

COMENTÁRIO
AO
REGULAMENTO GERAL
DE PROTEÇÃO DE DADOS
E À
LEI N.º 58/2019

CÓDIGOS COMENTADOS
DO CENTRO DE INVESTIGAÇÃO DE DIREITO PRIVADO

COMENTÁRIO
AO
REGULAMENTO GERAL
DE PROTEÇÃO DE DADOS
E À
LEI N.º 58/2019

A. BARRETO MENEZES CORDEIRO
COORDENADOR

COMENTÁRIO AO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS E À LEI N.º 58/2019

COORDENAÇÃO

A. BARRETO MENEZES CORDEIRO

EDITOR

EDIÇÕES ALMEDINA, S.A.

Rua Fernandes Tomás, n.º 76-80

3000-167 Coimbra

Tel.: 239 851 904 · Fax: 239 851 901

www.almedina.net · editora@almedina.net

DESIGN DE CAPA

FBA

PRÉ-IMPRESSÃO

EDIÇÕES ALMEDINA, SA

IMPRESSÃO E ACABAMENTO

PUBLITO - BRAGA

Março, 2021

DEPÓSITO LEGAL

481068/21

ISBN

978-972-40-9261-4.

Os dados e as opiniões inseridos na presente publicação
são da exclusiva responsabilidade do(s) seu(s) autor(es).

Toda a reprodução desta obra, por fotocópia ou outro qualquer
processo, sem prévia autorização escrita do Editor, é ilícita
e passível de procedimento judicial contra o infrator.

COLABORADORES

A. BARRETO MENEZES CORDEIRO, LLM

Doutor em Direito; Professor Associado da FDL
Investigador do CIDP

(1.º a 11.º e 77.º a 84.º do RGPD; 1.º-2.º, 16.º-17.º, 29.º-30.º, 32.º-35.º e 56.º da LE)

DIOGO PEREIRA DUARTE

Doutor em Direito; Professor Auxiliar da FDL
Investigador do CIDP

(37.º-43.º e 88.º do RGPD; 9.º-15.º e 28.º LE)

FRANCISCO PAES MARQUES

Doutor em Direito; Professor Auxiliar da FDL
Investigador do ICJP/CIDP

(85.º-87.º, 89.º e 91.º do RGPD; 19.º, 23.º-27.º e 31.º LE)

FRANCISCO RODRIGUES ROCHA

Doutor em Direito; Assistente Convidado da FDL
Investigador do CIDP

(24.º-36.º do RGPD; 21.º da LE)

VÍTOR PALMELA FIDALGO

Mestre em Direito; Assistente Convidado da FDL
Investigador do CIDP

(12.º-23.º do RGPD; 18.º e 20.º da LE)

TIAGO GERALDO

Assistente Convidado da FDL
Investigador do CIDPCC

(46.º-54.º da LE)

INÊS SÍTIMA

Assistente Convidada da FDL
Investigadora do CIDP

(51.º-59.º e 90.º do RGPD; 3.º-8.º, 36.º-45.º e 55.º da LE)

DANIELA RODRIGUES DE SOUSA

Assistente Convidada da FDL
Investigadora do CIDP

(60.º-76.º do RGPD)

DINA FREITAS TEIXEIRA

Assistente Convidada da FDL
Investigador do CIDP

(44.º-50.º e 94.º-99.º do RGPD; 22.º e 57-62 da LE)

ADVERTÊNCIAS

As disposições legais não acompanhadas de fonte correspondem a artigos do Regulamento Geral de Proteção de Dados – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.

A obra encontra-se atualizada com referência a elementos publicados até agosto de 2020.

ÍNDICE GERAL

Abreviaturas	17
------------------------	----

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, DE 27 DE ABRIL DE 2016

Considerandos	21
-------------------------	----

Capítulo I – Disposições gerais

Artigo 1.º – Objeto e objetivos	62
Artigo 2.º – Âmbito de aplicação material	66
Artigo 3.º – Âmbito de aplicação territorial	70
Artigo 4.º – Definições	77

Capítulo II – Princípios

Artigo 5.º – Princípios relativos ao tratamento de dados pessoais	101
Artigo 6.º – Licitude do tratamento	107
Artigo 7.º – Condições aplicáveis ao consentimento	120
Artigo 8.º – Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação.	125
Artigo 9.º – Tratamento de categorias especiais de dados pessoais	130
Artigo 10.º – Tratamento de dados pessoais relacionados com condenações penais e infrações	142
Artigo 11.º – Tratamento que não exige identificação	144

Capítulo III – Direitos do titular dos dados

Secção 1 – Transparência e regras para o exercício dos direitos dos titulares dos dados

Artigo 12.º – Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados	146
---	-----

Secção 2 – Informação e acesso aos dados pessoais

Artigo 13.º – Informações a facultar quando os dados pessoais são recolhidos junto do titular	156
Artigo 14.º – Informações a facultar quando os dados pessoais não são recolhidos junto do titular	164
Artigo 15.º – Direito de acesso do titular dos dados	173

Secção 3 – Retificação e apagamento

Artigo 16.º – Direito de retificação	180
Artigo 17.º – Direito ao apagamento dos dados («direito a ser esquecido»)	185
Artigo 18.º – Direito à limitação do tratamento	196
Artigo 19.º – Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento	201
Artigo 20.º – Direito de portabilidade dos dados.	204

Secção 4 – Direito de oposição e decisões individuais automatizadas

Artigo 21.º – Direito de oposição	213
Artigo 22.º – Decisões individuais automatizadas, incluindo definição de perfis.	220

Secção 5 – Limitações

Artigo 23.º – Limitações	227
------------------------------------	-----

Capítulo IV – Responsável pelo tratamento e subcontratante

Secção 1 – Obrigações gerais

Artigo 24.º – Responsabilidade do responsável pelo tratamento	232
Artigo 25.º – Proteção de dados desde a conceção e por defeito	238
Artigo 26.º – Responsáveis conjuntos pelo tratamento	244
Artigo 27.º – Representantes dos responsáveis pelo tratamento ou dos subcontratantes não estabelecidos na União	248
Artigo 28.º – Subcontratante	251
Artigo 29.º – Tratamento sob a autoridade do responsável pelo tratamento ou do subcontratante	257
Artigo 30.º – Registos das atividades de tratamento	259
Artigo 31.º – Cooperação com a autoridade de controlo.	264

Secção 2 – Segurança dos dados pessoais

Artigo 32.º – Segurança do tratamento.	266
Artigo 33.º – Notificação de uma violação de dados pessoais à autoridade de controlo	269
Artigo 34.º – Comunicação de uma violação de dados pessoais ao titular dos dados	275

Secção 3 – Avaliação de impacto sobre a proteção de dados e consulta prévia

Artigo 35.º – Avaliação de impacto sobre a proteção de dados	279
Artigo 36.º – Consulta prévia	285

Secção 4 – Encarregado da proteção de dados

Artigo 37.º – Designação do encarregado da proteção de dados.	288
---	-----

Artigo 38.º – Posição do encarregado da proteção de dados	295
Artigo 39.º – Funções do encarregado da proteção de dados	299

Secção 5 – Códigos de conduta e certificação

Artigo 40.º – Códigos de conduta	302
Artigo 41.º – Supervisão dos códigos de conduta aprovados	306
Artigo 42.º – Certificação	309
Artigo 43.º – Organismos de certificação	313

Capítulo V – Transferências de dados pessoais para países terceiros ou organizações internacionais

Artigo 44.º – Princípio geral das transferências	317
Artigo 45.º – Transferências com base numa decisão de adequação	320
Artigo 46.º – Transferências sujeitas a garantias adequadas	329
Artigo 47.º – Regras vinculativas aplicáveis às empresas	336
Artigo 48.º – Transferências ou divulgações não autorizadas pelo direito da União	344
Artigo 49.º – Derrogações para situações específicas	346
Artigo 50.º – Cooperação internacional no domínio da proteção de dados pessoais	352

Capítulo VI – Autoridades de controlo independentes

Secção 1 – Estatuto independente

Artigo 51.º – Autoridade de controlo	356
Artigo 52.º – Independência	363
Artigo 53.º – Condições gerais aplicáveis aos membros da autoridade de controlo	370
Artigo 54.º – Regras aplicáveis à constituição da autoridade de controlo	376

Secção 2 – Competência, atribuições e poderes

Artigo 55.º – Competência	381
Artigo 56.º – Competência da autoridade de controlo principal	386
Artigo 57.º – Atribuições	395
Artigo 58.º – Poderes	406
Artigo 59.º – Relatórios de atividades	417

Capítulo VII – Cooperação e coerência

Secção 1 – Cooperação

Artigo 60.º – Cooperação entre a autoridade de controlo principal e as outras autoridades de controlo interessadas	422
---	-----

Artigo 61.º – Assistência mútua	430
Artigo 62.º – Operações conjuntas das autoridades de controlo	435

Secção 2 – Coerência

Artigo 63.º – Procedimento de controlo da coerência	439
Artigo 64.º – Parecer do Comité	441
Artigo 65.º – Resolução de litígios pelo Comité.	447
Artigo 66.º – Procedimento de urgência	452
Artigo 67.º – Troca de informações	455

Secção 3 – Comité europeu para a proteção de dados

Artigo 68.º – Comité Europeu para a Proteção de Dados	457
Artigo 69.º – Independência	460
Artigo 70.º – Atribuições do Comité	462
Artigo 71.º – Relatórios	469
Artigo 72.º – Procedimento	470
Artigo 73.º – Presidente	472
Artigo 74.º – Funções do presidente	474
Artigo 75.º – Secretariado	476
Artigo 76.º – Confidencialidade	479

Capítulo VIII – Vias de recurso, responsabilidade e sanções

Artigo 77.º – Direito de apresentar reclamação a uma autoridade de controlo.	481
Artigo 78.º – Direito à ação judicial contra uma autoridade de controlo.	484
Artigo 79.º – Direito à ação judicial contra um responsável pelo tratamento ou um subcontratante	486
Artigo 80.º – Representação dos titulares dos dados	489
Artigo 81.º – Suspensão do processo	492
Artigo 82.º – Direito de indemnização e responsabilidade	494
Artigo 83.º – Condições gerais para a aplicação de coimas.	498
Artigo 84.º – Sanções	510

Capítulo IX – Disposições relativas a situações específicas de tratamento

Artigo 85.º – Tratamento e liberdade de expressão e de informação	512
Artigo 86.º – Tratamento e acesso do público aos documentos oficiais	516
Artigo 87.º – Tratamento do número de identificação nacional	519
Artigo 88.º – Tratamento no contexto laboral.	523
Artigo 89.º – Garantias e derrogações relativas ao tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos	527
Artigo 90.º – Obrigações de sigilo	532
Artigo 91.º – Normas vigentes em matéria de proteção dos dados das igrejas e associações religiosas	537

Capítulo X – Atos delegados e atos de execução

Artigo 92.º – Exercício da delegação	540
Artigo 93.º – Procedimento de comité.	543

Capítulo XI – Disposições finais

Artigo 94.º – Revogação da Diretiva 95/46/CE.	546
Artigo 95.º – Relação com a Diretiva 2002/58/CE	549
Artigo 96.º – Relação com acordos celebrados anteriormente	552
Artigo 97.º – Relatórios da Comissão	554
Artigo 98.º – Revisão de outros atos jurídicos da União em matéria de proteção de dados	557
Artigo 99.º – Entrada em vigor e aplicação.	559

LEI N.º 58/2019, DE 8 DE AGOSTO**Capítulo I – Disposições gerais**

Artigo 1.º – Objeto	561
Artigo 2.º – Âmbito de aplicação	563

Capítulo II – Comissão Nacional de Proteção de Dados

Artigo 3.º – Autoridade de controlo nacional	566
Artigo 4.º – Natureza e independência.	567
Artigo 5.º – Composição e funcionamento	570
Artigo 6.º – Atribuições e competências.	575
Artigo 7.º – Avaliações prévias de impacto	578
Artigo 8.º – Dever de colaboração.	579

Capítulo III – Encarregado de proteção de dados

Artigo 9.º – Disposição geral	582
Artigo 10.º – Dever de sigilo e confidencialidade	584
Artigo 11.º – Funções do encarregado de proteção de dados	585
Artigo 12.º – Encarregados de proteção de dados em entidades públicas.	586
Artigo 13.º – Encarregados de proteção de dados em entidades privadas.	588

Capítulo IV – Acreditação, certificação e códigos de conduta

Artigo 14.º – Acreditação e certificação	588
Artigo 15.º – Códigos de conduta	589

Capítulo V – Disposições especiais

Artigo 16.º – Consentimento de menores	590
Artigo 17.º – Proteção de dados pessoais de pessoas falecidas	591
Artigo 18.º – Portabilidade e interoperabilidade dos dados.	594
Artigo 19.º – Videovigilância	596
Artigo 20.º – Dever de segredo	598
Artigo 21.º – Prazo de conservação de dados pessoais	600
Artigo 22.º – Transferências de dados	606
Artigo 23.º – Tratamento de dados pessoais por entidades públicas para finalidades diferentes.	608

Capítulo VI – Situações específicas de tratamento de dados pessoais

Artigo 24.º – Liberdade de expressão e informação.	611
Artigo 25.º – Publicação em jornal oficial	614
Artigo 26.º – Acesso a documentos administrativos	616
Artigo 27.º – Publicação de dados no âmbito da contratação pública	618
Artigo 28.º – Relações laborais	620
Artigo 29.º – Tratamento de dados de saúde e dados genéticos.	624
Artigo 30.º – Bases de dados ou registos centralizados de saúde	626
Artigo 31.º – Tratamentos para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos.	627

Capítulo VII – Tutela administrativa e jurisdicional

Secção I – Disposições gerais

Artigo 32.º – Tutela administrativa	629
Artigo 33.º – Responsabilidade civil	630
Artigo 34.º – Tutela jurisdicional	631
Artigo 35.º – Representação dos titulares dos dados	632
Artigo 36.º – Legitimidade da CNPD	633

Secção II – Contraordenações

Artigo 37.º – Contraordenações muito graves.	634
Artigo 38.º – Contraordenações graves.	637
Artigo 39.º – Determinação da medida da coima	639
Artigo 40.º – Prescrição do procedimento por contraordenação	644
Artigo 41.º – Prazo de prescrição das coimas	645
Artigo 42.º – Destino das coimas.	645
Artigo 43.º – Cumprimento do dever omitido	646
Artigo 44.º – Âmbito de aplicação das contraordenações	647
Artigo 45.º – Regime subsidiário	650

Secção III – Crimes

Artigo 46.º – Utilização de dados de forma incompatível com a finalidade da recolha	651
Artigo 47.º – Acesso indevido	652
Artigo 48.º – Desvio de dados	654
Artigo 49.º – Viciação ou destruição de dados.	656
Artigo 50.º – Inserção de dados falsos.	658
Artigo 51.º – Violação do dever de sigilo	659
Artigo 52.º – Desobediência	660
Artigo 53.º – Punibilidade da tentativa.	662
Artigo 54.º – Responsabilidade das pessoas coletivas	662

Secção IV – Disposições comuns

Artigo 55.º – Concurso de infrações	664
Artigo 56.º – Sanções acessórias.	666

Capítulo VIII – Disposições finais e transitórias

Artigo 57.º – Comissão Nacional de Proteção de Dados	667
Artigo 58.º – Orientações técnicas.	668
Artigo 59.º – Aplicabilidade das coimas às entidades públicas	669
Artigo 60.º – Situações de tratamentos de dados pessoais pré-existentes	671
Artigo 61.º – Renovação do consentimento	673
Artigo 62.º – Regimes de proteção de dados pessoais	676
Índice Ideográfico.	679

ABREVIATURAS

AEPD	– Autoridade Europeia para a Proteção de Dados
AIPD	– avaliação de impacto na proteção de dados
Albrecht/Jotzo, <i>Das neue Datenschutzrecht</i>	– Jan Philipp Albrecht/Florian Jotzo, <i>Das neue Datenschutzrecht in der EU: Grundlagen, Gesetzgebungsverfahren, Synopse</i> , Nomos: Baden-Baden (2017)
APD	– Anuário da Proteção de Dados
BCR	– <i>Binding Corporate Rules</i>
BeckOk	– <i>BeckOk Datenschutzrecht</i> , coord. Stefand Brink/Heinrich Amadeus Wolff, 28ª ed., Beck: Munique (2019)
B. Menezes Cordeiro, <i>DPD</i>	– A. Barreto Menezes Cordeiro, <i>Direito da proteção de dados: À luz do RGPD e da Lei n.º 58/2019</i> , Almedina: Coimbra (2020)
Bistolfi/Bolognini/Pelino	– Camilla Bistolfi/Luca Bolognini/Enrico Pelino, <i>Il Regolamento Privacy Europeu: Commentario alla nuova disciplina sulla protezione dei dati personali</i> , Giuffrè: Milão (2016)
BVerfG	– Bundesverfassungsgericht
Carta	– Carta dos Direitos Fundamentais da União Europeia
CC	– Código Civil
CCP	– Código dos Contratos Públicos
CNPD	– Comissão Nacional de Proteção de Dados
Comité	– Comité Europeu para a Proteção de Dados
Comissão	– Comissão Europeia
Comissão, <i>Proposta</i>	– <i>Proposta de Regulamento do Parlamento e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados)</i> , COM(2012) 11 final
Conselho	– Conselho da União Europeia
Conselho, <i>General Approach</i>	– Conselho da União Europeia, <i>General Data Protection Regulation Proposal: Preparation of a General Approach</i> , doc. 9657/15, 11 junho 2015
Convenção 108	– Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal
CMLR	– Common Market Law Review
CP	– Código Penal
CPA	– Código de Procedimento Administrativo
CPC	– Código de Processo Civil
CPP	– Código de Processo Penal
C&R	– Computer & Recht
CT	– Código do Trabalho
CRP	– Constituição da República Portuguesa

DSRITB	– Tagungsband Deutsche Stiftung für Recht und Informatik
D	– Diretiva
D 95/46	– 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
DL	– Decreto-Lei
DuD	– Datenschutz und Datensicherheit
Duke L & Tech Rev	– Duke Law & Technology Review
EDPL	– European Data Protection Law Review
EEE	– Espaço Económico Europeu
EH	– Estudos em Homenagem
<i>Ehmann/Selmayr</i>	– <i>Ehmann/Selmayr, Datenschutz-Grundverordnung</i> , 2ª ed., Beck: Munique (2018)
EL Rev	– European Law Review
EJLT	– European Journal of Law and Technology
EPD	– encarregado de proteção de dados
EM	– Estudos em Memória
EMP	– Estatuto do Ministério Público (Lei n.º 47/86, de 15 de outubro)
EuR	– Europarecht
EuZW	– Europäische Zeitschrift für Wirtschaftsrecht
Fordham Intell Prop Media & Ent LJ	– Fordham Intellectual Property, Media & Entertainment Law Journal
Forum PD	– Forum de Proteção de Dados
Geo LJ	– Georgetown Law Journal
<i>Gierschmann/Schlender/Stentzel/Veil</i>	– <i>Gierschmann/Schlender/Stentzel/Veil Kommentar Datenschutz-Grundverordnung</i> , Bundesanzeiger: Colónia (2017)
Guerra Martins, <i>Manual</i>	– Ana Maria Guerra Martins, <i>Manual de Direito da União Europeia: Após o Tratado de Lisboa</i> , 2ª ed., Almedina: Coimbra (2018)
<i>Gola</i>	– <i>Gola Datenschutz-Grundverordnung – DS-GVO (EU) 2016/679 Kommentar</i> , 2.ª ed., Beck: Munique (2018)
<i>Gola/Heckmann</i>	– <i>Gola/Heckmann Bundesdatenschutzgesetz – BDSG Kommentar</i> , 13.ª ed., Beck: Munique (2019)
GRUR Int	– <i>Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil</i>
GT 29	– Grupo de Trabalho do Artigo 29.º
GT-RGPD	– Grupo de Trabalho com o objetivo de preparar a legislação portuguesa para a aplicação do RGPD em Portugal
HDSG	– Hessische Datenschutzgesetz
HTLJ	– Santa Clara High Technology Law Journal
IDPL	– International Data Privacy Law
JOUE	– Jornal Oficial da União Europeia
<i>Kellerbauer/Klamert/Tomkin</i>	– <i>Commentary on the EU Treaties and the Charter of Fundamental Rights</i> , coord. Manuel Kellerbauer/Marcus Klamert/Jonathan Tomkin, OUP: Oxford (2019)

<i>Kühling/Buchner</i>	– <i>Kühling/Buchner Datenschutz-Grundverordnung, Bundesdatenschutzgesetz Kommentar</i> , 2ª ed., Beck: Munique (2018)
<i>Kuner/Bygrave/Docksey</i>	– <i>The EU General Data Protection Regulation (GDPR): A Commentary</i> , coord. Christopher Kuner/Lee A. Bygrave/Christopher Docksey, OUP: Oxford (2020)
LADA	– Lei de Acesso a Documentos Administrativos (Lei n.º 26/2016, de 22 de agosto)
LCNPD	– Lei de Organização e Funcionamento da Comissão Nacional de Proteção de Dados (Lei n.º 43/2004, de 18 de agosto)
LE	– Lei n.º 58/2019
LPD 98	– Lei da Proteção de Dados Pessoais (Lei n.º 67/98, de 28 de outubro)
Menezes Cordeiro, <i>Tratado</i>	– António Menezes Cordeiro, <i>Tratado de Direito Civil</i> , Almedina: Coimbra, I-XII
MMR	– Multimedia & Recht
MP	– Ministério Público
NJW	– Neue Juristische Wochenschrift
NVwZ	– Neue Zeitschrift für Verwaltungsrecht
p.	– parte
<i>Paal/Pauly</i>	– <i>Paal/Pauly Datenschutz-Grundverordnung – Bundesdatenschutzgesetz</i> , 2.ª ed., Beck: Munique (2018)
Parlamento	– Parlamento Europeu
Parlamento, <i>Relatório</i>	– Parlamento Europeu, <i>Relatório sobre a 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 (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)))</i>
<i>Plath</i>	– <i>Plath, Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen des TMG und TKG</i> , 3ª ed., Dr. Otto Schmidt: Colónia (2018)
R	– Regulamento
RCb	– Relação de Coimbra
RDA	– Revista de Direito Administrativo
RDC	– Revista de Direito Civil
RDES	– Revista de Direito e Estudos Sociais
RDFMC	– Revista de Direito Financeiro e dos Mercados de Capitais
RDTec	– Revista de Direito e Tecnologia
REv	– Relação de Évora
RFDUL	– Revista da Faculdade de Direito da Universidade de Lisboa
RGm	– Relação de Guimarães
RGCO	– Regime Geral das Contra-Ordenações (DL n.º 433/82, de 27 de outubro)
<i>RGPD/Sousa Pinheiro</i>	– <i>Comentário ao Regulamento Geral de Proteção de Dados</i> , coord. Alexandre Sousa Pinheiro, Coimbra: Almedina (2018)
<i>Riccio/Scorza/Belisario</i>	– <i>GDPR e normativa privacy commentario</i> , coord. Giovanni M. Riccio/Guido Scorza/Ernesto Belisario, Milão: Wolters Kluwer (2018)
RLx	– Relação de Lisboa
Rn.	– Randnummer

RPt	– Relação do Porto
Rutgers Computer & Tech LJ	– Rutgers Computer & Tech Law Journal
Schantz/Wolff, <i>Das neue Datenschutzrecht</i>	– Peter Schantz/Heinrich Amadeus Wolff, <i>Das neue Datenschutzrecht – Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis</i> , Beck: Munique (2017)
<i>Simitis/Hornung/Spiecker gen. Döhmann</i>	– <i>Simitis/Hornung/Spiecker gen. Döhmann Datenschutzrecht, DSGVO mit BDSG</i> , Nomos: Baden-Baden (2019)
STA	– Supremo Tribunal Administrativo
STJ	– Supremo Tribunal de Justiça
Sydow	– <i>Sydow Europäische Datenschutzgrundverordnung Handkommentar</i> , 2. ^a ed., Nomos: Baden-Baden (2018)
<i>Taeger/Gabel</i>	– <i>Taeger/Gabel Kommentar DSGVO – BDSG</i> , 3. ^a ed., R&W: Francoforte (2019)
TC	– Tribunal Constitucional
TEDH	– Tribunal Europeu dos Direitos do Homem
TFUE	– Tratado sobre o Funcionamento da União Europeia
TGUE	– Tribunal Geral da União Europeia
TJUE	– Tribunal de Justiça da União Europeia
TUE	– Tratado da União Europeia
Voigt/Bussche, <i>A Practical Guide</i>	– Paul Voigt/Axel von dem Bussche, <i>The EU General Data Protection Regulation (GDPR) - A Practical Guide</i> , Cham: Springer (2017)
ZD	– Zeitschrift für Datenschutz

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016

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

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

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

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu¹,

Tendo em conta o parecer do Comité das Regiões²,

Deliberando de acordo com o processo legislativo ordinário³,

Considerando o seguinte:

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

(2) Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.

¹ JO C 229 de 31.7.2012, p. 90.

² JO C 391 de 18.12.2012, p. 127.

³ Posição do Parlamento Europeu de 12 de março de 2014 (ainda não publicada no Jornal Oficial) e posição do Con-

selho em primeira leitura de 8 de abril de 2016 (ainda não publicada no Jornal Oficial). Posição do Parlamento Europeu de 14 de abril de 2016.

(3) A Diretiva 95/46/CE do Parlamento Europeu e do Conselho⁴ visa harmonizar a defesa dos direitos e das liberdades fundamentais das pessoas singulares em relação às atividades de tratamento de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros.

(4) O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística.

(5) A integração económica e social resultante do funcionamento do mercado interno provocou um aumento significativo dos fluxos transfronteiriços de dados pessoais. O intercâmbio de dados entre intervenientes públicos e privados, incluindo as pessoas singulares, as associações e as empresas, intensificou-se na União Europeia. As autoridades nacionais dos Estados-Membros são chamadas, por força do direito da União, a colaborar e a trocar dados pessoais entre si, a fim de poderem desempenhar as suas funções ou executar funções por conta de uma autoridade de outro Estado-Membro.

(6) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.

(7) Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.

(8) Caso o presente regulamento preveja especificações ou restrições das suas regras pelo direito de um Estado-Membro, estes podem incorporar elementos do presente regulamento no respetivo direito nacional, na medida do necessário para manter a coerência e tornar as disposições nacionais compreensíveis para as pessoas a quem se aplicam.

(9) Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à

⁴ 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).

proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE.

(10) A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogênea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais. No que diz respeito ao tratamento de dados pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-Membros deverão poder manter ou aprovar disposições nacionais para especificar a aplicação das regras do presente regulamento. Em conjugação com a legislação geral e horizontal sobre proteção de dados que dá aplicação à Diretiva 95/46/CE, os Estados-Membros dispõem de várias leis setoriais em domínios que necessitam de disposições mais específicas. O presente regulamento também dá aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»). Nessa medida, o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais.

(11) A proteção eficaz dos dados pessoais na União exige o reforço e a especificação dos direitos dos titulares dos dados e as obrigações dos responsáveis pelo tratamento e pela definição do tratamento dos dados pessoais, bem como poderes equivalentes para controlar e assegurar a conformidade das regras de proteção dos dados pessoais e sanções equivalentes para as infrações nos Estados-Membros.

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

(13) A fim de assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno, é necessário um regulamento que garanta a segurança jurídica e a transparência aos operadores económicos, incluindo as micro, pequenas e médias empresas, que assegure às pessoas singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes, que assegure um controlo coerente do tratamento dos dados pessoais, sanções equivalentes em todos os Estados-Membros, bem como uma cooperação efetiva entre as autoridades de controlo dos diferentes Estados-Membros. O bom funcionamento do mercado interno impõe que a livre circulação de dados pessoais na União não pode ser restringida ou proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais. Para ter em conta a situação particular das micro, pequenas e médias empresas, o presente regulamento prevê uma derrogação para as organizações com menos de 250 trabalhadores relativamente à conservação do registo de atividades. Além disso, as instituições e os órgãos da União, e os Estados-Membros e as suas autoridades de controlo, são incentivados a tomar em consideração as necessidades específicas

das micro, pequenas e médias empresas no âmbito de aplicação do presente regulamento. A noção de micro, pequenas e médias empresaster em conta deverá inspirar-se do artigo 2.º do anexo da Recomendação 2003/361/CE da Comissão⁵.

(14) A proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais. O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva.

(15) A fim de se evitar o sério risco sério de ser contornada a proteção das pessoas singulares, esta deverá ser neutra em termos tecnológicos e deverá ser independente das técnicas utilizadas. A proteção das pessoas singulares deverá aplicar-se ao tratamento de dados pessoais por meios automatizados, bem como ao tratamento manual, se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros. Os ficheiros ou os conjuntos de ficheiros bem como as suas capas, que não estejam estruturados de acordo com critérios específicos, não deverão ser abrangidos pelo âmbito de aplicação do presente regulamento.

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

(17) O Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho⁶ é aplicável ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n.º 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, deverão ser adaptados aos princípios e regras estabelecidos pelo presente regulamento e aplicados à luz do mesmo. A fim de proporcionar um quadro de proteção de dados sólido e coerente na União, e após a adoção do presente regulamento, deverão ser realizadas as necessárias adaptações do Regulamento (CE) n.º 45/2001, a fim de permitir a aplicação em simultâneo com o presente regulamento.

(18) O presente regulamento não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma atividade profissional ou comercial. As atividades pessoais ou domésticas poderão incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrónico no âmbito dessas atividades. Todavia, o presente regulamento é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas.

(19) A proteção das pessoas singulares em matéria de tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de um ato jurídico da União específico. O presente regulamento não deverá, por isso, ser aplicável às atividades de tratamento para esses efeitos.

⁵ Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas (JO L 124 de 20.5.2003, p. 36).

⁶ Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à prote-

ção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).

Todavia, os dados pessoais tratados pelas autoridades competentes ao abrigo do presente regulamento deverão ser regulados, quando forem usados para os efeitos referidos, por um ato jurídico da União mais específico, a saber, a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho⁷. Os Estados-Membros podem confiar às autoridades competentes na aceção da Diretiva (UE) 2016/680 funções não necessariamente a executar para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, de modo a que o tratamento dos dados pessoais para esses outros efeitos, na medida em que se insira na esfera do direito da União, seja abrangido pelo âmbito de aplicação do presente regulamento.

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

(20) Na medida em que o presente regulamento é igualmente aplicável, entre outras, às atividades dos tribunais e de outras autoridades judiciais, poderá determinar-se no direito da União ou dos Estados-Membros quais as operações e os procedimentos a seguir pelos tribunais e outras autoridades judiciais para o tratamento de dados pessoais. A competência das autoridades de controlo não abrange o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência do poder judicial no exercício da sua função jurisdicional, nomeadamente a tomada de decisões. Deverá ser possível confiar o controlo de tais operações de tratamento de dados a organismos específicos no âmbito do sistema judicial do Estado-Membro, que deverão, nomeadamente, assegurar o cumprimento das regras do presente regulamento, reforçar a sensibilização os membros do poder judicial para as obrigações que lhe são impostas pelo presente regulamento e tratar reclamações relativas às operações de tratamento dos dados.

(21) O presente regulamento aplica-se sem prejuízo da aplicação da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho⁸, nomeadamente das normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12.º a 15.º. A referida diretiva

⁷ Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (ver página 89 do presente Jornal Oficial).

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

tem por objetivo contribuir para o correto funcionamento do mercado interno, garantindo a livre circulação dos serviços da sociedade da informação entre Estados-Membros.

(22) Qualquer tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado na União deverá ser feito em conformidade com o presente regulamento, independentemente de o tratamento em si ser realizado na União. O estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável. A forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto.

(23) A fim de evitar que as pessoas singulares sejam privadas da proteção que lhes assiste por força do presente regulamento, o tratamento dos dados pessoais de titulares que se encontrem na União por um responsável pelo tratamento ou subcontratante não estabelecido na União deverá ser abrangido pelo presente regulamento se as atividades de tratamento estiverem relacionadas com a oferta de bens ou serviços a esses titulares, independentemente de estarem associadas a um pagamento. A fim de determinar se o responsável pelo tratamento ou subcontratante oferece ou não bens ou serviços aos titulares dos dados que se encontrem na União, há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União. O mero facto de estar disponível na União um sítio web do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União.

(24) O tratamento de dados pessoais de titulares de dados que se encontrem na União por um responsável ou subcontratante que não esteja estabelecido na União deverá ser também abrangido pelo presente regulamento quando esteja relacionado com o controlo do comportamento dos referidos titulares de dados, na medida em que o seu comportamento tenha lugar na União. A fim de determinar se uma atividade de tratamento pode ser considerada «controlo do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.

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

(26) Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em

conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação.

(27) O presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas.

(28) A aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento e os seus subcontratantes a cumprir as suas obrigações de proteção de dados. A introdução explícita da «pseudonimização» no presente regulamento não se destina a excluir eventuais outras medidas de proteção de dados.

(29) A fim de criar incentivos para aplicar a pseudonimização durante o tratamento de dados pessoais, deverá ser possível tomar medidas de pseudonimização, permitindo-se simultaneamente uma análise geral, no âmbito do mesmo responsável pelo tratamento quando este tiver tomado as medidas técnicas e organizativas necessárias para assegurar, relativamente ao tratamento em questão, a aplicação do presente regulamento e a conservação em separado das informações adicionais que permitem atribuir os dados pessoais a um titular de dados específico. O responsável pelo tratamento que tratar os dados pessoais deverá indicar as pessoas autorizadas no âmbito do mesmo responsável pelo tratamento.

(30) As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet) ou testemunhos de conexão (cookie) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares.

(31) As autoridades públicas a quem forem divulgados dados pessoais em conformidade com obrigações jurídicas para o exercício da sua missão oficial, tais como as autoridades fiscais e aduaneiras, as unidades de investigação financeira, as autoridades administrativas independentes ou as autoridades dos mercados financeiros, responsáveis pela regulamentação e supervisão dos mercados de valores mobiliários, não deverão ser consideradas destinatárias se receberem dados pessoais que sejam necessários para efetuar um inquérito específico de interesse geral, em conformidade com o direito da União ou dos Estados-Membros. Os pedidos de divulgação enviados pelas autoridades públicas deverão ser sempre feitos por escrito, fundamentados e ocasionais e não deverão dizer respeito à totalidade de um ficheiro nem implicar a interconexão de ficheiros. O tratamento desses dados pessoais por essas autoridades públicas deverá respeitar as regras de proteção de dados aplicáveis de acordo com as finalidades do tratamento.

(32) O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a

mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido.

(33) Muitas vezes não é possível identificar na totalidade a finalidade do tratamento de dados pessoais para efeitos de investigação científica no momento da recolha dos dados. Por conseguinte, os titulares dos dados deverão poder dar o seu consentimento para determinadas áreas de investigação científica, desde que estejam de acordo com padrões éticos reconhecidos para a investigação científica. Os titulares dos dados deverão ter a possibilidade de dar o seu consentimento unicamente para determinados domínios de investigação ou partes de projetos de investigação, na medida permitida pela finalidade pretendida.

(34) Os dados genéticos deverão ser definidos como os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que resultem da análise de uma amostra biológica da pessoa singular em causa, nomeadamente da análise de cromossomas, ácido desoxirribonucleico (ADN) ou ácido ribonucleico (ARN), ou da análise de um outro elemento que permita obter informações equivalentes.

(35) Deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. O que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho⁹, a essa pessoa singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico *in vitro*.

(36) O estabelecimento principal de um responsável pelo tratamento na União deverá ser o local onde se encontra a sua administração central na União, salvo se as decisões sobre as finalidades e os meios de tratamento dos dados pessoais forem tomadas noutra estabelecimento do responsável pelo tratamento na União. Nesse caso, esse outro estabelecimento deverá ser considerado o estabelecimento principal. O estabelecimento principal de um responsável pelo tratamento na União deverá ser determinado de acordo com critérios objetivos e deverá pressupor o exercício efetivo e real de atividades de gestão que determinem as decisões principais quanto às finalidades e aos meios de tratamento mediante instalações estáveis. Esse critério não deverá depender do facto de o tratamento ser realizado nesse local. A existência e utilização de meios técnicos e de tecnologias para o tratamento de dados pessoais ou as atividades de tratamento não constituem, em si mesmas, um estabelecimento principal nem são, portanto, um critério definidor de estabelecimento principal. O estabelecimento principal do subcontratante é o local da sua administração central na União, ou, caso não tenha administração central na União, o local onde são exercidas as principais atividades de tratamento de dados na União. Nos casos que impliquem tanto o responsável pelo tratamento

⁹ Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativa ao exercício dos direitos

dos doentes em matéria de cuidados de saúde transfronteiriços (JO L 88 de 4.4.2011, p. 45).

como o subcontratante, a autoridade de controlo principal deverá continuar a ser a autoridade de controlo do Estado-Membro onde o responsável pelo tratamento tem o estabelecimento principal, mas a autoridade de controlo do subcontratante deverá ser considerada uma autoridade de controlo interessada e deverá participar no processo de cooperação previsto pelo presente regulamento. Em qualquer caso, as autoridades de controlo do Estado-Membro ou Estados-Membros em que o subcontratante tenha um ou mais estabelecimentos não deverão ser consideradas autoridades de controlo interessadas caso o projeto de decisão diga respeito apenas ao responsável pelo tratamento. Sempre que o tratamento dos dados seja efetuado por um grupo empresarial, o estabelecimento principal da empresa que exerce o controlo deverá ser considerado o estabelecimento principal do grupo empresarial, exceto quando as finalidades e os meios do tratamento sejam determinados por uma outra empresa.

(37) Um grupo empresarial deverá abranger uma empresa que exerce o controlo e as empresas que controla, devendo a primeira ser a que pode exercer uma influência dominante sobre as outras empresas, por exemplo, em virtude da propriedade, da participação financeira ou das regras que a regem ou da faculdade de fazer aplicar as regras relativas à proteção de dados pessoais. Uma empresa que controla o tratamento dos dados pessoais nas empresas a ela associadas deverá ser considerada, juntamente com essas empresas, um «grupo empresarial».

(38) As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança.

(39) O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados. As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento. Em especial, as finalidades específicas do tratamento dos dados pessoais deverão ser explícitas e legítimas e ser determinadas aquando da recolha dos dados pessoais. Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. Os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica. Deverão ser adotadas todas as medidas razoáveis para que os dados pessoais inexa-

tos sejam retificados ou apagados. Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas.

(40) Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar.

(41) Caso o presente regulamento se refira a um fundamento jurídico ou a uma medida legislativa, não se trata necessariamente de um ato legislativo adotado por um parlamento, sem prejuízo dos requisitos que decorram da ordem constitucional do Estado-Membro em causa. No entanto, esse fundamento jurídico ou essa medida legislativa deverão ser claros e precisos e a sua aplicação deverá ser previsível para os seus destinatários, em conformidade com a jurisprudência do Tribunal de Justiça da União Europeia («Tribunal de Justiça») e pelo Tribunal Europeu dos Direitos do Homem.

(42) Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance. Em conformidade com a Diretiva 93/13/CEE do Conselho¹⁰, uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.

(43) A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.

(44) O tratamento deverá ser considerado lícito caso seja necessário no contexto de um contrato ou da intenção de celebrar um contrato.

¹⁰ Diretiva 93/13/CEE do Conselho, de 5 de abril de 1993, relativa às cláusulas abusivas nos contratos celebrados com os consumidores (JO L 95 de 21.4.1993, p. 29).

(45) Sempre que o tratamento dos dados for realizado em conformidade com uma obrigação jurídica à qual esteja sujeito o responsável pelo tratamento, ou se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública, o tratamento deverá assentar no direito da União ou de um Estado-Membro. O presente regulamento não exige uma lei específica para cada tratamento de dados. Poderá ser suficiente uma lei para diversas operações de tratamento baseadas numa obrigação jurídica à qual esteja sujeito o responsável pelo tratamento, ou se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública. Deverá também caber ao direito da União ou dos Estados-Membros determinar qual a finalidade do tratamento dos dados. Além disso, a referida lei poderá especificar as condições gerais do presente regulamento que regem a legalidade do tratamento dos dados pessoais, estabelecer regras específicas para determinar os responsáveis pelo tratamento, o tipo de dados pessoais a tratar, os titulares dos dados em questão, as entidades a que os dados pessoais podem ser comunicados, os limites a que as finalidades do tratamento devem obedecer, os prazos de conservação e outras medidas destinadas a garantir a licitude e equidade do tratamento. Deverá igualmente caber ao direito da União ou dos Estados-Membros determinar se o responsável pelo tratamento que exerce funções de interesse público ou prerrogativas de autoridade pública deverá ser uma autoridade pública ou outra pessoa singular ou coletiva de direito público, ou, caso tal seja do interesse público, incluindo por motivos de saúde, como motivos de saúde pública e proteção social e de gestão dos serviços de saúde, de direito privado, por exemplo uma associação profissional.

(46) O tratamento de dados pessoais também deverá ser considerado lícito quando for necessário à proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa singular. Em princípio, o tratamento de dados pessoais com base no interesse vital de outra pessoa singular só pode ter lugar quando o tratamento não se puder basear manifestamente noutra fundamento jurídico. Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana.

(47) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta.

(48) Os responsáveis pelo tratamento que façam parte de um grupo empresarial ou de uma instituição associada a um organismo central poderão ter um interesse legítimo em transmitir dados pessoais no âmbito do grupo de empresas para fins administrativos internos, incluindo o tratamento de dados pessoais de clientes ou funcionários. Os princípios gerais que regem a transmissão de dados pessoais, no âmbito de um grupo empresarial, para uma empresa localizada num país terceiro mantêm-se inalterados.

(49) O tratamento de dados pessoais, na medida estritamente necessária e proporcionada para assegurar a segurança da rede e das informações, ou seja, a capacidade de uma rede ou de um sistema informático de resistir, com um dado nível de confiança, a eventos acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais conservados ou transmitidos, bem como a segurança dos serviços conexos oferecidos ou acessíveis através destas redes e sistemas, pelas autoridades públicas, equipas de intervenção em caso de emergências informáticas (CERT), equipas de resposta a incidentes no domínio da segurança informática (CSIRT), fornecedores ou redes de serviços de comunicações eletrónicas e por fornecedores de tecnologias e serviços de segurança, constitui um interesse legítimo do responsável pelo tratamento. Pode ser esse o caso quando o tratamento vise, por exemplo, impedir o acesso não autorizado a redes de comunicações eletrónicas e a distribuição de códigos maliciosos e pôr termo a ataques de «negação de serviço» e a danos causados aos sistemas de comunicações informáticas e eletrónicas.

(50) O tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais. Se o tratamento for necessário para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, o direito da União ou dos Estados-Membros pode determinar e definir as tarefas e finalidades para as quais o tratamento posterior deverá ser considerado compatível e lícito. As operações de tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, deverão ser consideradas tratamento lícito compatível. O fundamento jurídico previsto no direito da União ou dos Estados-Membros para o tratamento dos dados pessoais pode igualmente servir de fundamento jurídico para o tratamento posterior. A fim de apurar se a finalidade de uma nova operação de tratamento dos dados é ou não compatível com a finalidade para que os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento, após ter cumprido todos os requisitos para a licitude do tratamento inicial, deverá ter em atenção, entre outros aspetos, a existência de uma ligação entre a primeira finalidade e aquela a que se destina a nova operação de tratamento que se pretende efetuar, o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, baseadas na sua relação com o responsável pelo tratamento; a natureza dos dados pessoais; as consequências que o posterior tratamento dos dados pode ter para o seu titular; e a existência de garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas.

Caso o titular dos dados tenha dado o seu consentimento ou o tratamento se baseie em disposições do direito da União ou de um Estado-Membro que constituam uma medida necessária e proporcionada, numa sociedade democrática, para salvaguardar, em especial, os importantes objetivos de interesse público geral, o responsável pelo tratamento deverá ser autorizado a proceder ao tratamento posterior dos dados pessoais, independentemente da compatibilidade das finalidades. Em todo o caso, deverá ser garantida a aplicação dos princípios enunciados pelo presente regulamento e, em particular, a obrigação de informar o titular dos dados sobre essas outras finalidades e sobre os

seus direitos, incluindo o direito de se opor. A indicação pelo responsável pelo tratamento de eventuais atos criminosos ou ameaças à segurança pública e a transmissão dos dados pessoais pertinentes, em casos individuais ou em vários casos relativos ao mesmo ato criminoso ou ameaça à segurança pública, a uma autoridade competente deverão ser consideradas como sendo do interesse legítimo do responsável pelo tratamento. Todavia, deverá ser proibido proceder à transmissão no interesse legítimo do responsável pelo tratamento ou ao tratamento posterior de dados pessoais se a operação não for compatível com alguma obrigação legal, profissional ou outra obrigação vinculativa de confidencialidade.

(51) Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais.

(52) As derrogações à proibição de tratamento de categorias especiais de dados pessoais deverão ser igualmente permitidas quando estiverem previstas no direito da União ou dos Estados-Membros sujeitas a salvaguardas adequadas, de forma a proteger os dados pessoais e outros direitos fundamentais, casotal seja do interesse público, nomeadamente o tratamento de dados pessoais em matéria de direito laboral, de direito de proteção social, incluindo as pensões, e para fins de segurança, monitorização e alerta em matéria de saúde, prevenção ou controlo de doenças transmissíveis e outras ameaças graves para a saúde. Essas derrogações poderão ser previstas por motivos sanitários, incluindo de saúde pública e de gestão de serviços de saúde, designadamente para assegurar a qualidade e a eficiência em termos de custos dos procedimentos utilizados para regularizar os pedidos de prestações sociais e de serviços no quadro do regime de seguro de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos. Uma derrogação deverá também permitir o tratamento desses dados pessoais quando tal for necessário à declaração, ao exercício ou à defesa de um direito, independentemente de se tratar de um processo judicial ou de um processo administrativo ou extrajudicial.

(53) As categorias especiais de dados pessoais que merecem uma proteção mais elevada só deverão ser objeto de tratamento para fins relacionados com a saúde quando tal for necessário para

atingir os objetivos no interesse das pessoas singulares e da sociedade no seu todo, nomeadamente no contexto da gestão dos serviços e sistemas de saúde ou de ação social, incluindo o tratamento por parte da administração e das autoridades sanitárias centrais nacionais desses dados para efeitos de controlo da qualidade, informação de gestão e supervisão geral a nível nacional e local do sistema de saúde ou de ação social, assegurando a continuidade dos cuidados de saúde ou de ação social e da prestação de cuidados de saúde transfronteiras, ou para fins de segurança, monitorização e alerta em matéria de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos baseados no direito da União ou dos Estados-Membros e que têm de cumprir um objetivo, assim como para os estudos realizados no interesse público no domínio da saúde pública. Por conseguinte, o presente regulamento deverá estabelecer condições harmonizadas para o tratamento de categorias especiais de dados pessoais relativos à saúde, tendo em conta necessidades específicas, designadamente quando o tratamento desses dados for efetuado para determinadas finalidades ligadas à saúde por pessoas sujeitas a uma obrigação legal de sigilo profissional. O direito da União ou dos Estados-Membros deverá prever medidas específicas e adequadas com vista à defesa dos direitos fundamentais e dos dados pessoais das pessoas singulares. Os Estados-Membros deverão ser autorizados a manter ou introduzir outras condições, incluindo limitações, no que diz respeito ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde. Tal não deverá, no entanto, impedir a livre circulação de dados pessoais na União, quando essas condições se aplicam ao tratamento transfronteiriço desses dados.

(54) O tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados. Esse tratamento deverá ser objeto de medidas adequadas e específicas, a fim de defender os direitos e liberdades das pessoas singulares. Neste contexto, a noção de «saúde pública» deverá ser interpretada segundo a definição constante do Regulamento (CE) n.º 1338/2008 do Parlamento Europeu e do Conselho¹¹, ou seja, todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade. Tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores ou as companhias de seguros e entidades bancárias.

(55) Além disso, o tratamento de dados pessoais pelas autoridades públicas tendo em vista realizar os objetivos, consagrados no direito constitucional ou no direito internacional público, de associações religiosas oficialmente reconhecidas, é efetuado por motivos de interesse público.

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

(57) Se os dados pessoais tratados pelo responsável pelo tratamento não lhe permitirem identificar uma pessoa singular, aquele não deverá ser obrigado a obter informações suplementares para identificar o titular dos dados com o único objetivo de dar cumprimento a uma disposição do presente regulamento. Todavia, o responsável pelo tratamento não deverá recusar receber informações

¹¹ Regulamento (CE) n.º 1338/2008 do Parlamento Europeu e do Conselho, de 16 de dezembro de 2008, relativo às esta-

tísticas comunitárias sobre saúde pública e saúde e segurança no trabalho (JO L 354 de 31.12.2008, p. 70).

suplementares fornecidas pelo titular no intuito de apoiar o exercício dos seus direitos. A identificação deverá incluir a identificação digital do titular dos dados, por exemplo com recurso a um procedimento de autenticação com os mesmos dados de identificação usados pelo titular dos dados para aceder aos serviços do responsável pelo tratamento por via eletrónica.

(58) O princípio da transparência exige que qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado. Essas informações poderão ser fornecidas por via eletrónica, por exemplo num sítio web, quando se destinarem ao público. Isto é especialmente relevante em situações em que a proliferação de operadores e a complexidade tecnológica das práticas tornam difícil que o titular dos dados saiba e compreenda se, por quem e para que fins os seus dados pessoais estão a ser recolhidos, como no caso da publicidade por via eletrónica. Uma vez que as crianças merecem proteção específica, sempre que o tratamento lhes seja dirigido, qualquer informação e comunicação deverá estar redigida numa linguagem clara e simples que a criança compreenda facilmente.

(59) Deverão ser previstas regras para facilitar o exercício pelo titular dos dados dos direitos que lhe são conferidos ao abrigo do presente regulamento, incluindo procedimentos para solicitar e, sendo caso disso, obter a título gratuito, em especial, o acesso a dados pessoais, a sua retificação ou o seu apagamento e o exercício do direito de oposição. O responsável pelo tratamento deverá fornecer os meios necessários para que os pedidos possam ser apresentados por via eletrónica, em especial quando os dados sejam também tratados por essa via. O responsável pelo tratamento deverá ser obrigado a responder aos pedidos do titular dos dados sem demora injustificada e o mais tardar no prazo de um mês e expor as suas razões quando tiver intenção de recusar o pedido.

(60) Os princípios do tratamento equitativo e transparente exigem que o titular dos dados seja informado da operação de tratamento de dados e das suas finalidades. O responsável pelo tratamento deverá fornecer ao titular as informações adicionais necessárias para assegurar um tratamento equitativo e transparente tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais forem tratados. O titular dos dados deverá também ser informado da definição de perfis e das consequências que daí advêm. Sempre que os dados pessoais forem recolhidos junto do titular dos dados, este deverá ser também informado da eventual obrigatoriedade de fornecer os dados pessoais e das consequências de não os facultar. Essas informações podem ser fornecidas em combinação com ícones normalizados a fim de dar, de modo facilmente visível, inteligível e claramente legível uma útil perspetiva geral do tratamento previsto. Se forem apresentados por via eletrónica, os ícones deverão ser de leitura automática.

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

(62) Todavia, não é necessário impor a obrigação de fornecer informações caso o titular dos dados já disponha da informação, caso a lei disponha expressamente o registo ou a comunicação dos dados pessoais ou caso a informação ao titular dos dados se revele impossível de concretizar ou

implicar um esforço desproporcionado. Este último seria, nomeadamente, o caso de um tratamento efetuado para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos. Para esse efeito, deverá ser considerado o número de titulares de dados, a antiguidade dos dados e as devidas garantias que tenham sido adotadas.

(63) Os titulares de dados deverão ter o direito de aceder aos dados pessoais recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de conhecer e verificar a tomar conhecimento do tratamento e verificar a sua licitude. Aqui se inclui o seu direito de acederem a dados sobre a sua saúde, por exemplo os dados dos registos médicos com informações como diagnósticos, resultados de exames, avaliações dos médicos e quaisquer intervenções ou tratamentos realizados. Por conseguinte, cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências. Quando possível, o responsável pelo tratamento deverá poder facultar o acesso a um sistema seguro por via eletrónica que possibilite ao titular aceder diretamente aos seus dados pessoais. Esse direito não deverá prejudicar os direitos ou as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o software. Todavia, essas considerações não deverão resultar na recusa de prestação de todas as informações ao titular dos dados. Quando o responsável proceder ao tratamento de grande quantidade de informação relativa ao titular dos dados, deverá poder solicitar que, antes de a informação ser fornecida, o titular especifique a que informações ou a que atividades de tratamento se refere o seu pedido.

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

(65) Os titulares dos dados deverão ter direito a que os dados que lhes digam respeito sejam retificados e o «direito a serem esquecidos» quando a conservação desses dados violar o presente regulamento ou o direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento. Em especial, os titulares de dados deverão ter direito a que os seus dados pessoais sejam apagados e deixem de ser objeto de tratamento se deixarem de ser necessários para a finalidade para a qual foram recolhidos ou tratados, se os titulares dos dados retirarem o seu consentimento ou se opuserem ao tratamento de dados pessoais que lhes digam respeito ou se o tratamento dos seus dados pessoais não respeitar o disposto no presente regulamento. Esse direito assume particular importância quando o titular dos dados tiver dado o seu consentimento quando era criança e não estava totalmente ciente dos riscos inerentes ao tratamento, e mais tarde deseje suprimir esses dados pessoais, especialmente na Internet. O titular dos dados deverá ter a possibilidade de exercer esse direito independentemente do facto de já ser adulto. No entanto, o prolongamento da conservação dos dados pessoais deverá ser efetuado de forma lícita quando tal se revele necessário para o exercício do direito de liberdade de expressão e informação, para o cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, por razões de interesse público no domínio da saúde pública, para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

(66) Para reforçar o direito a ser esquecido no ambiente por via eletrónica, o âmbito do direito ao apagamento deverá ser alargado através da imposição ao responsável pelo tratamento que

tenha tornado públicos os dados pessoais da adoção de medidas razoáveis, incluindo a aplicação de medidas técnicas, para informar os responsáveis que estejam a tratar esses dados pessoais de que os titulares dos dados solicitaram a supressão de quaisquer ligações para esses dados pessoais ou de cópias ou reproduções dos mesmos. Ao fazê-lo, esse responsável pelo tratamento deverá adotar as medidas que se afigurarem razoáveis, tendo em conta a tecnologia disponível e os meios ao seu dispor, incluindo medidas técnicas, para informar do pedido do titular dos dados pessoais os responsáveis que estejam a tratar os dados.

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

(68) Para reforçar o controlo sobre os seus próprios dados, sempre que o tratamento de dados pessoais for automatizado, o titular dos dados deverá ser autorizado a receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo tratamento num formato estruturado, de uso corrente, de leitura automática e interoperável, e a transmiti-los a outro responsável. Os responsáveis pelo tratamento de dados deverão ser encorajados a desenvolver formatos interoperáveis que permitam a portabilidade dos dados. Esse direito deverá aplicar-se também se o titular dos dados tiver fornecido os dados pessoais com base no seu consentimento ou se o tratamento for necessário para o cumprimento de um contrato. Não deverá ser aplicável se o tratamento se basear num fundamento jurídico que não seja o consentimento ou um contrato. Por natureza própria, esse direito não deverá ser exercido em relação aos responsáveis pelo tratamento que tratem dados pessoais na prossecução das suas atribuições públicas. Por conseguinte, esse direito não deverá ser aplicável quando o tratamento de dados pessoais for necessário para o cumprimento de uma obrigação jurídica à qual o responsável esteja sujeito, para o exercício de atribuições de interesse público ou para o exercício da autoridade pública de que esteja investido o responsável pelo tratamento. O direito do titular dos dados a transmitir ou receber dados pessoais que lhe digam respeito não deverá implicar para os responsáveis pelo tratamento a obrigação de adotar ou manter sistemas de tratamento que sejam tecnicamente compatíveis. Quando um determinado conjunto de dados pessoais disser respeito a mais de um titular, o direito de receber os dados pessoais não deverá prejudicar os direitos e liberdades de outros titulares de dados nos termos do presente regulamento. Além disso, esse direito também não deverá prejudicar o direito dos titulares dos dados a obter o apagamento dos dados pessoais nem as restrições a esse direito estabelecidas no presente regulamento e, nomeadamente, não deverá implicar o apagamento dos dados pessoais relativos ao titular que este tenha fornecido para execução de um contrato, na medida em que e enquanto os dados pessoais forem necessários para a execução do referido contrato. Sempre que seja tecnicamente possível, o titular dos dados deverá ter o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento.

(69) No caso de um tratamento de dados pessoais lícito realizado por ser necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento ou ainda por motivos de interesse legítimo do responsável pelo tratamento ou de terceiros, o titular não deverá deixar de ter o direito de se opor ao tratamento dos dados pessoais que digam respeito à sua situação específica. Deverá caber ao responsável pelo tratamento

provar que os seus interesses legítimos imperiosos prevalecem sobre os interesses ou direitos e liberdades fundamentais do titular dos dados.

(70) Sempre que os dados pessoais forem objeto de tratamento para efeitos de comercialização direta, o titular deverá ter o direito de se opor, em qualquer momento e gratuitamente, a tal tratamento, incluindo a definição de perfis na medida em que esteja relacionada com a referida comercialização, quer se trate do tratamento inicial quer do tratamento posterior. Esse direito deverá ser explicitamente levado à atenção do titular e apresentado de modo claro e distinto de quaisquer outras informações.

(71) O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar. No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. Essa medida não deverá dizer respeito a uma criança.

A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados, e evitar, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou que o tratamento dos dados resulte em medidas que venham a ter tais efeitos.»

(72) A definição de perfis está sujeita às regras do presente regulamento que regem o tratamento de dados pessoais, como o fundamento jurídico do tratamento ou os princípios da proteção de dados. O Comité Europeu para a Proteção de Dados criado pelo presente regulamento («Comité») deverá poder emitir orientações nesse âmbito.

(73) O direito da União ou dos Estados-Membros podem impor restrições relativas a princípios específicos e aos direitos de informação, acesso e retificação ou apagamento de dados pessoais

e ao direito à portabilidade dos dados, ao direito de oposição, às decisões baseadas na definição de perfis, bem como à comunicação de uma violação de dados pessoais ao titular dos dados, e a determinadas obrigações conexas dos responsáveis pelo tratamento, na medida em que sejam necessárias e proporcionadas numa sociedade democrática para garantir a segurança pública, incluindo a proteção da vida humana, especialmente em resposta a catástrofes naturais ou provocadas pelo homem, para a prevenção, a investigação e a repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública ou violações da deontologia de profissões regulamentadas, para outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, para a conservação de registos públicos por motivos de interesse público geral, para posterior tratamento de dados pessoais arquivados para a prestação de informações específicas relacionadas com o comportamento político no âmbito de antigos regimes totalitários ou para efeitos de defesa do titular dos dados ou dos direitos e liberdades de terceiros, incluindo a proteção social, a saúde pública e os fins humanitários. Essas restrições deverão respeitar as exigências estabelecidas na Carta e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.

(74) Deverá ser consagrada a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas. Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares.

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

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

(77) As orientações sobre a execução de medidas adequadas e sobre a comprovação de conformidade pelos responsáveis pelo tratamento ou subcontratantes, em especial no que diz respeito

à identificação dos riscos relacionados com o tratamento, à sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como à identificação das melhores práticas para a atenuação dos riscos, poderão ser obtidas nomeadamente recorrendo a códigos de conduta aprovados, a certificações aprovadas, às orientações fornecidas pelo Comité ou às indicações fornecidas por um encarregado da proteção de dados. O Comité poderá emitir igualmente orientações sobre operações de tratamento de dados que não sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares e indicar quais as medidas adequadas em tais casos para diminuir esse risco.

(78) A defesa dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige a adoção de medidas técnicas e organizativas adequadas, a fim de assegurar o cumprimento dos requisitos do presente regulamento. Para poder comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a conceção e da proteção de dados por defeito. Tais medidas podem incluir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança. No contexto do desenvolvimento, conceção, seleção e utilização de aplicações, serviços e produtos que se baseiam no tratamento de dados pessoais ou recorrem a este tratamento para executarem as suas funções, haverá que incentivar os fabricantes dos produtos, serviços e aplicações a ter em conta o direito à proteção de dados quando do seu desenvolvimento e conceção e, no devido respeito pelas técnicas mais avançadas, a garantir que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações em matéria de proteção de dados. Os princípios de proteção de dados desde a conceção e, por defeito, deverão também ser tomados em consideração no contexto dos contratos públicos.

(79) A defesa dos direitos e liberdades dos titulares dos dados, bem como a responsabilidade dos responsáveis pelo seu tratamento e dos subcontratantes, incluindo no que diz respeito à supervisão e às medidas adotadas pelas autoridades de controlo, exigem uma clara repartição das responsabilidades nos termos do presente regulamento, nomeadamente quando o responsável pelo tratamento determina as finalidades e os meios do tratamento conjuntamente com outros responsáveis, ou quando uma operação de tratamento de dados é efetuada por conta de um responsável pelo tratamento.

(80) Sempre que um responsável pelo tratamento ou um subcontratante não estabelecidos na União efetuarem o tratamento de dados pessoais de titulares de dados que se encontrem na União, e as suas atividades de tratamento estiverem relacionadas com a oferta de bens ou serviços a esses titulares de dados na União, independentemente de a estes ser exigido um pagamento, ou com o controlo do seu comportamento na medida que o seu comportamento tenha lugar na União, o responsável pelo tratamento ou o subcontratante deverão designar um representante, a não ser que o tratamento seja ocasional, não inclua o tratamento, em larga escala, de categorias especiais de dados pessoais, nem o tratamento de dados pessoais relativos a condenações penais e infrações, e não seja suscetível de implicar riscos para os direitos e liberdades das pessoas singulares, tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento ou se o responsável pelo tratamento for uma autoridade ou organismo público. O representante deverá agir em nome do responsável pelo tratamento ou do subcontratante e deverá poder ser contactado por qualquer autoridade de controlo. O representante deverá ser explicitamente designado por um mandato do responsável pelo tratamento ou do subcontratante, emitido por escrito, que permita ao representante agir em

seu nome no que diz respeito às obrigações que lhes são impostas pelo presente regulamento. A designação de um tal representante não afeta as responsabilidades que incumbem ao responsável pelo tratamento ou ao subcontratante nos termos do presente regulamento. O representante deverá executar as suas tarefas em conformidade com o mandato que recebeu do responsável pelo tratamento ou do subcontratante, incluindo no que toca à cooperação com as autoridades de controlo competentes relativamente a qualquer ação empreendida no sentido de garantir o cumprimento do presente regulamento. O representante designado deverá estar sujeito a procedimentos de execução em caso de incumprimento pelo responsável pelo tratamento ou pelo subcontratante.

(81) Para assegurar o cumprimento do presente regulamento no que se refere ao tratamento a efetuar pelo subcontratante por conta do responsável pelo tratamento, este, quando confiar atividades de tratamento a um subcontratante, deverá recorrer exclusivamente a subcontratantes que ofereçam garantias suficientes, especialmente em termos de conhecimentos especializados, fiabilidade e recursos, quanto à execução de medidas técnicas e organizativas que cumpram os requisitos do presente regulamento, nomeadamente no que se refere à segurança do tratamento. O facto de o subcontratante cumprir um código de conduta aprovado ou um procedimento de certificação aprovado poderá ser utilizado como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento. A realização de operações de tratamento de dados em subcontratação deverá ser regulada por um contrato ou por outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento e em que seja estabelecido o objeto e a duração do contrato, a natureza e as finalidades do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, tendo em conta as tarefas e responsabilidades específicas do subcontratante no contexto do tratamento a realizar e o risco em relação aos direitos e liberdades do titular dos dados. O responsável pelo tratamento e o subcontratante poderão optar por utilizar um contrato individual ou cláusulas contratuais-tipo que são adotadas quer diretamente pela Comissão quer por uma autoridade de controlo em conformidade com o procedimento de controlo da coerência e adotadas posteriormente pela Comissão. Após concluído o tratamento por conta do responsável pelo tratamento, o subcontratante deverá, consoante a escolha do primeiro, devolver ou apagar os dados pessoais, a menos que seja exigida a conservação dos dados pessoais ao abrigo do direito da União ou do Estado-Membro a que o subcontratante está sujeito.

(82) A fim de comprovar a observância do presente regulamento, o responsável pelo tratamento ou o subcontratante deverá conservar registos de atividades de tratamento sob a sua responsabilidade. Os responsáveis pelo tratamento e subcontratantes deverão ser obrigados a cooperar com a autoridade de controlo e a facultar-lhe esses registos, a pedido, para fiscalização dessas operações de tratamento.

(83) A fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem. Essas medidas deverão assegurar um nível de segurança adequado, nomeadamente a confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função dos riscos e da natureza dos dados pessoais a proteger. Ao avaliar os riscos para a segurança dos dados, deverão ser tidos em conta os riscos apresentados pelo tratamento dos dados pessoais, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais.

(84) A fim de promover o cumprimento do presente regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liber-

dades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco. Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais.

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

(86) O responsável pelo tratamento deverá informar, sem demora injustificada, o titular dos dados da violação de dados pessoais quando for provável que desta resulte um elevado risco para os direitos e liberdades da pessoa singular, a fim de lhe permitir tomar as precauções necessárias. A comunicação deverá descrever a natureza da violação de dados pessoais e dirigir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos. Essa comunicação aos titulares dos dados deverá ser efetuada logo que seja razoavelmente possível, em estreita cooperação com a autoridade de controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia. Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá uma pronta comunicação aos titulares dos dados, mas a necessidade de aplicar medidas adequadas contra violações de dados pessoais recorrentes ou similares poderá justificar um período mais alargado para a comunicação.

(87) Há que verificar se foram aplicadas todas as medidas tecnológicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação de dados pessoais e para informar rapidamente a autoridade de controlo e o titular. Para comprovar que a notificação foi enviada sem demora injustificada importa ter em consideração, em especial, a natureza e a gravidade da violação dos dados pessoais e as respetivas consequências e efeitos adversos para o titular dos dados. Essa notificação poderá resultar numa intervenção da autoridade de controlo em conformidade com as suas funções e competências, definidas pelo presente regulamento.

(88) Ao estabelecer regras pormenorizadas relativamente ao formato e aos procedimentos aplicáveis à notificação das violações de dados pessoais, deverá ter-se devidamente em conta as circunstâncias dessa violação, nomeadamente a existência ou não de proteção dos dados pessoais através de medidas técnicas de proteção adequadas para reduzir eficazmente a probabilidade de usurpação da identidade ou outras formas de utilização abusiva. Além disso, tais regras e procedimentos deverão ter em conta os legítimos interesses das autoridades de polícia nos casos em que a divulgação precoce

de informações possa dificultar desnecessariamente a investigação das circunstâncias da violação de dados pessoais.

(89) A Diretiva 95/46/CE estabelece uma obrigação geral de notificação do tratamento de dados pessoais às autoridades de controlo. Além de esta obrigação originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais. Tais obrigações gerais e indiscriminadas de notificação deverão, por isso, ser suprimidas e substituídas por regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades. Os referidos tipos de operações de tratamento poderão, nomeadamente, envolver a utilização de novas tecnologias, ou pertencer a um novo tipo e não ter sido antecedidas por uma avaliação de impacto sobre a proteção de dados por parte do responsável pelo tratamento, ou ser consideradas necessárias à luz do período decorrido desde o tratamento inicial responsável pelo tratamento.

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

(91) Tal deverá aplicar-se, nomeadamente, às operações de tratamento de grande escala que visem o tratamento de uma grande quantidade de dados pessoais a nível regional, nacional ou supranacional, possam afetar um número considerável de titulares de dados e sejam suscetíveis de implicar um elevado risco, por exemplo, em razão da sua sensibilidade, nas quais, em conformidade com o nível de conhecimentos tecnológicos alcançado, seja utilizada em grande escala uma nova tecnologia, bem como a outras operações de tratamento que impliquem um elevado risco para os direitos e liberdades dos titulares dos dados, em especial quando tais operações dificultem aos titulares o exercício dos seus direitos. Dever-se-á realizar também uma avaliação de impacto sobre a proteção de dados nos casos em que os dados pessoais são tratados para tomar decisões relativas a determinadas pessoas singulares na sequência de qualquer avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares baseada na definição dos perfis desses dados ou na sequência do tratamento de categorias especiais de dados pessoais, de dados biométricos ou de dados sobre condenações penais e infrações ou medidas de segurança conexas. É igualmente exigida uma avaliação do impacto sobre a proteção de dados para o controlo de zonas acessíveis ao público em grande escala, nomeadamente se forem utilizados mecanismos optoeletrónicos, ou para quaisquer outras operações quando a autoridade de controlo competente considere que o tratamento é suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos direitos, em especial por impedirem estes últimos de exercer um direito ou de utilizar um serviço ou um contrato, ou por serem realizadas sistematicamente em grande escala. O tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado. Nesses casos, a realização de uma avaliação de impacto sobre a proteção de dados não deverá ser obrigatória.

(92) Em certas circunstâncias pode ser razoável e económico alargar a avaliação de impacto sobre a proteção de dados para além de um projeto único, por exemplo se as autoridades ou organismos públicos pretenderem criar uma aplicação ou uma plataforma de tratamento comum, ou se vários responsáveis pelo tratamento planearem criar uma aplicação ou um ambiente de tratamento

comum em todo um setor ou segmento profissional, ou uma atividade horizontal amplamente utilizada.

(93) No contexto da adoção da legislação dos Estados-Membros que regula a prossecução das atribuições da autoridade ou do organismo público, bem como a operação ou o conjunto de operações em questão, os Estados-Membros podem considerar necessário proceder à avaliação antes de iniciar as atividades de tratamento.

(94) Sempre que uma avaliação de impacto relativa à proteção de dados indicar que o tratamento, na falta de garantias e de medidas e procedimentos de segurança para atenuar os riscos, implica um elevado risco para os direitos e liberdades das pessoas singulares e o responsável pelo tratamento considerar que o risco não poderá ser atenuado através de medidas razoáveis, atendendo à tecnologia disponível e aos custos de aplicação, a autoridade de controlo deverá ser consultada antes de as atividades de tratamento terem início. Provavelmente, esse elevado risco decorre de determinados tipos de tratamento e da extensão e frequência do tratamento, que podem originar igualmente danos ou interferir com os direitos e liberdades da pessoa singular. A autoridade de controlo deverá responder ao pedido de consulta dentro de um determinado prazo. Contudo, a ausência de reação da autoridade de controlo no decorrer desse prazo não prejudicará qualquer intervenção que esta autoridade venha a fazer em conformidade com as suas funções e competências, definidas pelo presente regulamento, incluindo a competência para proibir certas operações de tratamento. No âmbito desse processo de consulta, o resultado de uma avaliação do impacto sobre a proteção de dados efetuada relativamente ao tratamento em questão pode ser apresentado à autoridade de controlo, em especial as medidas previstas para atenuar o risco para os direitos e liberdades das pessoas singulares.

(95) O subcontratante deverá prestar assistência ao responsável pelo tratamento, se necessário e a pedido deste, para assegurar o cumprimento das obrigações decorrentes da realização de avaliações do impacto sobre a proteção de dados e da consulta prévia à autoridade de controlo.

(96) Deverá ter também lugar uma consulta à autoridade de controlo durante os trabalhos de elaboração de uma medida legislativa ou regulamentar que preveja o tratamento de dados pessoais, de modo a assegurar a conformidade do tratamento pretendido com o presente regulamento e, em particular, a atenuar o respetivo risco para o titular dos dados.

(97) Sempre que o tratamento dos dados for efetuado por uma autoridade pública, com exceção dos tribunais ou de autoridades judiciais independentes no exercício da sua função jurisdicional, sempre que, no setor privado, for efetuado por um responsável pelo tratamento cujas atividades principais consistam em operações de tratamento que exijam o controlo regular e sistemático do titular dos dados em grande escala, ou sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados pessoais e de dados relacionados com condenações penais e infrações, o responsável pelo tratamento destes ou o subcontratante pode ser assistido por um especialista em legislação e prática de proteção de dados no controlo do cumprimento do presente regulamento a nível interno. No setor privado, as atividades principais do responsável pelo tratamento dizem respeito às suas atividades primárias e não estão relacionadas com o tratamento de dados pessoais como atividade auxiliar. O nível necessário de conhecimentos especializados deverá ser determinado, em particular, em função do tratamento de dados realizado e da proteção exigida para os dados pessoais tratados pelo responsável pelo seu tratamento ou pelo subcontratante. Estes encarregados da proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência.

(98) As associações ou outras entidades que representem categorias de responsáveis pelo tratamento ou de subcontratantes deverão ser incentivadas a elaborar códigos de conduta, no respeito do

presente regulamento, com vista a facilitar a sua aplicação efetiva, tendo em conta as características específicas do tratamento efetuado em determinados setores e as necessidades específicas das micro, pequenas e médias empresas. Esses códigos de conduta poderão nomeadamente regular as obrigações dos responsáveis pelo tratamento e dos subcontratantes, tendo em conta o risco que poderá resultar do tratamento dos dados no que diz respeito aos direitos e às liberdades das pessoas singulares.

(99) Durante o processo de elaboração de um código de conduta, ou na sua alteração ou aditamento, as associações e outros organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes deverão consultar as partes interessadas, nomeadamente os titulares dos dados, se possível, e ter em conta os contributos recebidos e as opiniões expressas em resposta a essas consultas.

(100) A fim de reforçar a transparência e o cumprimento do presente regulamento, deverá ser encorajada a criação de procedimentos de certificação e selos e marcas de proteção de dados, que permitam aos titulares avaliar rapidamente o nível de proteção de dados proporcionado pelos produtos e serviços em causa.

(101) A circulação de dados pessoais, com origem e destino quer a países não pertencentes à União quer a organizações internacionais, é necessária ao desenvolvimento do comércio e da cooperação internacionais. O aumento dessa circulação criou novos desafios e novas preocupações em relação à proteção dos dados pessoais. Todavia, quando os dados pessoais são transferidos da União para responsáveis pelo tratamento, para subcontratantes ou para outros destinatários em países terceiros ou para organizações internacionais, o nível de proteção das pessoas singulares assegurado na União pelo presente regulamento deverá continuar a ser garantido, inclusive nos casos de posterior transferência de dados pessoais do país terceiro ou da organização internacional em causa para responsáveis pelo tratamento, subcontratantes desse país terceiro ou de outro, ou para uma organização internacional. Em todo o caso, as transferências para países terceiros e organizações internacionais só podem ser efetuadas no pleno respeito pelo presente regulamento. Só poderão ser realizadas transferências se, sob reserva das demais disposições do presente regulamento, as condições constantes das disposições do presente regulamento relativas a transferências de dados pessoais para países terceiros e organizações internacionais forem cumpridas pelo responsável pelo tratamento ou subcontratante.

(102) O presente regulamento não prejudica os acordos internacionais celebrados entre a União Europeia e países terceiros que regulem a transferência de dados pessoais, incluindo as garantias adequadas em benefício dos titulares dos dados. Os Estados-Membros poderão celebrar acordos internacionais que impliquem a transferência de dados pessoais para países terceiros ou organizações internacionais, desde que tais acordos não afetem o presente regulamento ou quaisquer outras disposições do direito da União e prevejam um nível adequado de proteção dos direitos fundamentais dos titulares dos dados.

(103) A Comissão pode decidir, com efeitos no conjunto da União, que um país terceiro, um território ou um setor determinado de um país terceiro, ou uma organização internacional, oferece um nível adequado de proteção de dados adequado, garantindo assim a segurança jurídica e a uniformidade ao nível da União relativamente ao país terceiro ou à organização internacional que seja considerado apto a assegurar tal nível de proteção. Nestes casos, podem realizar-se transferências de dados pessoais para esse país ou organização internacional sem que para tal seja necessária mais nenhuma autorização. A Comissão pode igualmente decidir, após enviar ao país terceiro ou organização internacional uma notificação e uma declaração completa dos motivos, revogar essa decisão.

(104) Em conformidade com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou setor específico de um país terceiro, ter em consideração em que medida esse país

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

(105) Além dos compromissos internacionais assumidos pelo país terceiro ou pela organização internacional, a Comissão deverá ter em conta as obrigações decorrentes da participação do país terceiro ou da organização internacional nos sistemas multilaterais ou regionais, em especial no que diz respeito à proteção dos dados pessoais, bem como o cumprimento de tais obrigações. Em especial, há que ter em conta a adesão do país terceiro em causa à Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, de 28 de janeiro de 1981, e ao seu Protocolo Adicional. A Comissão deverá consultar o Comité quando avaliar o nível de proteção nos países terceiros ou organizações internacionais.

(106) A Comissão deverá controlar a eficácia das decisões sobre o nível de proteção assegurado num país terceiro, num território ou num setor específico de um país terceiro, ou numa organização internacional, e acompanhar a eficácia das decisões adotadas com base no artigo 25.º, n.º 6, ou no artigo 26.º, n.º 4, da Diretiva 95/46/CE. Nas suas decisões de adequação, a Comissão deverá prever um procedimento de avaliação periódica da aplicação destas. Essa revisão periódica deverá ser feita em consulta com o país terceiro ou a organização internacional em questão e ter em conta todos os desenvolvimentos pertinentes verificados no país terceiro ou organização internacional. Para efeitos de controlo e de realização das revisões periódicas, a Comissão deverá ter em consideração os pontos de vista e as conclusões a que tenham chegado o Parlamento Europeu e o Conselho, bem como outros organismos e fontes pertinentes. A Comissão deverá avaliar, num prazo razoável, a eficácia destas últimas decisões e comunicar quaisquer resultados pertinentes ao comité na aceção do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho¹², tal como estabelecido no presente regulamento, ao Parlamento Europeu e ao Conselho.

(107) A Comissão pode reconhecer que um país terceiro, um território ou um setor específico de um país terceiro, ou uma organização internacional, deixou de assegurar um nível adequado de proteção de dados. Por conseguinte, deverá ser proibida a transferência de dados pessoais para esse país terceiro ou organização internacional, a menos que sejam cumpridos os requisitos constantes do presente regulamento relativos a transferências sujeitas a garantias adequadas, incluindo regras vinculativas aplicáveis às empresas, e derrogações para situações específicas. Nesse caso, deverão ser tomadas medidas que visem uma consulta entre a Comissão e esse país terceiro ou organização internacional. A Comissão deverá, em tempo útil, informar o país terceiro ou a organização inter-

¹² 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 con-

trolo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).

nacional das razões da proibição e iniciar consultas com o país ou organização em causa, a fim de corrigir a situação.

(108) Na falta de uma decisão sobre o nível de proteção adequado, o responsável pelo tratamento ou o subcontratante deverá adotar as medidas necessárias para colmatar a insuficiência da proteção de dados no país terceiro dando para tal garantias adequadas ao titular dos dados. Tais garantias adequadas podem consistir no recurso a regras vinculativas aplicáveis às empresas, cláusulas-tipo de proteção de dados adotadas pela Comissão, cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo, ou cláusulas contratuais autorizadas por esta autoridade. Essas medidas deverão assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da União, incluindo a existência de direitos do titular de dados e de medidas jurídicas corretivas eficazes, nomeadamente o direito de recurso administrativo ou judicial e de exigir indemnização, quer no território da União quer num país terceiro. Deverão estar relacionadas, em especial, com o respeito pelos princípios gerais relativos ao tratamento de dados pessoais e pelos princípios de proteção de dados desde a conceção e por defeito. Também podem ser efetuadas transferências por autoridades ou organismos públicos para autoridades ou organismos públicos em países terceiros ou para organizações internacionais que tenham deveres e funções correspondentes, nomeadamente com base em disposições a inserir no regime administrativo, como seja um memorando de entendimento, que prevejam a existência de direitos efetivos e oponíveis dos titulares dos dados. Deverá ser obtida a autorização da autoridade de controlo competente quando as garantias previstas em regimes administrativos não forem juridicamente vinculativas.

(109) A possibilidade de o responsável pelo tratamento ou o subcontratante utilizarem cláusulas-tipo de proteção de dados adotadas pela Comissão ou por uma autoridade de controlo não os deverá impedir de incluírem estas cláusulas num contrato mais abrangente, como um contrato entre o subcontratante e outro subcontratante, nem de acrescentarem outras cláusulas ou garantias adicionais desde que não entrem, direta ou indiretamente, em contradição com as cláusulas contratuais-tipo adotadas pela Comissão ou por uma autoridade de controlo, e sem prejuízo dos direitos ou liberdades fundamentais dos titulares dos dados. Os responsáveis pelo tratamento e os subcontratantes deverão ser encorajados a apresentar garantias suplementares através de compromissos contratuais que complementem as cláusulas-tipo de proteção.

(110) Os grupos empresariais ou os grupos de empresas envolvidas numa atividade económica conjunta deverão poder utilizar as regras vinculativas aplicáveis às empresas aprovadas para as suas transferências internacionais da União para entidades pertencentes ao mesmo grupo empresarial ou grupo de empresas envolvidas numa atividade económica conjunta, desde que essas regras incluam todos os princípios essenciais e direitos oponíveis que visem assegurar garantias adequadas às transferências ou categorias de transferências de dados pessoais.

(111) Deverá prever-se a possibilidade de efetuar transferências em determinadas circunstâncias em que o titular dos dados dê o seu consentimento explícito, em que a transferência seja ocasional e necessária em relação a um contrato ou a um contencioso judicial, independentemente de se tratar de um processo judicial, de um processo administrativo ou de um qualquer procedimento não judicial, incluindo procedimentos junto de organismos de regulação. Deverá também estar prevista a possibilidade de efetuar transferências no caso de motivos importantes de interesse público previstos pelo direito da União ou de um Estado-Membro o exigirem, ou se a transferência for efetuada a partir de um registo criado por lei e destinado à consulta por parte do público ou de pessoas com um interesse legítimo. Neste último caso, a transferência não deverá abranger a totalidade dos dados nem categorias completas de dados pessoais contidos nesse registo e, quando este último se destinar

a ser consultado por pessoas com um interesse legítimo, a transferência apenas deverá ser efetuada a pedido dessas pessoas ou, caso sejam os seus destinatários, tendo plenamente em conta os interesses e os direitos fundamentais do titular dos dados.

(112) Essas derrogações deverão ser aplicáveis, em especial, às transferências de dados exigidas e necessárias por razões importantes de interesse público, por exemplo em caso de intercâmbio internacional de dados entre autoridades de concorrência, administrações fiscais ou aduaneiras, entre autoridades de supervisão financeira, entre serviços competentes em matéria de segurança social ou de saúde pública, por exemplo em caso de localização de contactos no que respeita a doenças contagiosas ou para reduzir e/ou eliminar a dopagem no desporto. Deverá igualmente ser considerada legal uma transferência de dados pessoais que seja necessária para a proteção de um interesse essencial para os interesses vitais do titular dos dados ou de outra pessoa, nomeadamente a integridade física ou a vida, se o titular dos dados estiver impossibilitado de dar o seu consentimento. Na falta de uma decisão de adequação, o direito da União ou de um Estado-Membro pode, por razões importantes de interesse público, estabelecer expressamente limites à transferência de categorias específicas de dados para países terceiros ou organizações internacionais. Os Estados-Membros deverão notificar essas decisões nacionais à Comissão. As transferências, para uma organização humanitária internacional, de dados pessoais de um titular que seja física ou legalmente incapaz de dar o seu consentimento, com vista ao desempenho de missões, ao abrigo das Convenções de Genebra ou para cumprir o direito internacional humanitário aplicável aos conflitos armados, poderão ser consideradas necessárias por uma razão importante de interesse público ou por ser do interesse vital do titular dos dados.

(113) As transferências que possam ser classificadas como não repetitivas e que apenas digam respeito a um número limitado de titulares de dados podem igualmente ser admitidas para efeitos dos interesses legítimos imperiosos visados pelo responsável pelo tratamento, desde que a tais interesses não se sobreponham os interesses ou os direitos e liberdades do titular dos dados e desde que o responsável pelo tratamento destes tenha avaliado todas as circunstâncias associadas à operação de transferência. O responsável pelo tratamento deverá atender especialmente à natureza dos dados pessoais, à finalidade e à duração da operação ou operações de tratamento previstas, bem como à situação vigente no país de origem, no país terceiro e no país de destino final, e deverá apresentar as garantias adequadas para defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento dos seus dados pessoais. Tais transferências só deverão ser possíveis em raros casos em que não se aplique nenhum dos outros motivos de transferência. Para fins de investigação científica ou histórica ou fins estatísticos, deverão ser tidas em consideração as expectativas legítimas da sociedade em matéria de avanço do conhecimento. O responsável pelo tratamento deverá informar da transferência a autoridade de controlo e o titular dos dados.

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

(115) Alguns países terceiros aprovam leis, regulamentos e outros atos normativos destinados a regular diretamente as atividades de tratamento pelas pessoas singulares e coletivas sob a jurisdição dos Estados-Membros. Pode ser o caso de sentenças de órgãos jurisdicionais ou de decisões de autoridades administrativas de países terceiros que exijam que o responsável pelo tratamento ou subcontratante transfira ou divulgue dados pessoais sem fundamento em nenhum acordo internacional, como seja um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União ou um dos Estados-Membros. Em virtude da sua aplicabilidade extraterritorial, essas

leis, regulamentos e outros atos normativos podem violar o direito internacional e obstar à realização do objetivo de proteção das pessoas singulares, assegurado na União Europeia pelo presente regulamento. As transferências só deverão ser autorizadas quando estejam preenchidas as condições estabelecidas pelo presente regulamento para as transferências para os países terceiros. Pode ser esse o caso, nomeadamente, sempre que a divulgação for necessária por um motivo importante de interesse público, reconhecido pelo direito da União ou dos Estados-Membros ao qual o responsável pelo tratamento está sujeito.

(116) Sempre que dados pessoais atravessarem fronteiras fora do território da União, aumenta o risco de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem da utilização ilegal ou da divulgação dessas informações. Paralelamente, as autoridades de controlo podem ser incapazes de dar seguimento a reclamações ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras. Os seus esforços para colaborar no contexto transfronteiras podem ser também restringidos por poderes preventivos ou medidas de reparação insuficientes, regimes jurídicos incoerentes e obstáculos práticos, tais como a limitação de recursos. Por conseguinte, revela-se necessário promover uma cooperação mais estreita entre as autoridades de controlo da proteção de dados, a fim de que possam efetuar o intercâmbio de informações e realizar investigações com as suas homólogas internacionais. Para efeitos de criação de regras de cooperação internacional que facilitem e proporcionem assistência mútua internacional para a aplicação da legislação de proteção de dados pessoais, a Comissão e as autoridades de controlo deverão trocar informações e colaborar com as autoridades competentes de países terceiros em atividades relacionadas com o exercício dos seus poderes, com base na reciprocidade e em conformidade com o presente regulamento.

(117) A criação de autoridades de controlo nos Estados-Membros, habilitadas a desempenhar as suas funções e a exercer os seus poderes com total independência, constitui um elemento essencial da proteção das pessoas singulares no que respeita ao tratamento dos seus dados pessoais. Os Estados-Membros deverão poder criar mais do que uma autoridade de controlo, de modo a refletir a sua estrutura constitucional, organizacional e administrativa.

(118) A independência das autoridades de controlo não deverá implicar que estas autoridades não possam ser sujeitas a procedimentos de controlo ou monitorização no que diz respeito às suas despesas nem a fiscalização judicial.

(119) Os Estados-Membros que criem várias autoridades de controlo deverão prever na sua legislação procedimentos que garantam a participação efetiva dessas mesmas autoridades no procedimento de controlo da coerência. Esses Estados-Membros deverão, em particular, designar a autoridade de controlo que servirá de ponto de contacto único, para permitir a participação efetiva dessas autoridades no referido procedimento, a fim de assegurar uma cooperação rápida e fácil com outras autoridades de controlo, com o Comité e com a Comissão.

(120) Deverão ser dados às autoridades de controlo os recursos financeiros e humanos, as instalações e as infraestruturas necessárias ao desempenho eficaz das suas atribuições, incluindo as relacionadas com a assistência e a cooperação mútuas com outras autoridades de controlo da União. As autoridades de controlo deverão ter orçamentos anuais públicos separados, que poderão estar integrados no orçamento geral do Estado ou nacional.

(121) As condições gerais aplicáveis aos membros da autoridade de controlo deverão ser definidas por lei em cada Estado-Membro e deverão prever, em especial, que os referidos membros sejam nomeados, com recurso a um processo transparente, pelo Parlamento, pelo Governo ou pelo Chefe de Estado do Estado-Membro com base numa proposta do Governo, de um dos seus membros, do Parlamento ou de uma sua câmara, ou por um organismo independente incumbido

da nomeação nos termos do direito do Estado-Membro. A fim de assegurar a independência da autoridade de controlo, os membros que a integram deverão exercer as suas funções com integridade, abster-se de qualquer ato incompatível com as mesmas e, durante o seu mandato, não deverão exercer nenhuma atividade, seja ou não remunerada, que com elas seja incompatível. A autoridade de controlo deverá dispor do seu próprio pessoal, selecionado por si mesma ou por um organismo independente criado nos termos do direito do Estado-Membro, que deverá estar exclusivamente sujeito à orientação do membro ou membros da autoridade de controlo.

(122) As autoridades de controlo deverão ser competentes no território do respetivo Estado-Membro para exercer os poderes e desempenhar as funções que lhes são conferidas nos termos do presente regulamento. Deverá ser abrangido, em especial, o tratamento de dados efetuado no contexto das atividades de um estabelecimento do responsável pelo tratamento ou do subcontratante no território do seu próprio Estado-Membro, o tratamento de dados pessoais efetuado por autoridades públicas ou por organismos privados que atuem no interesse público, o tratamento que afete os titulares de dados no seu território, ou o tratamento de dados efetuado por um responsável ou subcontratante não estabelecido na União quando diga respeito a titulares de dados residentes no seu território. Deverá ficar abrangido o tratamento de reclamações apresentadas por um titular de dados, a realização de investigações sobre a aplicação do presente regulamento e a promoção da sensibilização do público para os riscos, regras, garantias e direitos associados ao tratamento de dados pessoais.

(123) As autoridades de controlo deverão controlar a aplicação das disposições do presente regulamento e contribuir para a sua aplicação coerente em toda a União, a fim de proteger as pessoas singulares relativamente ao tratamento dos seus dados pessoais e facilitar a livre circulação desses dados a nível do mercado interno. Para esse efeito, as autoridades de controlo deverão cooperar entre si e com a Comissão, sem necessidade de qualquer acordo entre os Estados-Membros quer sobre a prestação de assistência mútua quer sobre tal cooperação.

(124) Quando o tratamento de dados pessoais ocorra no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante na União e o responsável pelo tratamento ou o subcontratante esteja estabelecido em vários Estados-Membros, ou quando o tratamento no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, na União, afete ou seja suscetível de afetar substancialmente titulares de dados em diversos Estados-Membros, a autoridade de controlo do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento ou do subcontratante deverá agir na qualidade de autoridade de controlo principal. Esta autoridade deverá cooperar com as outras autoridades interessadas, porque o responsável pelo tratamento ou o subcontratante tem um estabelecimento no território do seu Estado-Membro, porque há titulares de dados residentes no seu território que são substancialmente afetados, ou porque lhe foi apresentada uma reclamação. Além do mais, quando tenha sido apresentada uma reclamação por um titular de dados que não resida nesse Estado-Membro, a autoridade de controlo à qual a reclamação tiver sido apresentada deverá ser também autoridade de controlo interessada. No âmbito das suas funções de emissão de orientações sobre qualquer assunto relativo à aplicação do presente regulamento, o Comité deverá poder emitir orientações nomeadamente sobre os critérios a ter em conta para apurar se o tratamento em causa afeta substancialmente titulares de dados em mais do que um Estado-Membro e sobre aquilo que constitui uma objeção pertinente e fundamentada.

(125) A autoridade principal deverá ser competente para adotar decisões vinculativas relativamente a medidas que deem execução às competências que lhe tenham sido atribuídas nos termos do presente regulamento. Na sua qualidade de autoridade principal, a autoridade de controlo deverá implicar no processo decisório e coordenar as autoridades de controlo interessadas. Nos casos em que

a decisão consista em rejeitar no todo ou em parte a reclamação apresentada pelo titular dos dados, esta deverá ser adotada pela autoridade de controlo à qual a reclamação tenha sido apresentada.

(126) As decisões deverão ser acordadas conjuntamente pela autoridade de controlo principal e as autoridades de controlo interessadas e deverão visar o estabelecimento principal ou único do responsável pelo tratamento ou do subcontratante e ser vinculativas para ambos. O responsável pelo tratamento ou o subcontratante deverá tomar as medidas necessárias para assegurar o cumprimento do disposto no presente regulamento e a execução da decisão notificada pela autoridade de controlo principal ao estabelecimento principal do responsável pelo tratamento ou do subcontratante no que diz respeito às atividades de tratamento de dados na União.

(127) As autoridades de controlo que não atuem como autoridade de controlo principal deverão ter competência para tratar casos a nível local quando o responsável pelo tratamento ou subcontratante estiver estabelecido em vários Estados-Membros, mas o assunto do tratamento específico disser respeito unicamente ao tratamento efetuado num só Estado-Membro, e envolver somente titulares de dados nesse Estado-Membro, por exemplo, no caso de o assunto dizer respeito ao tratamento de dados pessoais de trabalhadores num contexto específico de emprego num Estado-Membro. Nesses casos, a autoridade de controlo deverá informar imediatamente do assunto a autoridade de controlo principal. Após ter sido informada, a autoridade de controlo principal decidirá se trata o caso de acordo com o disposto em matéria de cooperação entre a autoridade de controlo principal e a outra autoridade de controlo interessada («mecanismo de balcão único»), ou se deverá ser a autoridade de controlo que a informou a tratar o caso a nível local. Ao decidir se trata o caso, a autoridade de controlo principal deverá ter em conta se há algum estabelecimento do responsável pelo tratamento ou subcontratante no Estado-Membro da autoridade de controlo que a informou, a fim de garantir a eficaz execução da decisão relativamente ao responsável pelo tratamento ou subcontratante. Quando a autoridade de controlo principal decide tratar o caso, a autoridade de controlo que a informou deverá ter a possibilidade de apresentar um projeto de decisão, que a autoridade de controlo principal deverá ter na melhor conta quando prepara o seu projeto de decisão no âmbito desse mecanismo de balcão único.

(128) As regras relativas à autoridade de controlo principal e ao mecanismo de balcão único não se deverão aplicar quando o tratamento dos dados for efetuado por autoridades públicas ou organismos privados que atuem no interesse público. Em tais casos, a única autoridade de controlo competente para exercer as competências que lhe são conferidas nos termos do presente regulamento deverá ser a autoridade de controlo do Estado-Membro em que estiver estabelecida tal autoridade pública ou organismo privado.

(129) A fim de assegurar o controlo e a aplicação coerentes do presente regulamento em toda a União, as autoridades de controlo deverão ter, em cada Estado-Membro, as mesmas funções e poderes efetivos, incluindo poderes de investigação, poderes de correção e de sanção, e poderes consultivos e de autorização, nomeadamente em caso de reclamação apresentada por pessoas singulares, sem prejuízo dos poderes das autoridades competentes para o exercício da ação penal ao abrigo do direito do Estado-Membro, tendo em vista levar as violações ao presente regulamento ao conhecimento das autoridades judiciais e intervir em processos judiciais. Essas competências deverão incluir o poder de impor uma limitação temporário ou definitiva ao tratamento, ou mesmo a sua proibição. Os Estados-Membros podem estabelecer outras funções relacionadas com a proteção de dados pessoais ao abrigo do presente regulamento. Os poderes das autoridades de controlo deverão ser exercidos em conformidade com as garantias processuais adequadas previstas no direito da União e do Estado-Membro, com imparcialidade, com equidade e num prazo razoável. Em particular, cada medida deverá ser adequada, necessária e proporcionada a fim de garantir a conformidade com o presente regulamento, tendo em conta as circunstâncias de cada caso concreto, respeitar o direito

de todas as pessoas a serem ouvidas antes de ser tomada qualquer medida individual que as prejudique, e evitar custos supérfluos e inconvenientes excessivos para as pessoas em causa. Os poderes de investigação em matéria de acesso às instalações deverão ser exercidos em conformidade com os requisitos específicos do direito processual do Estado-Membro, como, por exemplo, a obrigação de obter autorização judicial prévia. As medidas juridicamente vinculativas da autoridade de controlo deverão ser emitidas por escrito, claras e inequívocas, indicar a autoridade de controlo que as emitiu e a data de emissão, ostentar a assinatura do diretor ou do membro da autoridade de controlo por eles autorizada, indicar os motivos que as justifica e mencionar o direito de recurso efetivo. Tal não deverá impedir que sejam estabelecidos requisitos suplementares nos termos do direito processual do Estado-Membro. A adoção de uma decisão juridicamente vinculativa pode dar origem a controlo jurisdicional nos Estados-Membros da autoridade de controlo que tenha adotado a decisão.

(130) Nos casos em que a autoridade de controlo a que a reclamação é apresentada não seja a principal, a autoridade de controlo principal deverá cooperar estreitamente com a autoridade de controlo à qual tiver sido apresentada a reclamação, de acordo com as disposições em matéria de cooperação e coerência do presente regulamento. Nestes casos, a autoridade de controlo principal, ao tomar medidas destinadas a produzir efeitos jurídicos, incluindo a imposição de coimas, deverá ter na melhor conta o parecer da autoridade de controlo à qual tiver sido apresentada a reclamação, que deverá continuar a ser competente para levar a cabo qualquer investigação no território do respetivo Estado-Membro, em ligação com a autoridade de controlo principal.

(131) Nos casos em que as funções de autoridade principal de controlo devessem ser exercidas por outra autoridade de controlo relativamente às atividades de tratamento do responsável pelo tratamento ou do subcontratante, mas em que o conteúdo concreto da reclamação ou a eventual violação diga respeito apenas às atividades de tratamento do responsável ou do subcontratante realizadas no Estado-Membro onde tenha sido apresentada a reclamação ou detetada a eventual infração, e o assunto não afete nem seja suscetível de afetar substancialmente titulares de dados noutros Estados-Membros, a autoridade de controlo que recebe uma reclamação, deteta ou é de outro modo informada de situações que impliquem eventuais violações do presente regulamento deverá procurar obter um acordo amigável. Se tal não lhe for possível, deverá exercer todos os poderes de que dispõe. Deverão ficar abrangidas: as atividades de tratamento específicas realizadas no território do Estado-Membro da autoridade de controlo ou que digam respeito a titulares de dados em território desse Estado-Membro; as atividades de tratamento realizadas no contexto de uma oferta de bens ou serviços destinados especificamente a titulares de dados no território do Estado-Membro da autoridade de controlo; ou as atividades de tratamento que tenham de ser analisadas tomando em consideração as obrigações legais aplicáveis ao abrigo do direito do Estado-Membro.

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

(133) As autoridades de controlo deverão prestar-se mutuamente assistência no desempenho das suas funções, por forma a assegurar a execução e aplicação coerentes do presente regulamento no mercado interno. A autoridade de controlo que solicite assistência mútua pode adotar uma medida provisória se não obtiver resposta relativamente a um pedido de assistência mútua no prazo de um mês a contar da receção desse pedido da outra autoridade de controlo.

(134) As autoridades de controlo deverão participar, sempre que for adequado, em operações conjuntas com outras autoridades de controlo. A autoridade de controlo requerida deverá ser obrigada a responder ao pedido num prazo determinado.

(135) A fim de assegurar a aplicação coerente do presente regulamento em toda a União, deverá ser criado um procedimento de controlo da coerência e para a cooperação entre as autoridades de controlo. Esse procedimento deverá ser aplicável, nomeadamente, quando uma autoridade de controlo tenciona adotar uma medida que vise produzir efeitos legais em relação a operações de tratamento que afetem substancialmente um número significativo de titulares de dados em vários Estados-Membros. Deverá aplicar-se igualmente sempre que uma autoridade de controlo interessada, ou a Comissão, solicitar que essa matéria seja tratada no âmbito do procedimento de controlo da coerência. Esse procedimento não deverá prejudicar medidas que a Comissão possa tomar no exercício das suas competências nos termos dos Tratados.

(136) Quando aplicar o procedimento de controlo da coerência, o Comité deverá emitir um parecer, num prazo determinado, se a maioria dos seus membros assim o decidir ou se tal lhe solicitado por qualquer autoridade de controlo interessada ou pela Comissão. O Comité deverá também ser habilitado a adotar decisões juridicamente vinculativas em caso de litígio entre as autoridades de controlo. Para esse efeito, deverá emitir, em princípio por maioria de dois terços dos seus membros, decisões vinculativas em casos claramente definidos em que as autoridades de controlo tenham posições contraditórias, em especial no âmbito da cooperação entre a autoridade de controlo principal e as autoridades de controlo interessadas, a respeito da questão de fundo, designadamente se há violação do presente regulamento.

(137) Pode ser urgente agir, a fim de defender os direitos e liberdades dos titulares de dados, em especial quando haja perigo de impedimento considerável do exercício de um direito do titular dos dados. Por essa razão, a autoridade de controlo deverá poder adotar no seu território medidas provisórias devidamente justificadas, válidas por um período determinado que não deverá exceder os três meses.

(138) A aplicação desse procedimento deverá ser condição de legalidade das medidas tomadas pelas autoridades de controlo que visem produzir efeitos legais nos casos em que a sua aplicação seja obrigatória. Noutros casos com dimensão transfronteiras, deverá ser aplicado o procedimento de cooperação entre a autoridade de controlo principal e as autoridades de controlo interessadas e a assistência mútua e as operações conjuntas poderão ser realizadas entre as autoridades de controlo interessadas, bilateral ou multilateralmente, sem desencadear o procedimento de controlo da coerência.

(139) A fim de promover a aplicação coerente do presente regulamento, o Comité deverá ser um órgão independente da União. Para atingir os seus objetivos, o Comité deverá ser dotado de personalidade jurídica. O Comité é representado pelo seu presidente. Este Comité deverá substituir o Grupo de Trabalho sobre a proteção das pessoas no que diz respeito ao tratamento de dados pessoais instituído pelo artigo 29.º da Diretiva 95/46/CE. Deverá ser composto pelo diretor de uma autoridade de controlo de cada Estado-Membro e da Autoridade Europeia para a Proteção de Dados ou pelos seus representantes. A Comissão deverá participar nas atividades do Comité, mas sem direito de voto, e a Autoridade Europeia para a Proteção de Dados deverá também participar nas suas atividades com direito de voto em casos particulares. O Comité deverá contribuir para a aplicação coerente do presente regulamento em toda a União, incluindo mediante o aconselhamento da Comissão, nomeadamente no que respeita ao nível de proteção em países terceiros ou em organizações internacionais, e mediante a promoção da cooperação das autoridades de controlo em toda a União. O Comité deverá ser independente no prosseguimento das suas atribuições.

(140) O Comité deverá ser assistido por um secretariado disponibilizado pela Autoridade Europeia para a Proteção de Dados. O pessoal da Autoridade Europeia para a Proteção de Dados

encarregado de exercer as funções conferidas ao Comité pelo presente regulamento deverá agir sob a direção exclusiva do presidente deste Comité, sendo responsável perante o mesmo.

(141) Os titulares dos dados deverão ter direito a apresentar reclamação a uma única autoridade de controlo única, particularmente no Estado-Membro da sua residência habitual, e direito a uma ação judicial efetiva, nos termos do artigo 47.º da Carta, se considerarem que os direitos que lhes são conferidos pelo presente regulamento foram violados ou se a autoridade de controlo não responder a uma reclamação, a recusar ou rejeitar, total ou parcialmente, ou não tomar as iniciativas necessárias para proteger os seus direitos. A investigação decorrente de uma reclamação deverá ser realizada, sob reserva de controlo jurisdicional, na medida adequada ao caso específico. A autoridade de controlo deverá informar o titular dos dados do andamento e do resultado da reclamação num prazo razoável. Se o caso exigir maior investigação ou a coordenação com outra autoridade de controlo, deverão ser comunicadas informações intermédias ao titular dos dados. As autoridades de controlo deverão tomar medidas para facilitar a apresentação de reclamações, nomeadamente fornecendo formulários de reclamação que possam também ser preenchidos eletronicamente, sem excluir outros meios de comunicação.

(142) Se o titular dos dados considerar que os direitos que lhe são conferidos pelo presente regulamento foram violados, deverá ter o direito de mandar um organismo, organização ou associação sem fins lucrativos que seja constituído ao abrigo do direito de um Estado-Membro, cujos objetivos estatutários sejam de interesse público e que exerça a sua atividade no domínio da proteção dos dados pessoais, para apresentar uma reclamação em seu nome junto de uma autoridade de controlo, ou exercer o direito de recurso judicial em nome dos titulares dos dados ou, se tal estiver previsto no direito de um Estado-Membro, exercer o direito à indemnização em nome dos titulares dos dados. Os Estados-Membros podem prever que esse organismo, organização ou associação tenha o direito de apresentar no Estado-Membro em causa uma reclamação, independentemente do mandato do titular dos dados, e o direito a um recurso judicial efetivo, se tiver razões para considerar que ocorreu uma violação dos direitos do titular dos dados por o tratamento dos dados pessoais violar o presente regulamento. Esse organismo, organização ou associação pode não ser autorizado a pedir uma indemnização em nome do titular dos dados independentemente do mandato que lhe é conferido por este.

(143) Todas as pessoas singulares ou coletivas têm o direito de interpor recurso de anulação das decisões do Comité para o Tribunal de Justiça nas condições previstas no artigo 263.º do TFUE. Enquanto destinatárias dessas decisões, as autoridades de controlo interessadas que as pretendam contestar têm de interpor recurso no prazo de dois meses a contar da sua notificação, em conformidade com o artigo 263.º do TFUE. Se as decisões do Comité disserem direta e individualmente respeito a um responsável pelo tratamento, um subcontratante ou ao autor da reclamação, este pode interpor recurso de anulação dessas decisões no prazo de dois meses a contar da sua publicação no sítio web do Comité, em conformidade com o artigo 263.º do TFUE. Sem prejuízo do direito que lhes assiste ao abrigo do artigo 263.º do TFUE, todas as pessoas, singulares ou coletivas, deverão ter direito a interpor junto dos tribunais nacionais competentes recurso efetivo das decisões das autoridades de controlo que produzam efeitos jurídicos em relação a essas pessoas. Tais decisões dizem respeito, em especial, ao exercício de poderes de investigação, correção e autorização pelas autoridades de controlo ou à recusa ou rejeição de reclamações. Porém, o direito a um recurso judicial efetivo não abrange medidas tomadas pelas autoridades de controlo que não sejam juridicamente vinculativas, como os pareceres emitidos ou o aconselhamento prestado pela autoridade de controlo. Os recursos interpostos contra as autoridades de controlo deverão ser interpostos nos tribunais do Estado-Membro em cujo território se encontrem estabelecidas e obedecer às disposições processuais

desse Estado-Membro. Estes tribunais deverão ter jurisdição plena, incluindo o poder de analisar todas as questões de facto e de direito relevantes para o litígio.

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

(144) Sempre que um tribunal chamado a pronunciar-se num recurso da decisão de uma autoridade de supervisão tiver motivos para crer que foi interposto perante um tribunal competente noutro Estado-Membro um processo relativo ao mesmo tratamento, designadamente o mesmo assunto no que se refere às atividades de tratamento do mesmo responsável ou subcontratante, ou ações com o mesmo pedido e a mesma causa de pedir, deverá contactar esse outro tribunal a fim de confirmar a existência de tal processo relacionado. Se estiverem pendentes processos relacionados perante um tribunal de outro Estado-Membro, o tribunal em que a ação tiver sido intentada em segundo lugar poderá suspender o processo ou pode, a pedido de uma das partes, declarar-se incompetente a favor do tribunal em que a ação tiver sido intentada em primeiro lugar se este for competente para o processo em questão e a sua legislação permitir a apensação deste tipo de processos conexos. Consideram-se relacionados os processos ligados entre si por um nexo tão estreito que haja interesse em que sejam instruídos e julgados simultaneamente a fim de evitar soluções que poderiam ser inconciliáveis se as causas fossem julgadas separadamente.

(145) No que diz respeito a ações intentadas contra o responsável pelo tratamento ou o subcontratante, o requerente pode optar entre intentar a ação nos tribunais do Estado-Membro em que está estabelecido o responsável ou o subcontratante, ou nos tribunais do Estado-Membro de residência do titular dos dados, salvo se o responsável pelo tratamento for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos.

(146) O responsável pelo tratamento ou o subcontratante deverão reparar quaisquer danos de que alguém possa ser vítima em virtude de um tratamento que viole o presente regulamento/responsável pelo tratamento. O responsável pelo tratamento ou o subcontratante pode ser exonerado da responsabilidade se provar que o facto que causou o dano não lhe é de modo algum imputável. O conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do presente regulamento. Tal não prejudica os pedidos de indemnização por danos provocados pela violação de outras regras do direito da União ou dos Estados-Membros. Os tratamentos que violem o presente regulamento abrangem igualmente os que violem os atos delegados e de execução adotados nos termos do presente regulamento e o direito dos Estados-Membros que dê execução a regras do presente regulamento. Os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido. Sempre que os responsáveis pelo tratamento ou os subcontratantes estiverem envolvidos no mesmo trata-

mento, cada um deles deverá ser responsabilizado pela totalidade dos danos causados. Porém, se os processos forem associados a um mesmo processo judicial, em conformidade com o direito dos Estados-Membros, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido. Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento.

(147) Quando o presente regulamento previr regras específicas relativas à competência, nomeadamente no que respeita à interposição de recurso judicial, incluindo os pedidos de indemnização, contra um responsável pelo tratamento ou um subcontratante, a aplicação das regras específicas não deverá ser prejudicada por regras de competência gerais como as previstas no Regulamento (UE) n.º 1215/2012 do Parlamento Europeu e do Conselho¹³.

(148) A fim de reforçar a execução das regras do presente regulamento, deverão ser impostas sanções, incluindo coimas, por violação do presente regulamento, para além, ou em substituição, das medidas adequadas que venham a ser impostas pela autoridade de controlo nos termos do presente regulamento. Em caso de infração menor, ou se o montante da coima suscetível de ser imposta constituir um encargo desproporcionado para uma pessoa singular, pode ser feita uma reprensão em vez de ser aplicada uma coima. Importa, porém, ter em devida conta a natureza, gravidade e duração da infração, o seu caráter doloso, as medidas tomadas para atenuar os danos sofridos, o grau de responsabilidade ou eventuais infrações anteriores, a via pela qual a infração chegou ao conhecimento da autoridade de controlo, o cumprimento das medidas ordenadas contra o responsável pelo tratamento ou subcontratante, o cumprimento de um código de conduta ou quaisquer outros fatores agravantes ou atenuantes. A imposição de sanções, incluindo coimas, deverá estar sujeita às garantias processuais adequadas em conformidade com os princípios gerais do direito da União e a Carta, incluindo a proteção jurídica eficaz e um processo equitativo.

(149) Os Estados-Membros deverão poder definir as normas relativas às sanções penais aplicáveis por violação do presente regulamento, inclusive por violação das normas nacionais adotadas em conformidade com o presente regulamento, e dentro dos seus limites. Essas sanções penais podem igualmente prever a privação dos lucros auferidos em virtude da violação do presente regulamento. Contudo, a imposição de sanções penais por infração às referidas normas nacionais, bem como de sanções administrativas, não deverá implicar a violação do princípio *ne bis in idem*, conforme é interpretado pelo Tribunal de Justiça.

(150) A fim de reforçar e harmonizar as sanções administrativas para violações do presente regulamento, as autoridades de controlo deverão ter competência para impor coimas. O presente regulamento deverá definir as violações e o montante máximo e o critério de fixação do valor das coimas daí decorrentes, que deverá ser determinado pela autoridade de controlo competente, em cada caso individual, tendo em conta todas as circunstâncias relevantes da situação específica, ponderando devidamente, em particular, a natureza, a gravidade e a duração da violação e das suas consequências e as medidas tomadas para garantir o cumprimento das obrigações constantes do presente regulamento e para prevenir ou atenuar as consequências da infração. Sempre que forem impostas coimas a empresas, estas deverão ser entendidas como empresas nos termos dos artigos 101.º e 102.º

¹³ Regulamento (UE) n.º 1215/2012 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2012, relativo à competência judiciária, ao reconhecimento e à execu-

ção de decisões em matéria civil e comercial (JO L 351 de 20.12.2012, p. 1).

do TFUE para esse efeito. Sempre que forem impostas coimas a pessoas que não sejam empresas, a autoridade de supervisão deverá ter em conta o nível geral de rendimentos no Estado-Membro, bem como a situação económica da pessoa em questão, no momento de estabelecer o montante adequado da coima. O procedimento de controlo da coerência pode ser utilizado igualmente para a promoção de uma aplicação coerente das coimas. Deverá caber aos Estados-Membros determinar se as autoridades públicas deverão estar sujeitas a coimas, e em que medida. A imposição de uma coima ou o envio de um aviso não afetam o exercício de outros poderes das autoridades de controlo ou a aplicação de outras sanções previstas no presente regulamento.

(151) Os sistemas jurídicos da Dinamarca e da Estónia não conhecem as coimas tal como são previstas no presente regulamento. As regras relativas às coimas podem ser aplicadas de modo que a coima seja imposta, na Dinamarca, pelos tribunais nacionais competentes como sanção penal e, na Estónia, pela autoridade de controlo no âmbito de um processo por infração menor, na condição de tal aplicação das regras nestes Estados-Membros ter um efeito equivalente às coimas impostas pelas autoridades de controlo. Por esse motivo, os tribunais nacionais competentes deverão ter em conta a recomendação da autoridade de controlo que propõe a coima. Em todo o caso, as coimas impostas deverão ser efetivas, proporcionadas e dissuasivas.

(152) Sempre que o presente regulamento não harmonize sanções administrativas, ou se necessário noutros casos, por exemplo, em caso de infrações graves às disposições do presente regulamento, os Estados-Membros deverão criar um sistema que preveja sanções efetivas, proporcionadas e dissuasivas. A natureza das sanções, penal ou administrativa, deverá ser determinada pelo direito do Estado-Membro.

(153) O direito dos Estados-Membros deverá conciliar as normas que regem a liberdade de expressão e de informação, nomeadamente jornalística, académica, artística e/ou literária com o direito à proteção de dados pessoais nos termos do presente regulamento. O tratamento de dados pessoais para fins exclusivamente jornalísticos ou para fins de expressão académica, artística ou literária deverá estar sujeito à derrogação ou isenção de determinadas disposições do presente regulamento se tal for necessário para conciliar o direito à proteção dos dados pessoais com o direito à liberdade de expressão e de informação, tal como consagrado no artigo 11.º da Carta. Tal deverá ser aplicável, em especial, ao tratamento de dados pessoais no domínio do audiovisual e em arquivos de notícias e hemerotecas. Por conseguinte, os Estados-Membros deverão adotar medidas legislativas que prevejam as isenções e derrogações necessárias para o equilíbrio desses direitos fundamentais. Os Estados-Membros deverão adotar essas isenções e derrogações aos princípios gerais, aos direitos do titular dos dados, ao responsável pelo tratamento destes e ao subcontratante, à transferência de dados pessoais para países terceiros ou para organizações internacionais, às autoridades de controlo independentes e à cooperação e à coerência e a situações específicas de tratamento de dados. Se estas isenções ou derrogações divergirem de um Estado-Membro para outro, deverá ser aplicável o direito do Estado-Membro a que esteja sujeito o responsável pelo tratamento. A fim de ter em conta a importância da liberdade de expressão em qualquer sociedade democrática, há que interpretar de forma lata as noções associadas a esta liberdade, como por exemplo o jornalismo.

(154) O presente regulamento permite tomar em consideração o princípio do direito de acesso do público aos documentos oficiais na aplicação do mesmo. O acesso do público aos documentos oficiais pode ser considerado de interesse público. Os dados pessoais que constem de documentos na posse dessas autoridades públicas ou organismos públicos deverão poder ser divulgados publicamente por tais autoridades ou organismos, se a divulgação estiver prevista no direito da União ou do Estado-Membro que lhes for aplicável. Essas legislações deverão conciliar o acesso do público aos documentos oficiais e a reutilização da informação do setor público com o direito à pro-

teção dos dados pessoais e podem pois prever a necessária conciliação com esse mesmo direito nos termos do presente regulamento. A referência a autoridades e organismos públicos deverá incluir, nesse contexto, todas as autoridades ou outros organismos abrangidos pelo direito do Estado-Membro relativo ao acesso do público aos documentos. A Diretiva 2003/98/CE do Parlamento Europeu e do Conselho¹⁴ não modifica nem de modo algum afeta o nível de proteção das pessoas singulares relativamente ao tratamento de dados pessoais nos termos das disposições do direito da União ou do Estado-Membro, nem altera, em particular, as obrigações e direitos estabelecidos no presente regulamento. Em particular, a referida diretiva não deverá ser aplicável a documentos não acessíveis ou de acesso restrito por força dos regimes de acesso por motivos de proteção de dados pessoais nem a partes de documentos acessíveis por força desses regimes que contenham dados pessoais cuja reutilização tenha sido prevista na lei como incompatível com o direito relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

(155) O direito do Estado-Membro ou as convenções coletivas (incluindo «acordos setoriais») podem prever regras específicas para o tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente no que respeita às condições em que os dados pessoais podem ser tratados no contexto laboral, com base no consentimento do assalariado, para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas por lei ou por convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no trabalho, de saúde e segurança no trabalho, e para efeitos de exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.

(156) O tratamento de dados pessoais para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, deverá ficar sujeito à garantia adequada dos direitos e liberdades do titular dos dados nos termos do presente regulamento. Essas garantias deverão assegurar a existência de medidas técnicas e organizativas que assegurem, nomeadamente, o princípio da minimização dos dados. O tratamento posterior de dados pessoais para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, deverá ser efetuado quando o responsável pelo tratamento tiver avaliado a possibilidade de tais fins serem alcançados por um tipo de tratamento de dados pessoais que não permita ou tenha deixado de permitir a identificação dos titulares dos dados, na condição de existirem as garantias adequadas (como a pseudonimização dos dados pessoais). Os Estados-Membros deverão prever garantias adequadas para o tratamento dos dados pessoais para fins de arquivo de interesse público, ou fins de investigação científica ou histórica ou para fins estatísticos. Os Estados-Membros deverão ser autorizados a estabelecer, sob condições específicas e mediante garantias adequadas para o titular dos dados, especificações e derrogações dos requisitos de informação e direitos à retificação, ao apagamento dos dados pessoais, a ser esquecido, à limitação do tratamento e à portabilidade dos dados e de oposição aquando do tratamento de dados pessoais para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos. As condições e garantias em causa podem implicar procedimentos específicos para o exercício desses direitos por parte do titular de dados, se tal for adequado à luz dos fins visados pelo tratamento específico a par de medidas técnicas e organizativas destinadas a reduzir o tratamento de dados pessoais de acordo com os princípios da proporcionalidade e da necessidade. O tratamento de dados para fins científicos deverá igualmente respeitar outra legislação aplicável, tal como a relativa aos ensaios clínicos.

¹⁴ Diretiva 2003/98/CE do Parlamento Europeu e do Conselho, de 17 de novembro de 2003, relativa à reutilização

de informações do setor público (JO L 345 de 31.12.2003, p. 90).

(157) Combinando informações provenientes dos registos, os investigadores podem obter novos conhecimentos de grande valor relativamente a problemas médicos generalizados, como as doenças cardiovasculares, o cancro e a depressão. Com base nos registos, os resultados da investigação podem ser melhorados, já que assentam numa população mais ampla. No âmbito das ciências sociais, a investigação com base em registos permite que os investigadores adquiram conhecimentos essenciais sobre a correlação a longo prazo entre uma série de condições sociais, como o desemprego e o ensino, e outras condições de vida. Os resultados da investigação obtidos através de registos fornecem conhecimentos sólidos e de elevada qualidade, que podem servir de base para a elaboração e a execução de políticas assentes no conhecimento, para melhorar a qualidade de vida de uma quantidade de pessoas e a eficácia dos serviços sociais. A fim de facilitar a investigação científica, os dados pessoais podem ser tratados para fins de investigação científica, sob reserva do estabelecimento de condições e garantias adequadas no direito da União ou dos Estados-Membros.

(158) Quando os dados pessoais sejam tratados para fins de arquivo, o presente regulamento deverá ser também aplicável, tendo em mente que não deverá ser aplicável a pessoas falecidas. As autoridades públicas ou os organismos públicos ou privados que detenham registos de interesse público deverão ser serviços que, nos termos do direito da União ou dos Estados-Membros, tenham a obrigação legal de adquirir, conservar, avaliar, organizar, descrever, comunicar, promover, divulgar e facultar o acesso a registos de valor duradouro no interesse público geral. Os Estados-Membros deverão também ser autorizados a determinar o posterior tratamento dos dados pessoais para efeitos de arquivo, por exemplo tendo em vista a prestação de informações específicas relacionadas com o comportamento político no âmbito de antigos regimes totalitários, genocídios, crimes contra a humanidade, em especial o Holocausto, ou crimes de guerra.

(159) Quando os dados pessoais sejam tratados para fins de investigação científica, o presente regulamento deverá ser também aplicável. Para efeitos do presente regulamento, o tratamento de dados pessoais para fins de investigação científica deverá ser entendido em sentido lato, abrangendo, por exemplo, o desenvolvimento tecnológico e a demonstração, a investigação fundamental, a investigação aplicada e a investigação financiada pelo setor privado. Deverá, além disso, ter em conta o objetivo da União mencionado no artigo 179.º, n.º 1, do TFUE, que consiste na realização de um espaço europeu de investigação. Os fins de investigação científica deverão também incluir os estudos de interesse público realizados no domínio da saúde pública. A fim de atender às especificidades do tratamento de dados pessoais para fins de investigação científica, deverão ser aplicáveis condições específicas designadamente no que se refere à publicação ou outra forma de divulgação de dados pessoais no âmbito dos fins de investigação científica. Se o resultado da investigação científica designadamente no domínio da saúde justificar a tomada de novas medidas no interesse do titular dos dados, as normas gerais do presente regulamento deverão ser aplicáveis no que respeita a essas medidas.

(160) Quando os dados pessoais sejam tratados para fins de investigação histórica, o presente regulamento deverá ser também aplicável. Deverá também incluir-se nesse âmbito a investigação histórica e a investigação para fins genealógicos, tendo em mente que o presente regulamento não deverá ser aplicável a pessoas falecidas.

(161) Para efeitos do consentimento na participação em atividades de investigação científica em ensaios clínicos deverão ser aplicáveis as disposições relevantes do Regulamento (UE) n.º 536/2014 do Parlamento Europeu e do Conselho¹⁵.

¹⁵ Regulamento (UE) n.º 536/2014 do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativo aos ensaios

clínicos de medicamentos para uso humano e que revoga a Diretiva 2001/20/CE (JO L 158 de 27.5.2014, p. 1).

(162) Quando os dados pessoais sejam tratados para fins estatísticos, o presente regulamento deverá ser aplicável. O direito da União ou dos Estados-Membros deverá, dentro dos limites do presente regulamento, determinar o conteúdo estatístico, o controlo de acesso, as especificações para o tratamento de dados pessoais para fins estatísticos e as medidas adequadas para garantir os direitos e liberdades do titular dos dados e para assegurar o segredo estatístico. Por fins estatísticos entende-se todas as operações de recolha e de tratamento de dados pessoais necessárias à realização de estudos estatísticos ou à produção de resultados estatísticos. Esses resultados estatísticos podem ser utilizados posteriormente para fins diferentes, inclusive fins de investigação científica. No fim estatístico está implícito que os resultados do tratamento para esse fim não sejam já dados pessoais, mas dados agregados e que esses resultados ou os dados pessoais não sejam utilizados para justificar medidas ou decisões tomadas a respeito de uma pessoa singular.

(163) Deverão ser protegidas as informações confidenciais que a União e as autoridades nacionais de estatística recolham para a produção de estatísticas oficiais europeias e nacionais. Deverão ser desenvolvidas, elaboradas e divulgadas estatísticas europeias de acordo com os princípios estatísticos enunciados no artigo 338.º, n.º 2, do TFUE, devendo as estatísticas nacionais cumprir também o disposto no direito do Estado-Membro. O Regulamento (CE) n.º 223/2009 do Parlamento Europeu e do Conselho¹⁶ fornece especificações suplementares em matéria de segredo estatístico aplicável às estatísticas europeias.

(164) No que se refere aos poderes das autoridades de controlo para obter, junto do responsável pelo tratamento ou do subcontratante, o acesso aos dados pessoais e o acesso às suas instalações, os Estados-Membros podem adotar no seu ordenamento jurídico, dentro dos limites do presente regulamento, normas específicas que visem preservar o sigilo profissional ou outras obrigações equivalentes, na medida do necessário para conciliar o direito à proteção dos dados pessoais com a obrigação de sigilo profissional. Tal não prejudica as obrigações de adotar regras em matéria de sigilo profissional a que os Estados-Membros fiquem sujeitos por força do direito da União.

(165) O presente regulamento respeita e não afeta o estatuto de que beneficiam, nos termos do direito constitucional vigente, as igrejas e associações ou comunidades religiosas nos Estados-Membros, reconhecido pelo artigo 17.º do TFUE.

(166) A fim de cumprir os objetivos do presente regulamento, a saber, defender os direitos e liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais, e assegurar a livre circulação desses dados na União, o poder de adotar atos nos termos do artigo 290.º do TFUE deverá ser delegado na Comissão. Em especial, deverão ser adotados atos delegados em relação aos critérios e requisitos aplicáveis aos procedimentos de certificação, às informações a fornecer por meio de ícones normalizados e aos procedimentos aplicáveis ao fornecimentos de tais ícones. É especialmente importante que a Comissão proceda a consultas adequadas ao longo dos seus trabalhos preparatórios, incluindo a nível de peritos. A Comissão, aquando da preparação e elaboração dos atos delegados, deverá assegurar o envio simultâneo, em tempo útil e em devida forma, dos documentos relevantes ao Parlamento Europeu e ao Conselho.

(167) A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão nos casos previstos no presente regulamento.

¹⁶ Regulamento (CE) n.º 223/2009 do Parlamento Europeu e do Conselho, de 11 de março de 2009, relativo às Estatísticas Europeias e que revoga o Regulamento (CE, Euratom) n.º 1101/2008 relativo à transmissão de informações abrangidas pelo segredo estatístico ao Serviço de Estatística das

Comunidades Europeias, o Regulamento (CE) n.º 322/97 do Conselho relativo às estatísticas comunitárias e a Decisão 89/382/CEE, Euratom do Conselho que cria o Comité do Programa Estatístico das Comunidades Europeias (JO L 87 de 31.3.2009, p. 164).

Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011. Nesse contexto, a Comissão deverá ponderar medidas específicas para as micro, pequenas e médias empresas.

(168) O procedimento de exame deverá ser utilizado para a adoção de atos de execução em matéria de cláusulas contratuais-tipo entre os responsáveis pelo tratamento e os subcontratantes e entre subcontratantes; códigos de conduta; normas técnicas e procedimentos de certificação; nível de proteção adequado conferido por um país terceiro, um território ou um setor específico nesse país terceiro ou uma organização internacional; cláusulas normalizadas de proteção; formatos e procedimentos de intercâmbio de informações entre os responsáveis pelo tratamento, os subcontratantes e as autoridades de controlo no que respeita às regras vinculativas aplicáveis às empresas; assistência mútua; e regras de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité.

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

(170) Atendendo a que o objetivo do presente regulamento, a saber, assegurar um nível equivalente de proteção das pessoas singulares e a livre circulação de dados pessoais na União, não pode ser suficientemente alcançado pelos Estados-Membros e pode, devido à dimensão e aos efeitos da ação, ser mais bem alcançado ao nível da União, a União pode adotar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia (TUE). Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para alcançar esse objetivo.

(171) A Diretiva 95/46/CE deverá ser revogada pelo presente regulamento. Os tratamentos de dados que se encontrem já em curso à data de aplicação do presente regulamento deverão passar a cumprir as suas disposições no prazo de dois anos após a data de entrada em vigor. Se o tratamento dos dados se basear no consentimento dado nos termos do disposto na Diretiva 95/46/CE, não será necessário obter uma vez mais o consentimento do titular dos dados, se a forma pela qual o consentimento foi dado cumprir as condições previstas no presente regulamento, para que o responsável pelo tratamento prossiga essa atividade após a data de aplicação do presente regulamento. As decisões da Comissão que tenham sido adotadas e as autorizações que tenham emitidas pelas autoridades de controlo com base na Diretiva 95/46/CE, permanecem em vigor até ao momento em que sejam alteradas, substituídas ou revogadas.

(172) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001 e emitiu parecer em 7 de março de 2012¹⁷.

(173) O presente regulamento deverá aplicar-se a todas as matérias relacionadas com a defesa dos direitos e das liberdades fundamentais em relação ao tratamento de dados pessoais, não sujeitas a obrigações específicas com o mesmo objetivo, enunciadas na Diretiva 2002/58/CE do Parlamento Europeu e do Conselho¹⁸, incluindo as obrigações que incumbem ao responsável pelo tratamento e os direitos das pessoas singulares. A fim de clarificar a relação entre o presente regulamento e a Diretiva 2002/58/CE, esta última deverá ser alterada em conformidade. Uma vez adotado o presente regulamento, a Diretiva 2002/58/CE deverá ser revista, em especial a fim de assegurar a coerência com o presente regulamento,

¹⁷ JO C 192 de 30.6.2012, p. 7.

¹⁸ Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados

pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).