europeu para a Proteção de Dados.

CAPÍTULO VII
COOPERAÇÃO

Artigo 48.º
Assistência mútua

1. Os Estados-Membros devem prever que as autoridades de controlo prestem entre si assistência mútua, a fim de executar e aplicar de forma coerente as disposições adotadas em conformidade com a presente diretiva, e que ponham em prática medidas para cooperar eficazmente entre si. A assistência mútua deve cobrir, em especial, pedidos de informação e de medidas de controlo, tais como pedidos de consulta prévia, de inspeção e de investigação.

2. Os Estados-Membros devem prever que a autoridade de controlo adote todas as medidas adequadas necessárias para satisfazer o pedido de outra autoridade de controlo.

3. A autoridade de controlo requerida deve informar a autoridade de controlo requerente dos resultados obtidos ou, consoante o caso, do andamento do dossiê ou das medidas adotadas para satisfazer o pedido da autoridade de controlo requerente.

Artigo 49.º
Atribuições do Comité Europeu para a Proteção de Dados

1. O Comité Europeu para a Proteção de Dados, instituído pelo Regulamento (UE)…./2012, exerce as seguintes atribuições no que diz respeito ao tratamento de dados no âmbito de aplicação da presente diretiva:

   (a) Aconselhar a Comissão sobre qualquer questão relacionada com a proteção de dados pessoais na UE, nomeadamente sobre qualquer projeto de alteração da presente diretiva;

   (b) Analisar, a pedido da Comissão ou por sua própria iniciativa ou por iniciativa de um dos seus membros, qualquer questão relativa à aplicação das disposições adotadas nos termos da presente diretiva e emitir diretrizes, recomendações e boas práticas destinadas às autoridades de controlo, a fim de incentivar a aplicação coerente dessas disposições;

   (c) Examinar a aplicação prática das diretrizes, recomendações e boas práticas referidas na alínea b) e informar regularmente a Comissão sobre esta matéria;

   (d) Comunicar à Comissão um parecer sobre a o nível de proteção assegurado por países terceiros ou por organizações internacionais;

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

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

(g) Promover o intercâmbio de conhecimentos e de documentação em relação a práticas e legislação no domínio da proteção de dados com autoridades de controlo de todos os países.

2. Sempre que a Comissão consultar o Comité Europeu para a Proteção de Dados, pode fixar um prazo para a formulação do referido parecer, tendo em conta a urgência da questão.

3. O Comité Europeu para a Proteção de Dados transmite os seus pareceres, diretrizes e boas práticas à Comissão e ao comité referido no artigo 57.º, n.º 1, e procede à sua publicação.

4. A Comissão informa o Comité Europeu para a Proteção de Dados das medidas adotadas em sequência de pareceres, diretrizes, recomendações e boas práticas, emitidos pelo referido comité.

CAPÍTULO VIII
VIAS DE RECURSO, RESPONSABILIDADE E SANÇÕES

Artigo 50.º
Direito de apresentar uma queixa a uma autoridade de controlo

1. Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, os Estados-Membros devem prever que qualquer titular de dados tem o direito de apresentar queixa a uma autoridade de controlo em qualquer Estado-Membro se considerar que o tratamento dos seus dados pessoais não respeita as disposições adotadas nos termos da presente diretiva.

2. Os Estados-Membros devem prever que qualquer organismo, organização ou associação que vise proteger os direitos e interesses dos titulares de dados em relação à proteção dos seus dados pessoais e que esteja devidamente constituído ao abrigo do direito de um Estado-Membro, tem o direito de apresentar queixa a uma autoridade de controlo em qualquer Estado-Membro por conta de uma ou mais pessoas em causa, se considerar que os direitos de que beneficia um titular de dados por força da presente diretiva foram violados na sequência do tratamento dos seus dados pessoais. A organização ou associação tem de ser devidamente mandatada pelo(s) titular(es) de dados.

3. Os Estados-Membros devem prever que qualquer organismo, organização ou associação referidos no n.º 2, independentemente de uma queixa do titular dos dados, pode apresentar uma queixa a uma autoridade de controlo em qualquer Estado-Membro, se considerar ter havido uma violação de dados pessoais.

Artigo 51.º

Direito de ação judicial contra uma autoridade de controlo

1. Os Estados-Membros devem prever o direito de ação judicial contra as decisões de uma autoridade de controlo.

2. Qualquer titular de dados tem o direito de ação judicial a fim de obrigar a autoridade de controlo a dar seguimento a uma queixa, na falta de uma decisão necessária para proteger os seus direitos, ou se a autoridade de controlo não informar a pessoa em causa, no prazo de três meses, sobre o andamento ou o resultado da sua queixa nos termos do artigo 45.º, n.º 1.

3. Os Estados-Membros devem prever que as ações contra uma autoridade de controlo são intentadas nos tribunais do Estado-Membro no território do qual se encontra estabelecida a autoridade de controlo.

Artigo 52.º

Direito de ação judicial contra um responsável pelo tratamento ou um subcontratante

Os Estados-Membros devem prever que, sem prejuízo de um eventual recurso administrativo disponível, nomeadamente o direito de apresentar queixa a uma autoridade de controlo, qualquer pessoa singular tem o direito de ação judicial se considerar ter havido violação dos direitos que lhe confere a presente diretiva, na sequência do tratamento dos seus dados pessoais efetuado em violação das disposições da referida diretiva.

Artigo 53.º

Regras comuns aplicáveis aos processos judiciais

1. Os Estados-Membros devem prever que qualquer organismo, organização ou associação referido no artigo 50.º, n.º 2, pode exercer os direitos referidos nos artigos 51.º e 52.º, por conta de um ou mais titulares de dados.

2. Cada autoridade de controlo pode intervir em processos judiciais e intentar uma ação em tribunal a fim de fazer respeitar as disposições adotadas em conformidade com a presente diretiva ou assegurar a coerência da proteção de dados pessoais na União.

3. Os Estados-Membros devem assegurar que quaisquer vias judiciais disponíveis no direito nacional permitam a adoção rápida de medidas, incluindo medidas provisórias, visando fazer cessar qualquer alegada violação e prevenir qualquer novo prejuízo contra os interesses envolvidos.

Artigo 54.º

Responsabilidade e direito a indemnização

1. Os Estados-Membros devem prever que qualquer pessoa que tenha sofrido um prejuízo devido ao tratamento ilícito ou outro ato incompatível com as disposições adotadas nos termos da presente diretiva tem o direito de receber uma indemnização do responsável pelo tratamento ou do subcontratante pelo prejuízo sofrido.

2. Sempre que vários responsáveis pelo tratamento ou subcontratantes estiverem envolvidos no tratamento de dados, cada um deles é conjunta e solidariamente responsável pelo montante total dos danos.

3. O responsável pelo tratamento ou o subcontratante pode ser exonerado dessa responsabilidade, total ou parcialmente, se provar que o facto que causou o dano não lhe é imputável.

Artigo 55.º
Sanções

Os Estados-Membros devem prever as disposições relativas às sanções aplicáveis às violações das disposições adotadas nos termos da presente diretiva e adotar todas as medidas necessárias para assegurar a sua aplicação. As sanções previstas devem ser eficazes, proporcionadas e dissuasivas.

CAPÍTULO IX
ATOS DELEGADOS E ATOS DE EXECUÇÃO

Artigo 56.º
Exercício de delegação

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

2. A delegação de poderes a que se refere o artigo 28.º, n.º 5, é conferida à Comissão por um período indeterminado a contar da data de entrada em vigor da presente diretiva.

3. A delegação de poderes a que se refere o artigo 28.º, n.º 5 pode ser revogada a qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A revogação produz efeitos no dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou numa data posterior nela especificada. A decisão de revogação não prejudica a validade dos atos delegados já em vigor.

4. Logo que adote um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

5. Um ato delegado adotado em conformidade com o artigo 28.º, n.º 5, só pode entrar em vigor se não forem formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de dois meses a contar da notificação desse ato ao Parlamento Europeu e ao Conselho ou se, antes do termo do referido prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não pretendem formular objeções. Esse prazo é prorrogável por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 57.º
Procedimento de comité

1. A Comissão é assistida por um comité. Esse comité é um comité na aceção do Regulamento (UE) n.º 182/2011.

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

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

CAPÍTULO X
DISPOSIÇÕES FINAIS

Artigo 58.º
Revogações

1. É revogada a Decisão-Quadro 2008/977/JAI do Conselho.

2. As referências à decisão-quadro revogada, referida no n.º 1, são consideradas referências à presente diretiva.

Artigo 59.º
Relação com atos da União Europeia adotados anteriormente no domínio da cooperação judiciária em matéria penal e da cooperação policial

As disposições específicas para a proteção de dados pessoais no que respeita ao tratamento desses dados pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, previstas nos atos da União Europeia adotados antes da data de adoção da presente diretiva que regulam o tratamento de dados pessoais entre os Estados-Membros e o acesso das autoridades dos Estados-Membros designadas aos sistemas informáticos criados por força dos Tratados, no âmbito da presente diretiva, continuam inalteradas.

Artigo 60.º
Relação com acordos internacionais concluídos anteriormente no domínio da cooperação judiciária em matéria penal e da cooperação policial.

Os acordos internacionais concluídos pelos Estados-Membros antes da entrada em vigor da presente diretiva são alterados, sempre que necessário, no prazo de cinco anos a contar da sua entrada em vigor.

Artigo 61.º
Avaliação

1. A Comissão deve avaliar a aplicação da presente diretiva.

2. A Comissão deve proceder ao reexame, no prazo de três anos a contar da entrada em vigor da presente diretiva, de outros atos adotados pela União Europeia que regulam o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, em especial os atos adotados pela União que são mencionados no artigo 59.º, a fim de avaliar a necessidade de os harmonizar com a presente diretiva e apresentar, 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.

3. A Comissão apresenta periodicamente ao Parlamento Europeu e ao Conselho relatórios sobre a avaliação e reexame da presente diretiva nos termos do n.º 1. O primeiro relatório deve ser apresentado o mais tardar quatro anos após a entrada em vigor da presente diretiva. Os relatórios subsequentes devem ser apresentados com uma periodicidade de quatro anos. A Comissão apresentará, se necessário, propostas adequadas com vista à alteração da presente diretiva e à harmonização de outros instrumentos jurídicos. O relatório é objeto de publicação.

Artigo 62.º
Transposição

1. Os Estados-Membros devem adotar e publicar, até [data/dois anos após a entrada em vigor], as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva. Os Estados-Membros devem comunicar imediatamente à Comissão o texto dessas disposições.

   Os Estados-Membros devem aplicar as referidas disposições a partir de xx.xx.201x [data/dois anos após a entrada em vigor].

   As disposições adotadas pelos Estados-Membros devem fazer referência à presente diretiva ou ser acompanhadas dessa referência aquando da sua publicação oficial. As modalidades da referência são estabelecidas pelos Estados-Membros.

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

Artigo 63.º
Entrada em vigor e aplicação

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

Artigo 64.º
Destinatários

Os destinatários da presente diretiva são os Estados-Membros.

Feito em Bruxelas, em 25.1.2012

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