COMISSÃO
EUROPEIA

Bruxelas, 23.2.2022
COM(2022) 68 final

2022/0047 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização (Regulamento Dados)

(Texto relevante para efeitos do EEE)

{SEC(2022) 81 final} - {SWD(2022) 34 final} - {SWD(2022) 35 final}

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

• Razões e objetivos da proposta

A presente exposição de motivos acompanha a proposta de regulamento relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização (Regulamento Dados).

Os dados são uma componente central da economia digital, e um recurso essencial para assegurar as transições ecológica e digital. O volume de dados gerados por seres humanos e máquinas tem vindo a aumentar exponencialmente nos últimos anos. No entanto, a maior parte dos dados não é utilizada, ou o seu valor está concentrado nas mãos de um número relativamente reduzido de grandes empresas. A baixa confiança, incentivos económicos contraditórios e obstáculos tecnológicos impedem a plena realização do potencial da inovação baseada em dados. Por conseguinte, é fundamental libertar esse potencial, proporcionando oportunidades para a reutilização de dados, bem como eliminando os obstáculos ao desenvolvimento da economia europeia dos dados, em conformidade com as regras europeias e no pleno respeito dos valores europeus, e em consonância com a missão de reduzir a divisão digital, para que todos beneficiem destas oportunidades. Garantir um maior equilíbrio na distribuição do valor dos dados a par da nova vaga de dados industriais não pessoais e da proliferação de produtos ligados à Internet das coisas significa que existe um enorme potencial para impulsionar uma economia de dados sustentável na Europa.

Regulamentar o acesso e a utilização dos dados constitui uma condição prévia essencial para aproveitar as oportunidades oferecidas pela era digital em que vivemos. A presidente da Comissão, Ursula von der Leyen, declarou nas suas orientações políticas para a Comissão 2019-2024 que a Europa tem de «equilibrar o fluxo e a amplitude da utilização dos dados, preservando, simultaneamente, padrões elevados de privacidade, de segurança e de ética»[1]. O Programa de trabalho da Comissão para 2020[2] definiu vários objetivos estratégicos, nomeadamente a estratégia europeia para os dados[3], adotada em fevereiro de 2020, que visa criar um verdadeiro mercado único de dados e fazer da Europa um líder mundial na economia ágil dos dados. Por este motivo, o Regulamento Dados é um pilar fundamental e a segunda grande iniciativa anunciada na estratégia para os dados. Em particular, contribui para a criação de um quadro de governação intersetorial para o acesso e a utilização dos dados, mediante legislação sobre questões que afetem as relações entre os intervenientes na economia dos dados, a fim de incentivar a partilha horizontal de dados entre setores.

As conclusões do Conselho Europeu de 21 e 22 de outubro de 2021 salientaram «a importância de se avançar com celeridade relativamente a outras iniciativas atuais e futuras, em especial, explorando o valor dos dados na Europa, nomeadamente por intermédio de um quadro regulamentar abrangente que favoreça a inovação, facilite uma melhor portabilidade dos dados e um acesso equitativo aos dados e assegure a interoperabilidade»[4]. Em 25 de março de 2021, o Conselho Europeu reiterou a importância de «explorar melhor o potencial dos dados e das tecnologias digitais, em benefício da sociedade, do ambiente e da

---

1 Ursula von der Leyen, Uma União mais ambiciosa - O meu programa para a Europa, Orientações políticas para a próxima Comissão Europeia 2019-2024, 16 de julho de 2019.

2 Comissão Europeia, Anexos do Programa de Trabalho da Comissão para 2020 - Uma União mais ambiciosa [COM (2020) 37, de 29 de janeiro de 2020].

3 COM/2020/66 final.

4 Conselho Europeu, Reunião do Conselho Europeu (21 e 22 de outubro de 2021) – Conclusões EUCO 17/21, 2021, p. 2.

economia»[5]. Em 1 e 2 de outubro de 2020, salientou «a necessidade de facilitar a disponibilização de dados de elevada qualidade e de promover e permitir uma melhor partilha e mutualização dos dados, bem como a interoperabilidade»[6]. No que respeita aos serviços de computação em nuvem, em 15 de outubro de 2020, os Estados-Membros da UE adotaram por unanimidade uma declaração comum intitulada «Construir a computação em nuvem da próxima geração para as empresas e o setor público na UE». Tal exigiria uma nova geração de serviços de computação em nuvem da UE que atingisse os mais elevados padrões, por exemplo, em termos de portabilidade e interoperabilidade[7].

Na sua resolução de 25 de março de 2021 sobre uma estratégia europeia para os dados, o Parlamento Europeu instou a Comissão a apresentar um ato legislativo sobre os dados, a fim de incentivar e permitir um fluxo de dados maior e mais justo entre empresas, entre empresas e administrações públicas, entre administrações públicas e empresas e entre administrações públicas em todos os setores[8]. Salientou também a necessidade de criar espaços europeus comuns de dados para assegurar a livre circulação de dados não pessoais a nível transfronteiriço e intersetorial e entre empresas, universidades, partes interessadas relevantes e o setor público. Nesta perspetiva, incentivou a Comissão a clarificar os direitos de utilização, especialmente nos contextos de mercado entre empresas e entre empresas e administrações públicas. Frisou ainda que os desequilíbrios do mercado decorrentes da concentração de dados restringem a concorrência, aumentam os obstáculos à entrada no mercado e limitam o acesso e a utilização dos dados.

Na sua resolução, o Parlamento Europeu também salientou que os acordos contratuais entre empresas não garantem necessariamente o acesso adequado das pequenas e médias empresas (PME) aos dados, devido às disparidades existentes em termos de poder negocial ou de conhecimentos especializados. Por conseguinte, o Parlamento Europeu salientou a necessidade de os contratos estabelecerem obrigações e responsabilidades claras no que respeita ao acesso, ao tratamento, à partilha e ao armazenamento dos dados, a fim de limitar a utilização abusiva dos mesmos.

Como tal, a Comissão e os Estados-Membros da UE foram convidados a examinar os direitos e as obrigações dos intervenientes em matéria de acesso aos dados em cuja produção estiveram envolvidos e a aumentarem a sua sensibilização, em particular, para os direitos de acesso aos dados, os direitos de portabilidade e os direitos de solicitar a outra parte que deixe de utilizar os dados, os corrija ou os apague, identificando os seus titulares e determinando a natureza desses direitos.

No que respeita às relações entre empresas e administrações públicas, o Parlamento Europeu solicitou à Comissão que definisse em que circunstâncias e condições o setor privado deve ser obrigado a disponibilizar os dados para utilização pelo setor público, bem como os incentivos previstos para tal, nomeadamente devido à necessidade desses dados para fins de organização dos serviços públicos baseados em dados, e também que examinasse os regimes obrigatórios de partilha de dados entre empresas e administrações públicas, por exemplo em situações que escapam ao controlo das pessoas.

---

5 Conselho Europeu, Declaração dos membros do Conselho Europeu (25 de março de 2021) – Declaração SN 18/21, p. 4.

6 Conselho Europeu, Reunião do Conselho Europeu (1 e 2 de outubro de 2020) – Conclusões EUCO 13/20, 2020, p. 5.

7 Comissão Europeia (2020). *Commission welcomes Member States' declaration on EU cloud federation* (não traduzido para português), comunicado de imprensa.

8 Resolução do Parlamento Europeu, de 25 de março de 2021, sobre uma estratégia europeia para os dados [2020/2217(INI)].

Neste contexto, a Comissão apresenta a proposta de **Regulamento Dados** com o **objetivo de garantir a equidade na distribuição do valor dos dados entre os intervenientes na economia dos dados e de promover o acesso e a utilização dos dados**.

A proposta contribuirá para alcançar os objetivos políticos mais vastos de garantir que as empresas da UE de todos os setores estão em condições de inovar e competir, de capacitar eficazmente as pessoas no que respeita aos seus dados, e de dotar melhor as empresas e os organismos do setor público de um mecanismo proporcional e previsível para fazer face aos principais desafios políticos e societais, nomeadamente emergências públicas e outras situações excecionais. As empresas poderão transferir facilmente os seus dados e outros ativos digitais entre prestadores concorrentes de serviços de computação em nuvem e outros serviços de tratamento de dados. A partilha de dados entre setores e dentro de cada setor da economia exige um quadro de interoperabilidade de medidas processuais e legislativas para reforçar a confiança e melhorar a eficiência. A criação de espaços comuns europeus de dados para setores estratégicos da economia e domínios de interesse público contribuirá para um verdadeiro mercado interno de dados, permitindo a partilha e utilização de dados entre setores. Por conseguinte, o presente regulamento contribui para esta infraestrutura e quadros de governação, bem como para a partilha de dados fora dos espaços de dados.

Indicam-se, em seguida, os objetivos específicos da proposta.

– **Facilitar o acesso aos dados e a sua utilização por parte dos consumidores e das empresas, preservando ao mesmo tempo os incentivos ao investimento em formas de gerar valor através dos dados.** Tal inclui aumentar a segurança jurídica em torno da partilha de dados obtidos ou gerados pela utilização de produtos ou serviços conexos, bem como operacionalizar regras para garantir a equidade nos contratos de partilha de dados. A proposta **clarifica** a aplicação dos direitos pertinentes ao abrigo da Diretiva 96/9/CE relativa à proteção jurídica das bases de dados (**Diretiva Bases de Dados**)[9] às suas disposições.

– **Prever a utilização, por parte dos organismos do setor público e das instituições, agências ou organismos da União, dos dados na posse de empresas em determinadas situações em que haja uma necessidade excecional de dados.** Tal diz principalmente respeito a emergências públicas, mas também a outras situações excecionais em que se justifica a partilha obrigatória de dados entre empresas e administrações públicas, a fim de apoiar políticas e serviços públicos baseados em dados concretos, eficazes, eficientes e orientados para o desempenho.

– **Facilitar a mudança entre serviços de computação em nuvem e serviços periféricos.** O acesso a serviços de tratamento de dados competitivos e interoperáveis é uma condição prévia para uma economia dos dados próspera, em que os dados possam ser facilmente partilhados no interior dos ecossistemas setoriais e entre eles. O nível de confiança nos serviços de tratamento de dados determina a adoção desses serviços pelos utilizadores em todos os setores da economia.

– **Criar garantias contra a transferência ilícita de dados sem notificação por parte dos prestadores de serviços de computação em nuvem**. Tal deve-se ao facto de terem sido manifestadas preocupações quanto ao acesso ilícito dos governos de países terceiros/do Espaço Económico Europeu (EEE) aos dados. Essas garantias devem reforçar ainda mais a confiança nos serviços de tratamento de dados que estão cada vez mais na base da economia europeia dos dados.

9 JO L 77 de 27.3.1996, p. 20.

– **Prever o desenvolvimento de normas de interoperabilidade para os dados a reutilizar entre setores**, a fim de eliminar os obstáculos à partilha de dados entre espaços comuns europeus de dados específicos de determinados domínios, em consonância com os requisitos de interoperabilidade setoriais, e entre outros dados que não se inserem no âmbito de um espaço comum europeu de dados específico. A proposta apoia também o estabelecimento de normas para os «contratos inteligentes». Trata-se de programas informáticos armazenados em livros-razão eletrónicos que executam e liquidam transações com base em condições predeterminadas. Têm potencial para proporcionar aos detentores e destinatários de dados garantias de que as condições para a partilha de dados são respeitadas.

- **Coerência com as disposições existentes da mesma política setorial**

A presente proposta é coerente com as regras existentes em matéria de **tratamento de dados pessoais** [incluindo o Regulamento Geral sobre a Proteção de Dados (RGPD)[10]] e de proteção da vida privada e da **confidencialidade das comunicações**, bem como de quaisquer dados (pessoais e não pessoais) armazenados em equipamentos terminais e acedidos a partir dos mesmos [Diretiva Privacidade Eletrónica[11], a substituir pelo Regulamento Privacidade Eletrónica, atualmente objeto de negociações legislativas]. Complementa os direitos existentes, nomeadamente os relativos aos dados gerados por um produto de um utilizador ligado a uma rede de comunicações eletrónicas publicamente disponível.

O **Regulamento Livre Fluxo de Dados Não Pessoais**[12] criou um elemento essencial da economia europeia dos dados, assegurando que os dados não pessoais podem ser armazenados, tratados e transferidos em qualquer ponto da União. Apresentou também uma abordagem de autorregulação para o problema da «vinculação a um prestador» ao nível dos prestadores de serviços de tratamento de dados, através da introdução de códigos de conduta para facilitar a transferência de dados entre serviços de computação em nuvem [os códigos de conduta *Switching Cloud Providers and Porting Data* (SWIPO – Mudança de prestadores de serviços em nuvem e portabilidade dos dados), desenvolvidos pela indústria]. A presente proposta baseia-se também neste aspeto, ajudando as empresas e os cidadãos a tirar o máximo partido do direito de mudar de prestador de serviços de computação em nuvem e de aplicar a portabilidade de dados. É também plenamente coerente com a Diretiva Cláusulas Contratuais Abusivas no que respeita ao direito contratual[13]. Relativamente aos serviços de computação em nuvem, uma vez que a abordagem de autorregulação não parece ter afetado significativamente a dinâmica do mercado, a presente proposta apresenta uma abordagem regulamentar ao problema salientado no Regulamento Livre Fluxo de Dados Não Pessoais.

O tratamento e o armazenamento de dados internacionais e as transferências de dados são regidos pelo RGPD, pelos compromissos comerciais da Organização Mundial do Comércio (OMC), pelo Acordo Geral sobre o Comércio de Serviços (GATS) e por acordos comerciais bilaterais.

O **direito da concorrência**[14] é aplicável no contexto, nomeadamente, do controlo das concentrações, da partilha de dados por empresas ou de um abuso de posição dominante de uma empresa.

---

10 JO L 119 de 4.5.2016, p. 1.
11 JO L 201 de 31.7.2002, p. 37.
12 JO L 303 de 28.11.2018, p. 59. SWIPO (2021), ver sítio Web.
13 JO L 95 de 21.4.1993, p. 29.
14 JO L 335 de 18.12.2010, p. 36.

A **Diretiva Bases de Dados**[15] prevê a proteção *sui generis* das bases de dados que tenham sido criadas na sequência de um investimento substancial, mesmo que a própria base de dados não seja uma criação intelectual original protegida pelo direito de autor. Com base na grande quantidade de jurisprudência que interpreta as disposições da Diretiva Bases de Dados, a presente proposta aborda as atuais incertezas jurídicas quanto à questão de saber se as bases de dados que contêm dados gerados ou obtidos através da utilização de produtos ou serviços conexos, como sensores, ou outros tipos de dados gerados por máquinas, teriam direito a essa proteção.

O **Regulamento P2B**[16] impõe obrigações de transparência, exigindo às plataformas que descrevam, para os utilizadores profissionais, os dados gerados pela prestação do serviço.

A **Diretiva Dados Abertos**[17] estabelece regras mínimas em matéria de reutilização de dados que se encontram na posse do setor público e de dados de investigações financiadas por fundos públicos disponibilizados ao público através de repositórios.

A **iniciativa Europa Interoperável** procura introduzir uma política de interoperabilidade cooperativa para um setor público modernizado. Surgiu com base no ISA^2, um programa de financiamento da União que decorreu entre 2016 e 2021 e apoiou o desenvolvimento de soluções digitais para permitir a interoperabilidade transfronteiriça e intersetorial dos serviços públicos[18].

A presente proposta complementa o **Regulamento Governação de Dados,** recentemente adotado, que visa facilitar a partilha voluntária de dados por indivíduos e empresas e harmoniza as condições de utilização de determinados dados do setor público, sem alterar direitos materiais relativos aos dados ou direitos de acesso e utilização de dados estabelecidos[19]. Complementa também a proposta de **Regulamento Mercados Digitais**, que exigirá que determinados prestadores de serviços essenciais de plataforma identificados como «controladores de acesso» proporcionem, nomeadamente, uma portabilidade mais efetiva dos dados gerados no decurso das atividades de utilizadores profissionais e de utilizadores finais[20].

A presente proposta não afeta as regras existentes nos domínios da propriedade intelectual (exceto a aplicação do direito *sui generis* da Diretiva Bases de Dados), da concorrência, da justiça, dos assuntos internos e da cooperação (internacional) conexa, das obrigações relacionadas com o comércio, ou da proteção jurídica de segredos comerciais.

Para promover a transição digital, são necessárias adaptações legislativas em vários domínios. Nos termos do passaporte digital europeu de produtos (no âmbito da Iniciativa Produtos Sustentáveis)[21] serão estabelecidas regras claras relativamente ao acesso a dados específicos necessários à circularidade e sustentabilidade de determinados produtos ao longo do seu ciclo de vida e em situações não excecionais. As regras do direito privado são um elemento fundamental no quadro geral. Por conseguinte, o presente regulamento adapta o direito contratual e outras regras para melhorar as condições de reutilização de dados no mercado

15 JO L 77 de 27.3.1996, p. 20.
16 JO L 186 de 11.7.2019, p. 57.
17 JO L 172 de 26.6.2019, p. 56.
18 JO L 318 de 4.12.2015, p. 1.
19 COM/2020/767 final.
20 JO L 186 de 11.7.2019, p. 57.
21 COM/2020/98 final.

interno e evitar que as partes nos contratos abusem dos desequilíbrios no poder negocial em detrimento das partes mais fracas.

Como proposta horizontal, o **Regulamento Dados** prevê **regras de base para todos os setores** no que respeita aos direitos de utilização dos dados, nomeadamente nos domínios das máquinas inteligentes ou dos bens de consumo. No entanto, os direitos e as obrigações em matéria de acesso e utilização dos dados também foram regulamentados em diferentes graus a nível setorial. O Regulamento Dados não alterará a legislação existente, mas a futura legislação nestes domínios deve, em princípio, ser alinhada com os seus princípios horizontais. A convergência com as regras horizontais do Regulamento Dados deve ser avaliada aquando da revisão dos instrumentos setoriais. A presente proposta deixa margem para que a legislação vertical estabeleça regras mais pormenorizadas para a consecução de objetivos regulamentares setoriais.

Tendo em conta a legislação setorial em vigor, no que respeita à criação do espaço de dados do Pacto Ecológico, a revisão[22] da **Diretiva INSPIRE**[23] permitirá uma maior disponibilidade e reutilização de dados espaciais e ambientais. Esta iniciativa visa facilitar o apoio, por parte das autoridades públicas, das empresas e dos cidadãos da UE, à transição para uma economia mais ecológica e neutra em termos de carbono e reduzindo os encargos administrativos. Prevê-se que apoie serviços de dados reutilizáveis em grande escala, a fim de ajudar a recolher, partilhar, tratar e analisar grandes volumes de dados necessários para garantir o cumprimento da legislação ambiental e das ações prioritárias definidas no Pacto Ecológico. Racionalizará a comunicação de informações e a redução dos encargos através de uma melhor reutilização dos dados existentes, da geração automática de relatórios através da prospeção de dados e da inteligência empresarial.

O **Regulamento Eletricidade**[24] da UE exige que os operadores de redes de transporte forneçam dados aos reguladores e prevê o planeamento da adequação dos recursos, ao passo que a **Diretiva Eletricidade**[25] da UE prevê o acesso transparente e não discriminatório aos dados e encarrega a Comissão de desenvolver requisitos e procedimentos de interoperabilidade conexos para facilitar esse processo. A **Diretiva Serviços de Pagamento 2**[26] abre alguns tipos de informações sobre operações de pagamento e contas em determinadas condições, permitindo assim a partilha de dados entre empresas no domínio da tecnologia financeira. No setor da mobilidade e dos transportes, existe uma grande variedade de regras em matéria de acesso e partilha de dados. A informação relativa à reparação e manutenção de veículos a motor e máquinas agrícolas está sujeita a obrigações específicas de acesso/partilha de dados ao abrigo da **legislação em matéria de homologação**[27]. No entanto, são necessárias novas regras para assegurar que a legislação existente em matéria de homologação de veículos é adequada à era digital e promove o desenvolvimento de veículos não poluentes, conectados e automatizados. Com base no Regulamento Dados enquanto quadro para o acesso e a utilização dos dados, estas regras abordarão desafios setoriais específicos, nomeadamente o acesso às funções e recursos dos veículos.

22 GreenData4All initiative (REFIT) | Legislative train schedule | European Parliament (europa.eu).
23 JO L 108 de 25.4.2007, p. 1.
24 JO L 158 de 14.6.2019, p. 54.
25 JO L 158 de 14.6.2019, p. 125.
26 JO L 337 de 23.12.2015, p. 35 JO L 337 de 23.12.2015, p. 35.
27 JO L 151 de 14.6.2018, p. 1. JO L 60 de 2.3.2013, p. 1.

No âmbito da **Diretiva Sistemas de Transporte Inteligentes**[28], foram e continuarão a ser elaborados vários regulamentos delegados, nomeadamente para especificar a acessibilidade dos dados para o transporte rodoviário e multimodal de passageiros, em especial através dos pontos de acesso nacionais. Na gestão do tráfego aéreo, os dados não operacionais são importantes para melhorar a intermodalidade e a conectividade. Os dados operacionais relacionados com a gestão do tráfego aéreo seriam abrangidos pelo regime específico definido no âmbito do **Céu Único Europeu**[29]. No acompanhamento do tráfego de navios, os dados relativos aos navios (localização e seguimento) são importantes para melhorar a intermodalidade e a conectividade: estes dados estão abrangidos pelo regime específico definido na Diretiva VTMIS[30]. São também da competência do sistema e dos serviços marítimos digitais[31]. A proposta de regulamento relativo à criação de uma **infraestrutura para combustíveis alternativos**[32] especifica os tipos de dados pertinentes a disponibilizar, em sinergia com o quadro geral estabelecido na Diretiva Sistemas de Transporte Inteligentes.

- **Coerência com outras políticas da União**

A presente proposta está em consonância com as prioridades da Comissão de **preparar a Europa para a era digital** e de construir uma economia preparada para o futuro que esteja ao serviço das pessoas[33], em que a digitalização do mercado interno se caracteriza por um elevado grau de confiança, segurança, proteção e escolha para os consumidores. A digitalização do mercado interno é altamente competitiva graças a um quadro que favorece a transparência, a concorrência e a inovação, e que é tecnologicamente neutro. Apoia o **Mecanismo de Recuperação e Resiliência**[34], retirando ensinamentos da pandemia de COVID-19 e os benefícios de dados mais facilmente acessíveis, sempre que necessário.

A presente proposta apoia o papel fundamental dos dados na consecução dos **objetivos do Pacto Ecológico Europeu** de várias formas. Em primeiro lugar, aprofundando a compreensão, por parte dos governos, das empresas e dos indivíduos, dos impactos na sociedade e na economia dos produtos, serviços e materiais ao longo de todas as cadeias de abastecimento. Em segundo lugar, mobilizando a riqueza existente de dados pertinentes do setor privado para combater problemas relacionados com o clima, a biodiversidade, a poluição[35] e os recursos naturais, em consonância com os objetivos do Pacto Ecológico Europeu[36], as conclusões pertinentes do Conselho[37] e as posições[38] do Parlamento Europeu. Em terceiro lugar, colmatando lacunas de conhecimentos e gerindo crises conexas através de ações reforçadas de atenuação, preparação, resposta e recuperação.

Em consonância com a **Estratégia Industrial**[39], a proposta aborda tecnologias altamente estratégicas, como a computação em nuvem e os sistemas de inteligência artificial: domínios

---

28 JO L 207 de 6.8.2010, p. 1.
29 JO L 96 de 31.3.2004, p. 1; JO L 96 de 31.3.2004, p. 10; JO L 96 de 31.3.2004, p. 20.
30 JO L 308 de 29.10.2014, p. 82.
31 JO L 96 de 12.4.2016, p. 46.
32 COM/2021/559 final.
33 COM/2020/67 final.
34 JO L 57 de 18.2.2021, p. 17.
35 COM(2021) 400 final.
36 COM/2019/640 final.
37 Digitalização em prol do ambiente, 11 de dezembro de 2020, Conclusões do Conselho sobre o novo Plano de Ação para a Economia Circular, 11 de dezembro de 2020, Conclusões do Conselho sobre a Estratégia de Biodiversidade da UE para 2030, 16 de outubro de 2020, Conclusões sobre a melhoria da qualidade do ar, 5 de março de 2020.
38 Emergência climática e ambiental - Quinta-feira, 28 de novembro de 2019 (europa.eu).
39 COM/2021/350 final.

cujo pleno potencial a UE, à beira da próxima vaga de dados industriais, ainda não aproveitou. Aplica o objetivo da **Estratégia para os Dados**[40] de as empresas serem mais capazes de inovar e competir com base nos valores da UE, e o princípio da **livre circulação de dados no mercado interno**. Está também em consonância com o **plano de ação em matéria de propriedade intelectual**[41], no qual a Comissão se comprometeu a rever a Diretiva Bases de Dados.

A presente proposta deve também respeitar os princípios do Plano de Ação sobre o Pilar Europeu dos Direitos Sociais (PEDS)[42] e os requisitos de acessibilidade da Diretiva (UE) 2019/882 relativa aos requisitos de acessibilidade dos produtos e serviços[43].

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

• Base jurídica

A base jurídica da presente proposta é o artigo 114.º do Tratado sobre o Funcionamento da União Europeia, cujo objetivo consiste no estabelecimento e funcionamento do mercado interno por intermédio do reforço de medidas relativas à aproximação das regras nacionais.

A presente proposta visa promover a realização do mercado interno dos dados, em que os dados do setor público, das empresas e das pessoas singulares são utilizados da melhor forma possível, respeitando simultaneamente os direitos relativos a esses dados e os investimentos realizados para os recolher. As disposições relativas à mudança entre serviços de tratamento de dados visam estabelecer condições de mercado equitativas e competitivas para o mercado interno dos serviços de computação em nuvem, periféricos e conexos.

A proteção dos dados comerciais confidenciais e dos segredos comerciais é um aspeto importante do bom funcionamento do mercado interno, tal como acontece noutros contextos em que há troca de serviços e comercialização de bens. A presente proposta garante o respeito dos segredos comerciais no contexto da utilização de dados entre empresas ou por consumidores. A iniciativa permitirá à União beneficiar da dimensão do mercado interno, dado que os produtos ou serviços conexos são muitas vezes desenvolvidos utilizando dados de diferentes Estados-Membros, e posteriormente comercializados na União.

Alguns Estados-Membros tomaram medidas legislativas para resolver os problemas acima descritos, em cenários entre empresas e entre empresas e administrações públicas, ao passo que outros não o fizeram. Tal pode levar a uma fragmentação legislativa no mercado interno e a diferentes regras e práticas na União, bem como a custos conexos para as empresas, que teriam de cumprir regimes diferentes. Por conseguinte, é importante assegurar que as medidas propostas são aplicadas de forma coerente em todos os Estados-Membros.

• Subsidiariedade (no caso de competência não exclusiva)

Dada a natureza transfronteiriça da utilização de dados e os muitos domínios de impacto do Regulamento Dados, as questões abordadas na presente proposta não podem ser tratadas de forma eficaz ao nível dos Estados-Membros. A fragmentação decorrente das diferenças entre as regras nacionais deve ser evitada, uma vez que levaria a custos de transação mais elevados, à ausência de transparência, à insegurança jurídica e a uma busca indesejável do foro mais favorável. Evitar a fragmentação é particularmente importante em todas as situações

40 COM/2020/66 final.
41 COM/2020/760 final.
42 COM/2021/102 final.
43 JO L 151 de 7.6.2019.

relacionadas com os aspetos dos dados das relações entre empresas, incluindo as cláusulas contratuais equitativas e as obrigações dos fabricantes de produtos da Internet das coisas ou de serviços conexos, aspetos que exigem homogeneidade do quadro em toda a União.

Uma avaliação dos aspetos transfronteiriços dos fluxos de dados no domínio da partilha de dados entre empresas e administrações públicas também demonstra a necessidade de agir a nível da União. Muitos intervenientes privados que possuem dados pertinentes são empresas multinacionais. Estas empresas não devem ser confrontadas com um regime jurídico fragmentado.

Os serviços de computação em nuvem raramente são oferecidos apenas num Estado-Membro. Em consonância com o RGPD e o Regulamento Livre Fluxo de Dados Não Pessoais, que permitem aos consumidores e às empresas tratar dados pessoais e não pessoais em qualquer parte da União que desejarem, o tratamento transfronteiriço de dados na União é essencial para o exercício de uma atividade empresarial no mercado interno. Por conseguinte, é fundamental que as disposições relativas à mudança de serviços de tratamento de dados sejam aplicadas a nível da União, a fim de evitar uma fragmentação prejudicial num mercado de serviços de tratamento de dados, de outra forma, unificado.

Apenas uma ação comum a nível da União pode permitir a consecução dos objetivos estabelecidos na presente proposta, incluindo a criação de condições equitativas inovadoras e competitivas para as empresas baseadas em dados e a capacitação dos cidadãos. Esta ação comum constitui um avanço confiante na concretização da visão de criar um verdadeiro mercado interno dos dados.

- **Proporcionalidade**

A presente proposta estabelece um equilíbrio entre os direitos e os interesses das partes interessadas afetadas e o objetivo geral de facilitar uma utilização mais ampla dos dados por parte de um vasto leque de intervenientes. Cria um quadro facilitador que não excede o necessário para atingir os objetivos. Aborda os obstáculos existentes à plena realização do potencial valor dos dados entre empresas, consumidores e o setor público. Estabelece também um quadro para futuras regras setoriais, a fim de evitar a fragmentação e a insegurança jurídica. Clarifica os direitos existentes e, se necessário, concede direitos de acesso aos dados, ajudando assim a desenvolver um mercado interno para a partilha de dados. A iniciativa deixa uma margem de flexibilidade significativa para a aplicação a nível setorial.

A presente proposta dará origem a custos financeiros e administrativos, que serão suportados principalmente pelas autoridades nacionais, pelos fabricantes e pelos prestadores de serviços, para cumprirem as obrigações estabelecidas no presente regulamento. No entanto, a exploração de diferentes opções e dos seus custos e benefícios previstos resultou numa conceção equilibrada do instrumento. Do mesmo modo, os custos para os utilizadores e detentores de dados serão contrabalançados pelo valor a retirar de um acesso e de uma utilização mais ampla dos dados, bem como da adoção por parte do mercado de novos serviços.

- **Escolha do instrumento**

O instrumento escolhido foi um regulamento porque é o melhor mecanismo para servir os objetivos políticos mais vastos de garantir que todas as empresas da União estão em condições de inovar e competir, que os consumidores estão mais aptos a assumir o controlo dos seus dados, e que as instituições, agências e organismos da União estão mais bem equipados para enfrentar grandes desafios políticos, incluindo emergências públicas. À luz do

objetivo de harmonização abrangente visado pela proposta, é necessário um regulamento para garantir a segurança jurídica e a transparência para os operadores económicos, incluindo as micro, pequenas e médias empresas, e para assegurar às pessoas coletivas e singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e de obrigações, com o intuito de garantir uma aplicação coerente em todos os Estados-Membros, bem como uma cooperação eficaz entre as autoridades competentes dos diferentes Estados-Membros.

A proposta reforçará o mercado interno dos dados, aumentando a segurança jurídica e garantindo um quadro jurídico uniforme, horizontal e coerente.

3. RESULTADOS DAS AVALIAÇÕES *EX POST*, DAS CONSULTAS DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

- **Avaliações *ex post*/balanços de qualidade da legislação existente**

A presente proposta baseia-se parcialmente na última avaliação da Diretiva Bases de Dados e no estudo da Comissão que apoia essa revisão[44]. A Diretiva Bases de Dados introduziu, entre outras coisas, um direito *sui generis* específico para proteger as bases de dados se o produtor de uma base de dados tiver feito um investimento substancial na obtenção, verificação e apresentação dos dados. Desde a sua primeira adoção, a diretiva foi avaliada duas vezes. Ambas as avaliações foram complementadas por comunicações da Comissão sobre a política para a economia dos dados[45].

O Tribunal de Justiça da União Europeia clarificou o entendimento de investimentos substanciais numa base de dados, esclarecendo que o direito *sui generis* visa proteger os investimentos na reunião de dados, e não na criação desses dados[46], enquanto subproduto de outra atividade económica. No entanto, subsiste incerteza quanto à aplicação acidental ou não intencional do direito *sui generis* às bases de dados que contêm dados gerados por máquinas, ou seja, dados obtidos através da utilização de produtos ou serviços conexos ou gerados por ela. É necessário equilibrar os objetivos políticos da proteção da propriedade intelectual dessas bases de dados no contexto da economia dos dados, em que a exclusividade dos dados como bem não rival é, em geral, considerada um obstáculo à inovação. Para garantir a coerência com as intervenções regulamentares propostas na presente proposta, a intervenção sobre o direito *sui generis* aborda especificamente a aplicação problemática identificada do direito *sui generis* no contexto da Internet das coisas. A Comissão está também a preparar a avaliação do Regulamento (UE) 2018/1807, prevista para novembro de 2022. Os relatórios iniciais elaborados por contratantes externos demonstraram o efeito limitado dos códigos de conduta SWIPO na mudança de prestador de serviços de computação em nuvem.

- **Consulta das partes interessadas**

Durante o mandato da anterior Comissão, deu-se início a um trabalho exaustivo para identificar os problemas que estão a impedir a União de realizar todo o potencial da inovação baseada em dados na economia. A proposta baseia-se em ações de consulta anteriores, como a

---

44 COM/2017/09 final; SWD(2018) 146 final, secção 5.4.2; *Study to Support an Impact Assessment for the Review of the Database Directive* (não traduzido para português).

45 COM/2017/09 final; COM/2020/66 final; COM/2020/760 final.

46 Acórdão do Tribunal de Justiça de 9 de novembro de 2004, *Fixtures Marketing Ltd/Oy Veikkaus Ab*, C-46/02, ECLI:EU:C:2004:694; Acórdão do Tribunal de Justiça de 9 de novembro de 2004, *Fixtures Marketing Ltd/Svenska Spel Ab*, C-338/02, ECLI:EU:C:2004:696; Acórdão do Tribunal de Justiça de 9 de novembro de 2004, *British Horseracing Board Ltd/William Hill*, C-203/02, ECLI:EU:C:2004:695; Acórdão do Tribunal de Justiça de 9 de novembro de 2004, *Fixtures Marketing Ltd/OPAP*, C-444/02, ECLI:EU:C:2004:697.

consulta pública de 2017 em apoio da Comunicação da Comissão «Construir uma economia europeia dos dados»[47], a consulta pública de 2017 sobre a avaliação da Diretiva Bases de Dados, a consulta pública de 2018 sobre a revisão da Diretiva relativa à reutilização de informações do setor público, a consulta do painel de PME de 2018 sobre os princípios e orientações em matéria de partilha de dados entre empresas, e a consulta pública em linha da Comissão sobre a Estratégia para os Dados[48], que decorreu de fevereiro a maio de 2020.

Em 28 de maio de 2021, foi publicada uma avaliação de impacto inicial no portal «Legislar Melhor», que esteve aberta à apresentação de observações durante quatro semanas. A Comissão recebeu 91 contribuições no portal «Legislar Melhor»[49], principalmente de empresas.

Posteriormente, em 3 de junho de 2021, foi publicada uma consulta pública em linha sobre o Regulamento Dados, que encerrou em 3 de setembro de 2021. A consulta abordou os pontos abrangidos pela iniciativa, com secções e perguntas pertinentes. Visou todos os tipos de partes interessadas, recolhendo contributos sobre a partilha de dados, o acesso e a utilização em contextos entre empresas e entre empresas e administrações públicas, a capacitação dos consumidores e a portabilidade dos dados, o potencial papel de medidas técnicas, como os contratos inteligentes, a capacidade de os utilizadores mudarem de serviço de computação em nuvem, os direitos de propriedade intelectual (ou seja, a proteção das bases de dados) e as garantias para os dados não pessoais no contexto internacional. Após uma análise aprofundada das respostas, a Comissão publicou um relatório de síntese no seu sítio Web[50].

No total, foram recebidas 449 contribuições de 32 países. As entidades empresariais constituíram o maior número de contribuições, incluindo 122 associações empresariais e 105 empresas/organizações empresariais. Além disso, 100 respondentes eram autoridades públicas e 58 eram membros individuais do público. De um modo geral, as respostas confirmaram a existência de uma série de obstáculos a uma partilha eficaz e eficiente de dados em todos os tipos de relações de dados.

No contexto entre empresas, apesar de a partilha de dados entre empresas ser uma prática comum, os respondentes que se depararam com dificuldades identificaram obstáculos, como os de natureza técnica (formatos, ausência de normas – 69 %); a recusa absoluta de concessão de acesso não relacionada com preocupações em matéria de concorrência (55 %) ou o abuso de um desequilíbrio contratual (44 %). Em matéria contratual, quase metade dos respondentes manifestaram-se a favor da introdução de um teste do caráter abusivo (46 %), mais do dobro dos respondentes que se mostraram contra (21 %). As PME revelaram um forte apoio (50 %) a um teste do caráter abusivo, com um número significativo de grandes empresas também a favor (41 %). Do mesmo modo, 46 % das partes interessadas de todos os setores manifestaram apoio a regras gerais de acesso baseadas em cláusulas equitativas, razoáveis e não discriminatórias (46 %). 60 % dos respondentes, em particular PME e microempresas (78 %), concordaram que modelos de cláusulas contratuais poderiam contribuir para uma maior partilha de dados. 70 % das partes interessadas expressaram a opinião de que há um problema de equidade com os dados gerados no contexto da Internet das coisas, e que os fabricantes de produtos conectados ou serviços conexos não devem poder decidir

47 COM/2017/09 final.

48 Comissão Europeia (2020). *Resultados da consulta em linha sobre a Estratégia Europeia para os Dados.*

49 *Sítio Web* da Comissão Europeia: *Dê a sua opinião - Ato legislativo sobre os dados e alteração da legislação sobre a proteção jurídica das bases de dados.*

50 Comissão Europeia (2021). *Consulta pública relativa ao ato legislativo sobre os dados: relatório de síntese*.

unilateralmente o que acontece aos dados gerados por esses produtos. 79 % dos respondentes consideraram que os contratos inteligentes poderiam ser um instrumento eficaz para implementar tecnicamente o acesso e a utilização dos dados no contexto dos dados cogerados pela Internet das coisas.

A insegurança e os obstáculos jurídicos, os desincentivos comerciais e a ausência de infraestruturas adequadas foram alguns dos principais fatores identificados pelos respondentes como impedindo a partilha de dados entre empresas e administrações públicas. Quase todas as autoridades públicas consideram que é necessária uma ação (da União ou dos Estados-Membros) em matéria de partilha de dados entre empresas e administrações públicas, em comparação com 80 % das instituições académicas/de investigação e 38 % das empresas/organizações/associações empresariais. Uma clara maioria de partes interessadas (em especial cidadãos e administrações públicas) manifestou também a opinião de que a partilha de dados entre empresas e administrações públicas deve ser obrigatória, com garantias claras para casos de utilização específicos com um claro interesse público em emergências e para efeitos de gestão de crises, para estatísticas oficiais, para a proteção do ambiente e para uma sociedade mais saudável em geral.

Os respondentes também confirmaram a utilidade de um direito à mudança para os utilizadores profissionais de serviços de computação em nuvem. No que respeita às garantias para os dados não pessoais em contextos internacionais, 76 % dos respondentes consideram que o potencial acesso aos dados por parte de autoridades estrangeiras com base em legislação estrangeira constitui um risco para a sua organização, tendo 19 % indicado que se trata de um risco importante.

- **Recolha e utilização de conhecimentos especializados**

A proposta foi apoiada por vários estudos, seminários e outros contributos de peritos:

– **Estudo de apoio à presente avaliação de impacto sobre o reforço da utilização de dados na Europa**, incluindo entrevistas com partes interessadas específicas. Incluiu dois seminários intersetoriais sobre a partilha de dados entre empresas e entre empresas e administrações públicas, bem como um seminário de validação final organizada na primavera de 2021.

– E**studo sobre modelos de cláusulas contratuais, o controlo da equidade na partilha de dados e nos contratos em nuvem e sobre os direitos de acesso aos dados** avaliou, em especial, os aspetos da equidade nas relações de partilha de dados entre empresas e incluiu entrevistas específicas com partes interessadas e um seminário de validação.

– **Estudo sobre os prejuízos económicos decorrentes de contratos de serviços de computação em nuvem abusivos e desequilibrados**. Incluiu um inquérito em linha a uma amostra de PME e empresas em fase de arranque que utilizam a computação em nuvem nas suas atividades.

– **Estudo sobre a mudança de prestadores de serviços de computação em nuvem**, incluindo um seminário intersetorial no segundo trimestre de 2017.

– **Estudo de apoio à revisão da Diretiva Bases de Dados**, incluindo entrevistas com partes interessadas específicas. Assistiu a Comissão na preparação da avaliação de impacto para acompanhar a revisão da Diretiva Bases de Dados, no contexto do Regulamento Dados e na consecução dos seus objetivos interligados.

– **Apoio metodológico à avaliação de impacto da utilização de dados de bases privadas por estatísticas oficiais**. Este exercício contribui para a avaliação do impacto da reutilização de dados entre empresas e administrações públicas em estatísticas oficiais, desenvolvendo uma abordagem metodológica e descrevendo os benefícios e os custos da reutilização de dados e de casos de utilização selecionados para diferentes domínios estatísticos e diferentes tipos de dados do setor privado. Além disso, contribui para a investigação e as deliberações em curso, a fim de alcançar uma melhor compreensão da partilha de dados entre empresas e administrações públicas.

– **Webinários sobre plataformas de dados pessoais e de dados industriais**. Em 6, 7 e 8 de maio de 2020 foram organizados três webinários, que reuniram os projetos de plataformas de dados pertinentes do portefólio da parceria público-privada em matéria de megadados (Big Data Value).

– **Relatório do grupo de peritos de alto nível sobre a partilha de dados entre empresas e administrações públicas.** O relatório apresenta uma análise dos problemas relacionados com a partilha de dados entre empresas e administrações públicas na União, e oferece um conjunto de recomendações para assegurar uma partilha de dados entre empresas e administrações públicas escalável, responsável e sustentável, no interesse público. Além de recomendar à Comissão que explore a opção de um quadro jurídico neste domínio, apresenta várias formas de incentivar as empresas privadas a partilhar os seus dados, incluindo incentivos monetários e não monetários, por exemplo incentivos fiscais, investimento de fundos públicos para apoiar o desenvolvimento de instrumentos técnicos de confiança e sistemas de reconhecimento para a partilha de dados.

– **Seminário sobre rótulos para/certificação de prestadores de soluções técnicas para o intercâmbio de dados**. Cerca de cem participantes de empresas (incluindo PME), de instituições europeias e do meio académico participaram neste webinário, em 12 de maio de 2020, que tinha por objetivo analisar se um sistema de rotulagem ou certificação poderia impulsionar a adoção, por parte das empresas, de intermediários de dados, reforçando a confiança no ecossistema de dados.

– **Dez seminários organizados entre julho e novembro de 2019, que envolveram mais de 300 partes interessadas e abrangeram diferentes setores**. Os seminários debateram a forma como a organização da **partilha de dados em determinados domínios,** como o ambiente, a agricultura, a energia ou os cuidados de saúde, poderia beneficiar a sociedade no seu conjunto, ajudando os intervenientes públicos a conceber melhores políticas e a melhorar os serviços públicos, bem como os intervenientes privados a produzir serviços que contribuam para responder aos problemas da sociedade.

– **Consulta do painel de PME.** Esta consulta, organizada de outubro de 2018 a janeiro de 2019, procurou obter os pontos de vista das PME sobre os princípios e orientações da Comissão em matéria de partilha de dados entre empresas, publicados na Comunicação «Rumo a um espaço comum europeu de dados» e no documento de trabalho dos serviços da Comissão que o acompanha, de 25 de abril de 2018[51].

– **O último Eurobarómetro sobre o impacto da digitalização.** Este inquérito geral sobre a vida quotidiana dos europeus inclui perguntas sobre o controlo e a partilha de informações pessoais por parte das pessoas. Publicado em 5 de março de 2020,

[51] COM(2018)232 final; SWD(2018)125 final de 25.4.2018.

fornece informações sobre a vontade dos cidadãos europeus de partilharem as suas informações pessoais, nomeadamente em que condições.

– **O parecer da Autoridade Europeia para a Proteção de Dados** (AEPD) sobre a estratégia europeia para os dados[52]. Em 16 de junho de 2020, a AEPD adotou o Parecer 3/2020 sobre a estratégia europeia para os dados. A AEPD congratulou-se com a estratégia, considerando que a sua aplicação constitui uma oportunidade para dar um exemplo de um modelo alternativo de economia dos dados.

• **Avaliação de impacto**

A presente proposta é acompanhada por uma avaliação de impacto[53], apresentada ao Comité de Controlo da Regulamentação (CCR) em 29 de setembro de 2021 e 13 de dezembro de 2021. Em 21 de janeiro de 2022, o Comité emitiu um parecer favorável, com reservas.

• **Adequação e simplificação da regulamentação**

Ao clarificar que o direito *sui generis* ao abrigo da Diretiva Bases de Dados (Diretiva 96/9/CE) não se aplica às bases de dados que contenham dados gerados ou obtidos pela utilização de produtos ou serviços conexos, a proposta garante que o direito *sui generis* não interfere com os direitos das empresas e dos consumidores de acederem e utilizarem dados e de partilharem dados previstos no presente regulamento. A clarificação alinhará a aplicação do direito *sui generis* com o objetivo da proposta legislativa e terá um impacto positivo na aplicação uniforme das regras no mercado interno e na economia dos dados.

Ao facilitar o acesso e a utilização dos dados, o Regulamento Dados deverá reduzir os encargos, tanto no setor público como entre as empresas, principalmente em resultado da redução dos custos de transação e em termos de ganhos de eficiência. No âmbito da abordagem «entra um, sai um»[54], que visa minimizar os encargos para os cidadãos e as empresas relacionados com as implicações e os custos da aplicação da legislação, os encargos administrativos líquidos estimados do Regulamento Dados, com base na avaliação de impacto, têm em conta os benefícios que provavelmente não só compensam como superam largamente os custos administrativos associados.

• **Direitos fundamentais**

A proposta está em conformidade com a legislação da União em matéria de proteção dos dados pessoais e de privacidade das comunicações e dos equipamentos terminais e prevê garantias adicionais para o acesso aos dados pessoais, bem como nos casos sujeitos a direitos de propriedade intelectual.

No capítulo II, um elevado nível de defesa do consumidor é reforçado com o novo direito de acesso aos dados gerados pelos utilizadores em situações anteriormente não abrangidas pelo direito da União. O direito de utilizar e de dispor de bens legalmente adquiridos é reforçado com um direito de acesso aos dados gerados pela utilização de um objeto da Internet das coisas. Desta forma, o proprietário pode beneficiar de uma melhor experiência do utilizador e de uma gama mais vasta de serviços, por exemplo, de reparação e manutenção. No contexto da defesa do consumidor, os direitos das crianças enquanto consumidores vulneráveis merecem uma atenção especial e as regras do Regulamento Dados contribuirão para clarificar as situações de acesso e utilização dos dados.

52 Parecer 3/2020 da AEPD sobre a Estratégia Europeia para os Dados.

53 **[Inserir ligações para o documento final e para a ficha de síntese].**

54 SWD(2021) 305 final.

O direito de acesso de terceiros aos dados da Internet das coisas, a pedido do utilizador, limita a liberdade de empresa e a liberdade contratual do fabricante ou projetista de um produto ou serviço conexo. A justificação dessa limitação é o reforço da defesa do consumidor, em especial para promover os seus interesses económicos. O fabricante ou projetista de um produto ou serviço conexo tem normalmente o controlo exclusivo relativamente à utilização dos dados gerados pela utilização de um produto ou serviço conexo, o que contribui para efeitos de dependência e dificulta a entrada no mercado dos intervenientes que oferecem serviços pós-venda. O direito de acesso aos dados da Internet das coisas aborda esta situação, capacitando ainda mais os consumidores que utilizam produtos ou serviços conexos a controlarem de forma significativa a forma como os dados gerados pela sua utilização do produto ou serviço conexo são utilizados e favorecendo a inovação por parte de mais intervenientes no mercado. Por conseguinte, os consumidores podem beneficiar de uma maior escolha nos serviços pós-venda, como a reparação e a manutenção, deixando de depender apenas dos serviços do fabricante. A proposta facilita a portabilidade dos dados do utilizador para terceiros, permitindo assim uma oferta competitiva de serviços pós-venda, bem como uma maior inovação baseada em dados e o desenvolvimento de produtos ou serviços não relacionados com os inicialmente adquiridos ou subscritos pelo utilizador.

A limitação da liberdade contratual e de empresa do fabricante ou do projetista é proporcional e atenuada pela sua capacidade não afetada de também utilizar os dados, na medida em que tal esteja em consonância com a legislação aplicável e o acordo com o utilizador. Além disso, o fabricante ou projetista também beneficiarão do direito de exigir uma compensação para permitir o acesso de terceiros. O direito de acesso não prejudica os direitos existentes de acesso e portabilidade dos titulares dos dados ao abrigo do RGPD. Garantias adicionais asseguram uma utilização proporcional dos dados por terceiros.

No capítulo IV, um sistema equitativo e eficaz de proteção contra cláusulas contratuais abusivas na partilha de dados contribuirá para a capacidade de as micro, pequenas ou médias empresas exercerem uma atividade empresarial. Esta disposição restringe de forma limitada a liberdade contratual das empresas no seu âmbito de aplicação, uma vez que apenas se aplica a cláusulas contratuais abusivas relacionadas com o acesso e a utilização dos dados impostas unilateralmente por uma parte contratante a uma micro, pequena ou média empresa. Tal justifica-se pelo facto de as PME se encontrarem normalmente numa posição negocial mais fraca e, muitas vezes, não terem outra opção senão aceitar cláusulas contratuais «de pegar ou largar». A liberdade contratual não é, em grande medida, afetada, uma vez que apenas são anuladas cláusulas excessivas e abusivas e, se possível, o contrato celebrado permanece válido sem as cláusulas abusivas. Além disso, as partes ainda podem negociar individualmente uma cláusula contratual específica ([55]).

No capítulo V, as disposições relativas à partilha de dados entre empresas e administrações públicas com base numa necessidade excecional reforçarão a capacidade das autoridades públicas para tomarem medidas em prol do bem comum, nomeadamente para responder, prevenir ou ajudar na recuperação de emergências públicas. O setor privado também beneficia da simplificação dos procedimentos de pedido de dados.

No capítulo VI, as disposições relativas à mudança de prestador de serviços de tratamento de dados reforçam a posição dos clientes profissionais e salvaguardam a sua escolha de mudar de prestador de serviços. A limitação do direito de empresa dos prestadores de serviços de tratamento de dados justifica-se porque as novas regras abordam os efeitos de dependência no

[55] Para mais explicações sobre o teste do caráter abusivo e o princípio da liberdade contratual, ver a avaliação de impacto, anexo 11.

mercado dos serviços de computação em nuvem e periféricos e melhoram a escolha para os utilizadores profissionais e as pessoas singulares em matéria de serviços de tratamento de dados.

No capítulo X, a intervenção relativa ao direito *sui generis* sobre as bases de dados da Diretiva Bases de Dados não limita a proteção da propriedade intelectual nela prevista. Contribui antes para a segurança jurídica nos casos em que a proteção do direito *sui generis* era anteriormente pouco clara.

4. INCIDÊNCIA ORÇAMENTAL

A presente proposta não tem qualquer incidência orçamental.

5. OUTROS ELEMENTOS

- **Planos de execução e acompanhamento, avaliação e prestação de informações**

A nível setorial e macroeconómico, o estudo em curso sobre a monitorização do mercado de dados ajudará a acompanhar o impacto económico da presente proposta no crescimento do mercado de dados na União.

O impacto nas PME, nomeadamente a sua perceção dos problemas relacionados com o acesso e a utilização dos dados, será avaliado através de uma consulta de um painel de PME cinco anos após a adoção do Regulamento Dados.

Tendo em conta o papel central dos espaços comuns europeus de dados na execução da estratégia europeia para os dados, muitos dos efeitos da presente iniciativa serão acompanhados ao nível dos espaços de dados setoriais, e as informações recolhidas pelo Centro de Apoio aos Espaços de Dados, a financiar ao abrigo do Programa Europa Digital. A interação regular entre os serviços da Comissão, o Centro de Apoio e o Comité Europeu da Inovação de Dados (a criar na sequência da entrada em vigor do Regulamento Governação de Dados) deve constituir uma fonte de informações fiável que permita avaliar os progressos realizados.

Por último, quatro anos após a adoção do Regulamento Dados será lançada uma avaliação para avaliar a iniciativa e, se necessário, preparar novas ações.

- **Explicação pormenorizada das disposições específicas da proposta**

O capítulo I define o objeto e o âmbito do regulamento e estabelece as definições utilizadas no instrumento.

O capítulo II aumenta a segurança jurídica para os consumidores e as empresas acederem aos dados gerados pelos produtos ou serviços conexos de que são proprietários, arrendatários ou locatários. Os fabricantes e os projetistas têm de conceber os produtos de forma a tornar os dados facilmente acessíveis por defeito, e terão de garantir a transparência no que respeita aos dados que serão acessíveis e à forma de aceder a esses dados. As disposições deste capítulo não afetam a possibilidade de os fabricantes acederem aos dados dos produtos ou serviços conexos que oferecem, e utilizarem esses dados, se tal for acordado com o utilizador. O detentor de dados tem a obrigação de disponibilizar esses dados a terceiros a pedido do utilizador. Os utilizadores terão o direito de autorizar o detentor de dados a conceder acesso aos dados a terceiros prestadores de serviços, como os prestadores de serviços pós-venda. As micro e pequenas empresas ficarão isentas destas obrigações.

O capítulo III estabelece as regras gerais aplicáveis às obrigações de disponibilização de dados. Caso um detentor de dados seja obrigado a disponibilizar dados a um destinatário de dados, conforme previsto no capítulo II ou noutra disposição do direito da União ou da legislação de um Estado-Membro, o quadro geral aborda as condições em que os dados são disponibilizados e a compensação por essa disponibilização. Quaisquer condições terão de ser equitativas e não discriminatórias, e qualquer compensação terá de ser razoável, sem impedir que outras disposições do direito da União ou da legislação nacional que transpõe o direito da União excluam a compensação ou prevejam uma compensação mais baixa pela disponibilização de dados. Qualquer compensação fixada para as PME não pode exceder os custos incorridos com a disponibilização dos dados, salvo disposição em contrário na legislação setorial. Os organismos de resolução de litígios certificados pelos Estados-Membros podem ajudar as partes que discordem no que respeita à compensação ou às condições a chegarem a um acordo.

O capítulo IV aborda o caráter abusivo das cláusulas contratuais nos contratos de partilha de dados entre empresas, em situações em que uma cláusula contratual é imposta unilateralmente por uma parte a uma micro, pequena ou média empresa. Este capítulo garante que os acordos contratuais sobre o acesso e a utilização dos dados não tiram partido dos desequilíbrios no poder negocial entre as partes contratantes. O instrumento de um teste do caráter abusivo inclui uma disposição geral que define o caráter abusivo de uma cláusula contratual relacionada com a partilha de dados, complementada por uma lista de cláusulas que são sempre abusivas ou que se presume serem abusivas. Em situações de poder negocial desigual, este teste protege a parte contratual mais fraca, a fim de evitar contratos abusivos. Esse caráter abusivo impede a utilização de dados por ambas as partes contratantes. Deste modo, as disposições asseguram uma distribuição mais equitativa do valor na economia dos dados[56]. Os modelos de cláusulas contratuais recomendados pela Comissão podem ajudar as partes comerciais a celebrar contratos baseados em cláusulas equitativas.

O capítulo V cria um quadro harmonizado para a utilização de dados na posse das empresas por organismos do setor público e instituições, agências e organismos da União em situações em que existe uma necessidade excecional dos dados solicitados. O quadro baseia-se numa obrigação de disponibilizar os dados e só será aplicável em caso de emergências públicas ou em situações em que os organismos do setor público tenham uma necessidade excecional de utilizar determinados dados, mas tais dados não possam ser obtidos no mercado, em tempo útil, através da adoção de nova legislação ou de obrigações de comunicação existentes. Em caso de necessidade excecional para responder a emergências públicas, como emergências de saúde pública, ou catástrofes naturais ou provocadas pelo homem de grandes proporções, os dados seriam disponibilizados gratuitamente. Noutros casos de necessidade excecional, nomeadamente para prevenir uma emergência pública ou apoiar a recuperação posterior, o detentor de dados que disponibiliza os dados deve ter direito a uma compensação que inclua os custos relacionados com a disponibilização dos dados pertinentes, acrescida de uma margem razoável. Para garantir que o direito de solicitar dados não é utilizado de forma abusiva e que o setor público continua a ser responsável pela sua utilização, os pedidos de dados devem ser proporcionais, indicar claramente o objetivo a alcançar, e respeitar os interesses da empresa que disponibiliza os dados. As autoridades competentes assegurariam a transparência e a disponibilização pública de todos os pedidos. Tratariam igualmente quaisquer reclamações daí resultantes.

[56] Para mais explicações sobre o teste do caráter abusivo, nomeadamente sobre o funcionamento na prática, ver o anexo 11 da avaliação de impacto.

O capítulo VI introduz requisitos regulamentares mínimos de natureza contratual, comercial e técnica, impostos aos prestadores de serviços de computação em nuvem, periféricos e outros serviços de tratamento de dados, a fim de permitir a mudança entre esses serviços. Em particular, a proposta garante que os clientes mantêm a equivalência funcional (um nível mínimo de funcionalidade) do serviço após terem mudado para outro prestador de serviços. A proposta contém uma exceção para a inviabilidade técnica, mas impõe o ónus da prova a este respeito ao prestador de serviços. A proposta não impõe normas ou interfaces técnicas específicas. No entanto, exige que os serviços sejam compatíveis com as normas europeias ou as especificações técnicas de interoperabilidade aberta, caso existam.

O capítulo VII aborda o acesso ilícito de terceiros a dados não pessoais detidos na União por serviços de tratamento de dados oferecidos no mercado da União. A proposta não afeta a base jurídica dos pedidos de acesso a dados na posse de cidadãos ou empresas da UE e não prejudica o quadro da União em matéria de proteção de dados e privacidade. Oferece garantias específicas, através da obrigação de os prestadores terem de tomar todas as medidas técnicas, jurídicas e organizativas razoáveis para impedir o acesso que seja incompatível com as obrigações concorrentes de proteger esses dados ao abrigo do direito da União, a menos que sejam cumpridas condições rigorosas. O regulamento respeita os compromissos internacionais da União no âmbito da OMC e dos acordos comerciais bilaterais.

O capítulo VIII prevê requisitos essenciais a cumprir em matéria de interoperabilidade para os operadores de espaços de dados e prestadores de serviços de tratamento de dados, bem como requisitos essenciais para contratos inteligentes. Permite também especificações de interoperabilidade aberta e normas europeias para a interoperabilidade dos serviços de tratamento de dados, a fim de promover um ambiente de computação em nuvem sem descontinuidades entre vários prestadores.

O capítulo IX estabelece o quadro de execução com as autoridades competentes em cada Estado-Membro, incluindo um mecanismo de tratamento de reclamações. A Comissão deve recomendar modelos de cláusulas contratuais voluntários no que respeita ao acesso e utilização dos dados. Em caso de infrações do presente regulamento são aplicáveis sanções.

O capítulo X contém uma disposição para que o direito *sui generis* estabelecido na Diretiva 96/9/CE não seja aplicável às bases de dados que contenham dados obtidos ou gerados pela utilização de um produto ou serviço conexo para impedir o exercício efetivo do direito dos utilizadores de acederem aos dados e de os utilizarem em conformidade com o artigo 4.º do presente regulamento ou do direito de partilharem esses dados com terceiros, em conformidade com o artigo 5.º do presente regulamento.

O capítulo XI confere à Comissão o poder de adotar atos delegados para introduzir um mecanismo de acompanhamento relativo aos encargos decorrentes da mudança impostos aos prestadores de serviços de tratamento de dados, para especificar mais pormenorizadamente os requisitos essenciais em matéria de interoperabilidade, e para publicar a referência das especificações de interoperabilidade aberta e normas europeias para a interoperabilidade dos serviços de tratamento de dados. Prevê também o procedimento de comité para a adoção de atos de execução destinados a facilitar a adoção de especificações comuns para a interoperabilidade e os contratos inteligentes nos casos em que não existam normas harmonizadas ou em que estas sejam insuficientes para garantir a conformidade com os requisitos essenciais. A proposta clarifica também a relação com outros atos jurídicos da União que regem os direitos e as obrigações em matéria de partilha de dados.

2022/0047 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização (Regulamento 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 114.º,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu[57],

Tendo em conta o parecer do Comité das Regiões[58],

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1) Nos últimos anos, as tecnologias baseadas em dados tiveram efeitos transformadores em todos os setores da economia. A proliferação de produtos ligados à Internet das coisas, em particular, aumentou o volume e o valor potencial dos dados para os consumidores, as empresas e a sociedade. Dados interoperáveis e de elevada qualidade provenientes de diferentes domínios aumentam a competitividade e a inovação e asseguram um crescimento económico sustentável. O mesmo conjunto de dados pode ser potencialmente utilizado e reutilizado para diversos fins e a um nível ilimitado, sem prejuízo da sua qualidade ou quantidade.

(2) Os obstáculos à partilha de dados impedem a melhor distribuição dos dados em benefício da sociedade. Esses obstáculos incluem a ausência de incentivos para que os detentores de dados celebrem voluntariamente acordos de partilha de dados, a incerteza quanto aos direitos e obrigações relacionados com os dados, os custos da contratação e da execução de interfaces técnicas, o elevado nível de fragmentação da informação em silos de dados, a má gestão dos metadados, a ausência de normas para a interoperabilidade semântica e técnica, os estrangulamentos que impedem o acesso aos dados, a ausência de práticas comuns de partilha de dados e os abusos de desequilíbrios contratuais no que respeita ao acesso e à utilização dos dados.

(3) Nos setores que se caracterizam pela presença de micro, pequenas e médias empresas, verifica-se muitas vezes a ausência de capacidades e competências digitais para recolher, analisar e utilizar dados, sendo o acesso frequentemente limitado caso um

[57] JO C […] de […], p. […].
[58] JO C […] de […], p. […].

único interveniente os detenha no sistema ou devido à falta de interoperabilidade entre dados, entre serviços de dados ou a nível transfronteiriço.

(4) A fim de responder às necessidades da economia digital e de eliminar os obstáculos ao bom funcionamento do mercado interno dos dados, é necessário estabelecer um quadro harmonizado que especifique quem, para além do fabricante ou de outro detentor de dados, tem direito a aceder aos dados gerados por produtos ou serviços conexos, em que condições e com que fundamento. Por conseguinte, os Estados-Membros não devem adotar ou manter requisitos nacionais adicionais sobre as matérias abrangidas pelo presente regulamento, salvo se explicitamente previsto no mesmo, uma vez que tal afetaria a sua aplicação direta e uniforme.

(5) O presente regulamento garante que os utilizadores de um produto ou serviço conexo na União podem aceder, em tempo útil, aos dados gerados pela utilização desse produto ou serviço conexo, e que podem utilizar esses dados, nomeadamente partilhando-os com terceiros da sua escolha. Impõe ao detentor de dados a obrigação de os disponibilizar, em determinadas circunstâncias, aos utilizadores e aos terceiros designados pelos utilizadores. Garante também que os detentores de dados disponibilizam os dados aos destinatários de dados na União ao abrigo de cláusulas equitativas, razoáveis e não discriminatórias e de forma transparente. As regras do direito privado são fundamentais no quadro global da partilha de dados. Por conseguinte, o presente regulamento adapta as regras do direito contratual e impede a exploração dos desequilíbrios contratuais que dificultam o acesso e a utilização equitativa dos dados pelas micro, pequenas ou médias empresas, na aceção da Recomendação 2003/361/CE. O presente regulamento garante também que, em caso de necessidade excecional, os detentores de dados disponibilizam aos organismos do setor público dos Estados-Membros e às instituições, agências ou organismos da União os dados necessários para o desempenho de funções de interesse público. Além disso, visa facilitar a mudança entre serviços de tratamento de dados e reforçar a interoperabilidade dos dados e dos mecanismos e serviços de partilha de dados na União. O presente regulamento não deve ser interpretado como reconhecendo ou criando qualquer base jurídica para que o detentor de dados conserve os dados, aceda aos mesmos ou proceda ao seu tratamento, nem como conferindo ao detentor de dados um novo direito de utilizar os dados gerados pela utilização de um produto ou serviço conexo. Em vez disso, toma como ponto de partida o controlo que o detentor de dados tem efetivamente, *de facto* ou *de jure*, sobre os dados gerados por produtos ou serviços conexos.

(6) A geração de dados é o resultado das ações de, pelo menos, dois intervenientes, a saber, o projetista ou o fabricante de um produto e o utilizador desse produto. Suscita questões de equidade na economia digital, uma vez que os dados registados por esses produtos ou serviços conexos constituem um contributo importante para os serviços pós-venda, auxiliares e outros. A fim de tirar partido dos importantes benefícios económicos dos dados como um bem não rival para a economia e a sociedade, é preferível adotar uma abordagem geral de atribuição de direitos de acesso e de utilização sobre os dados em detrimento da concessão de direitos exclusivos de acesso e utilização.

(7) O direito fundamental à proteção dos dados pessoais está salvaguardado, em particular, no Regulamento (UE) 2016/679 e no Regulamento (UE) 2018/1725. Além disso, a Diretiva 2002/58/CE protege a vida privada e a confidencialidade das comunicações, nomeadamente através da criação de condições para qualquer armazenamento de dados pessoais e não pessoais em equipamentos terminais e para

qualquer acesso a partir dos mesmos. Estes instrumentos constituem a base para um tratamento de dados sustentável e responsável, nomeadamente quando os conjuntos de dados incluem uma combinação de dados pessoais e não pessoais. O presente regulamento complementa e não prejudica o direito da União em matéria de proteção de dados e privacidade, nomeadamente o Regulamento (UE) 2016/679 e a Diretiva 2002/58/CE. Nenhuma disposição do presente regulamento deve ser aplicada ou interpretada de forma a diminuir ou limitar o direito à proteção dos dados pessoais ou o direito à privacidade e à confidencialidade das comunicações.

(8) Os princípios da minimização dos dados e da proteção de dados desde a conceção e por defeito são essenciais quando o tratamento envolve riscos significativos para os direitos fundamentais das pessoas. Tendo em conta as técnicas mais avançadas, todas as partes envolvidas na partilha de dados devem aplicar medidas técnicas e organizativas para proteger esses direitos, nomeadamente quando abrangidas pelo presente regulamento. Tais medidas incluem não só a pseudonimização e a cifragem, mas também a utilização de tecnologias cada vez mais disponíveis que permitem a introdução de algoritmos nos dados, bem como a obtenção de informações valiosas sem a transmissão entre as partes ou a cópia desnecessária dos próprios dados em bruto ou estruturados.

(9) O presente regulamento complementa e não prejudica o direito da União que visa promover os interesses dos consumidores e assegurar um elevado nível de defesa dos consumidores, a fim de proteger a sua saúde, segurança e interesses económicos, nomeadamente a Diretiva 2005/29/CE do Parlamento Europeu e do Conselho[59], a Diretiva 2011/83/UE do Parlamento Europeu e do Conselho[60] e a Diretiva 93/13/CEE do Parlamento Europeu e do Conselho[61].

(10) O presente regulamento não prejudica os atos jurídicos da União que preveem a partilha, o acesso e a utilização de dados para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, ou para efeitos aduaneiros e fiscais, independentemente da base jurídica do Tratado sobre o Funcionamento da União Europeia com base na qual tenham sido adotados. Tais atos incluem o Regulamento (UE) 2021/784 do Parlamento Europeu e do Conselho, de 29 de abril de 2021, relativo ao combate à difusão de conteúdos terroristas em linha, as [propostas relativas às provas eletrónicas [COM (2018) 225 e 226] uma vez adotadas], a [Proposta de] Regulamento do Parlamento Europeu e do Conselho relativo a um mercado único de serviços digitais (Regulamento Serviços Digitais) e que altera a Diretiva 2000/31/CE, bem como a cooperação internacional neste contexto, em particular com base na Convenção do Conselho da Europa sobre o cibercrime de 2001 («Convenção de Budapeste»). O presente regulamento não prejudica as competências

---

59 Diretiva 2005/29/CE do Parlamento Europeu e do Conselho, de 11 de maio de 2005, relativa às práticas comerciais desleais das empresas face aos consumidores no mercado interno e que altera a Diretiva 84/450/CEE do Conselho, as Diretivas 97/7/CE, 98/27/CE e 2002/65/CE e o Regulamento (CE) n. º2006/2004 («diretiva relativa às práticas comerciais desleais») (JO L 149 de 11.6.2005, p. 22).

60 Diretiva 2011/83/UE do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa aos direitos dos consumidores, que altera a Diretiva 93/13/CEE do Conselho e a Diretiva 1999/44/CE do Parlamento Europeu e do Conselho e que revoga a Diretiva 85/577/CEE do Conselho e a Diretiva 97/7/CE do Parlamento Europeu e do Conselho.

61 Diretiva 93/13/CEE do Conselho, de 5 de abril de 1993, relativa às cláusulas abusivas nos contratos celebrados com os consumidores. Diretiva (UE) 2019/2161 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, que altera a Diretiva 93/13/CEE do Conselho e as Diretivas 98/6/CE, 2005/29/CE e 2011/83/UE do Parlamento Europeu e do Conselho a fim de assegurar uma melhor aplicação e a modernização das regras da União em matéria de defesa dos consumidores.

dos Estados-Membros no que respeita às atividades relacionadas com a segurança pública, a defesa e a segurança nacional, em conformidade com o direito da União, e as atividades das alfândegas em matéria de gestão dos riscos e, em geral, de verificação do cumprimento do Código Aduaneiro pelos operadores económicos.

(11) O direito da União que estabelece requisitos em matéria de conceção física e de dados dos produtos a colocar no mercado da União não deve ser afetado pelo presente regulamento.

(12) O presente regulamento complementa e não prejudica o direito da União que visa estabelecer requisitos de acessibilidade de determinados produtos e serviços, em especial a Diretiva 2019/882[62].

(13) O presente regulamento não prejudica as competências dos Estados-Membros no que respeita às atividades relacionadas com a segurança pública, a defesa e a segurança nacional, em conformidade com o direito da União, e as atividades das alfândegas em matéria de gestão dos riscos e, em geral, de verificação do cumprimento do Código Aduaneiro pelos operadores económicos.

(14) Os produtos físicos que obtêm, geram ou recolhem, através dos seus componentes, dados relativos ao seu desempenho, utilização ou ambiente, e que são capazes de comunicar esses dados através de um serviço de comunicações eletrónicas acessível ao público (frequentemente designado por «Internet das coisas») devem ser abrangidos pelo presente regulamento. Os serviços de comunicações eletrónicas incluem as redes telefónicas terrestres, as redes de televisão por cabo, as redes por satélite e as redes de comunicação de campo próximo. Tais produtos podem incluir veículos, equipamentos domésticos e bens de consumo, dispositivos médicos e sanitários ou máquinas agrícolas e industriais. Os dados representam a digitalização das ações e eventos do utilizador e, por conseguinte, devem ser acessíveis ao mesmo, ao passo que as informações obtidas ou inferidas a partir desses dados, quando detidas legalmente, não devem considerar-se abrangidas pelo presente regulamento. Tais dados são potencialmente valiosos para o utilizador e apoiam a inovação e o desenvolvimento de serviços digitais e de outros serviços que protegem o ambiente, a saúde e a economia circular, em particular por facilitarem a manutenção e a reparação dos produtos em questão.

(15) Em contrapartida, determinados produtos que são principalmente concebidos para apresentar ou reproduzir conteúdos, ou para gravar e transmitir conteúdos, incluindo para utilização por um serviço em linha, não devem ser abrangidos pelo presente regulamento. Tais produtos incluem, por exemplo, computadores pessoais, servidores, tábletes e telemóveis inteligentes, câmaras fotográficas, câmaras Web, sistemas de gravação de som e digitalizadores de texto. Necessitam de intervenção humana para produzir várias formas de conteúdo, como documentos de texto, ficheiros de som, ficheiros de vídeo, jogos, mapas digitais.

(16) É necessário estabelecer regras aplicáveis aos produtos conectados que incorporem ou estejam interligados com um serviço cuja ausência impeça o produto de desempenhar as suas funções. Tais serviços conexos podem fazer parte do contrato de venda, arrendamento ou locação, ou são normalmente prestados para produtos do mesmo tipo, podendo o utilizador razoavelmente esperar que sejam fornecidos dada a natureza do produto e tendo em conta qualquer declaração pública feita pelo vendedor,

[62] Diretiva (UE) 2019/882 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos requisitos de acessibilidade dos produtos e serviços (JO L 151 de 7.6.2019, p. 70).

arrendatário, locador ou outras pessoas, ou em nome dos mesmos, em estádios anteriores da cadeia contratual, nomeadamente pelo fabricante. Esses serviços conexos podem, por sua vez, gerar dados de valor para o utilizador, independentemente das capacidades de recolha de dados do produto com o qual estão interligados. O presente regulamento deve também aplicar-se a um serviço conexo que não seja prestado pelo próprio vendedor, arrendatário ou locador, mas que seja prestado por um terceiro ao abrigo de um contrato de venda, arrendamento ou locação. Em caso de dúvida sobre se a prestação do serviço faz parte do contrato de venda, arrendamento ou locação, o presente regulamento deve ser aplicável.

(17) Os dados gerados pela utilização de um produto ou serviço conexo incluem os dados registados intencionalmente pelo utilizador. Incluem também os dados gerados como subproduto da ação do utilizador, como dados de diagnóstico, e sem qualquer ação por parte do mesmo, por exemplo quando o produto se encontra em «modo de espera», e os dados registados durante os períodos em que o produto está desligado. Devem incluir dados na forma e no formato em que são gerados pelo produto, mas não os dados resultantes de qualquer processo do *software* que calcule dados derivados desses dados, uma vez que esse processo pode estar sujeito a direitos de propriedade intelectual.

(18) O utilizador de um produto deve ser entendido como a pessoa singular ou coletiva, por exemplo uma empresa ou um consumidor, que adquiriu, arrendou ou alugou o produto. Em função do título jurídico ao abrigo do qual o utiliza, esse utilizador suporta os riscos e usufrui dos benefícios da utilização do produto conectado, devendo também beneficiar do acesso aos dados que gera. Por conseguinte, o utilizador deve ter o direito de retirar benefícios dos dados gerados por esse produto e por qualquer serviço conexo.

(19) Na prática, nem todos os dados gerados por produtos ou serviços conexos são facilmente acessíveis aos seus utilizadores e as possibilidades de portabilidade dos dados gerados por produtos conectados à Internet das Coisas são, muitas vezes, limitadas. Os utilizadores não conseguem obter os dados necessários para recorrer a prestadores de serviços de reparação e outros, e as empresas não conseguem lançar serviços inovadores, mais eficientes e convenientes. Em muitos setores, os fabricantes são frequentemente capazes de determinar, através do seu controlo da conceção técnica do produto ou dos serviços conexos, quais os dados gerados e a forma de lhes aceder apesar de não terem direito legal aos mesmos. Por conseguinte, é necessário assegurar que os produtos são concebidos e fabricados e que os serviços conexos são prestados de modo a que os dados gerados pela sua utilização sejam sempre facilmente acessíveis ao utilizador.

(20) Caso várias pessoas ou entidades sejam proprietárias de um produto ou sejam parte num contrato de locação ou de arrendamento e beneficiem do acesso a um serviço conexo, devem envidar-se esforços razoáveis na conceção do produto ou serviço conexo ou da interface pertinente para que todas as pessoas possam ter acesso aos dados que geram. Os utilizadores de produtos que geram dados exigem normalmente a criação de uma conta de utilizador. Tal permite a identificação do utilizador pelo fabricante, bem como um meio de comunicação para o exercício e o tratamento dos pedidos de acesso aos dados. Os fabricantes ou projetistas de um produto que seja normalmente utilizado por várias pessoas devem criar o mecanismo obrigatório que possibilite contas de utilizador separadas para pessoas individuais, se for caso disso, ou a várias pessoas utilizarem a mesma conta de utilizador. O acesso deve ser concedido ao utilizador mediante mecanismos de pedido simples que garantam a

execução automática e que não exijam uma análise ou autorização por parte do fabricante ou do detentor de dados. Tal significa que os dados só devem ser disponibilizados caso o utilizador efetivamente o deseje. Se a execução automática do pedido de acesso aos dados não for possível, por exemplo, através de uma conta de utilizador ou de uma aplicação móvel de acompanhamento fornecida com o produto ou serviço, o fabricante deve informar o utilizador sobre a forma de aceder aos dados.

(21) Os produtos podem ser concebidos para disponibilizar diretamente determinados dados a partir de um armazenamento de dados no dispositivo ou de um servidor remoto ao qual se comuniquem os dados. O acesso ao armazenamento de dados no dispositivo pode realizar-se por meio de redes locais por cabo ou sem fios ligadas a um serviço de comunicações eletrónicas acessível ao público ou a uma rede móvel. O servidor pode ser a capacidade do servidor local do próprio fabricante ou a capacidade de um terceiro ou de um prestador de serviços de computação em nuvem que funcione como detentor de dados, cuja conceção deve permitir que o utilizador ou um terceiro trate os dados no produto ou numa instância informática do fabricante.

(22) Os assistentes virtuais desempenham um papel cada vez mais importante na digitalização dos ambientes de consumo e funcionam como uma interface de fácil utilização para reproduzir conteúdos, obter informações ou ativar objetos físicos ligados à Internet das coisas. Podem funcionar como um portal único, por exemplo, num ambiente doméstico inteligente e registar quantidades significativas de dados pertinentes sobre a forma como os utilizadores interagem com os produtos ligados à Internet das coisas, incluindo os fabricados por outras partes, podendo também substituir a utilização de interfaces fornecidas pelos fabricantes, como ecrãs táteis ou aplicações para telemóveis inteligentes. O utilizador pode querer disponibilizar esses dados a fabricantes terceiros e permitir novos serviços domésticos inteligentes. Esses assistentes virtuais devem ser abrangidos pelo direito de acesso aos dados previsto no presente regulamento também no que respeita aos dados registados antes da ativação do assistente virtual pela palavra de ativação e aos dados gerados quando um utilizador interage com um produto através de um assistente virtual fornecido por uma entidade que não o fabricante do produto. No entanto, apenas os dados resultantes da interação entre o utilizador e o produto através do assistente virtual estão abrangidos pelo presente regulamento. Os dados produzidos pelo assistente virtual não relacionados com a utilização de um produto não são objeto do presente regulamento.

(23) Antes da celebração de um contrato de compra, arrendamento ou locação de um produto ou de prestação de um serviço conexo, devem ser facultadas ao utilizador informações claras e suficientes sobre a forma de aceder aos dados gerados. Esta obrigação proporciona transparência relativamente aos dados gerados e melhora a facilidade de acesso do utilizador. A obrigação de facultar informações não afeta a obrigação de o responsável pelo tratamento fornecer informações ao titular dos dados nos termos dos artigos 12.º, 13.º e 14.º do Regulamento (UE) 2016/679.

(24) O presente regulamento impõe aos detentores de dados a obrigação de disponibilizarem os dados em determinadas circunstâncias. Caso esteja em causa o tratamento de dados pessoais, o detentor de dados deve ser um responsável pelo tratamento nos termos do Regulamento (UE) 2016/679. Sempre que os utilizadores sejam titulares dos dados, os detentores de dados devem ser obrigados a facultar-lhes o acesso aos seus dados e a disponibilizá-los a terceiros escolhidos pelo utilizador, em conformidade com o presente regulamento. No entanto, o presente regulamento não cria uma base jurídica nos termos do Regulamento (UE) 2016/679 para que o detentor de dados faculte o acesso aos dados pessoais ou os disponibilize a terceiros, a pedido

de um utilizador que não seja titular dos dados, e não deve ser entendido como conferindo ao detentor de dados um novo direito de utilizar os dados gerados pela utilização de um produto ou serviço conexo. Tal aplica-se, em especial, quando o fabricante é o detentor de dados. Nesse caso, o fundamento para o fabricante utilizar dados não pessoais deve ser um acordo contratual entre o fabricante e o utilizador. Esse acordo pode fazer parte do acordo de venda, arrendamento ou locação relativo ao produto. Qualquer cláusula contratual do acordo que estipule que o detentor de dados pode utilizar os dados gerados pelo utilizador de um produto ou serviço conexo deve ser transparente para o utilizador, nomeadamente no que respeita à finalidade para a qual o detentor de dados tenciona utilizar os dados. O presente regulamento não deve impedir condições contratuais que tenham por efeito excluir ou limitar a utilização dos dados, ou de determinadas categorias dos mesmos, pelo detentor de dados. Também não deve impedir requisitos regulamentares setoriais ao abrigo do direito da União, ou do direito nacional compatível com o direito da União, que excluam ou limitem a utilização de determinados dados pelo detentor de dados por razões de ordem pública bem definidas.

(25) Nos setores que se caracterizam pela concentração de um pequeno número de fabricantes que fornecem utilizadores finais, os utilizadores dispõem apenas de opções limitadas no que respeita à partilha de dados com esses fabricantes. Em tais circunstâncias, os acordos contratuais podem não ser suficientes para alcançar o objetivo de capacitação dos utilizadores. Os dados tendem a permanecer sob o controlo dos fabricantes, o que dificulta que os utilizadores obtenham valor dos dados gerados pelos equipamentos que compram ou alugam. Consequentemente, o potencial para as pequenas empresas inovadoras oferecerem soluções baseadas em dados de forma competitiva e para uma economia de dados diversificada na Europa é limitado. Por conseguinte, o presente regulamento deve basear-se na evolução recente em setores específicos, como o Código de conduta sobre a partilha de dados agrícolas através de acordo contratual. Poderá apresentar-se legislação setorial para dar resposta a necessidades e objetivos setoriais específicos. Além disso, o detentor de dados não deve utilizar quaisquer dados gerados pela utilização do produto ou serviço conexo para obter informações sobre a situação económica do utilizador, os seus ativos ou métodos de produção, nem utilizá-los de qualquer outra forma que possa prejudicar a posição comercial do utilizador nos mercados em que tem atividade. Tal envolveria, por exemplo, utilizar os conhecimentos sobre o desempenho geral de uma empresa ou de uma exploração agrícola em negociações contratuais com o utilizador sobre a potencial aquisição dos produtos ou produtos agrícolas do utilizador em detrimento do mesmo, ou, por exemplo, utilizar essa informação para alimentar bases de dados maiores em certos mercados no agregado (por exemplo, bases de dados sobre os rendimentos das colheitas para a época de colheita seguinte), uma vez que tal utilização poderia afetar negativamente o utilizador de uma forma indireta. O utilizador deve dispor da interface técnica necessária para gerir as autorizações, de preferência com opções de autorização granulares (como «permitir uma vez» ou «permitir durante a utilização desta aplicação ou serviço»), incluindo a opção de retirar a autorização.

(26) Nos contratos entre um detentor de dados e um consumidor na qualidade de utilizador de um produto ou serviço conexo que gera dados, a Diretiva 93/13/CEE é aplicável às cláusulas contratuais, a fim de garantir que o consumidor não está sujeito a cláusulas contratuais abusivas. No caso de cláusulas contratuais abusivas impostas unilateralmente a uma micro, pequena ou média empresa, na aceção do artigo 2.º do

anexo da Recomendação 2003/361/CE[63], o presente regulamento estabelece que essas cláusulas abusivas não devem ser vinculativas para essa empresa.

(27) O detentor dos dados pode exigir que o utilizador se identifique de forma adequada para verificar o seu direito de acesso aos dados. No caso de dados pessoais tratados por um subcontratante em nome do responsável pelo tratamento, o detentor dos dados deve assegurar que o pedido de acesso é recebido e tratado pelo subcontratante.

(28) O utilizador deve ser livre de utilizar os dados para qualquer finalidade lícita, o que inclui o fornecimento dos dados que o utilizador recebeu, no exercício do direito nos termos do presente regulamento de um terceiro prestar um serviço pós-venda que possa estar em concorrência com um serviço prestado pelo detentor dos dados, ou dar instruções ao detentor dos dados para o fazer. O detentor dos dados deve assegurar que os dados disponibilizados a terceiros são tão exatos, completos, fiáveis, pertinentes e atualizados como os dados aos quais o próprio detentor pode ou tem direito a aceder a partir da utilização do produto ou serviço conexo. O tratamento dos dados deve respeitar quaisquer segredos comerciais ou direitos de propriedade intelectual. É importante preservar os incentivos ao investimento em produtos com funcionalidades baseadas na utilização de dados provenientes de sensores incorporados nesse produto. Por conseguinte, o objetivo do presente regulamento deve ser entendido no sentido de promover o desenvolvimento de produtos novos e inovadores ou de serviços conexos, estimular a inovação nos mercados pós-venda, mas também estimular o desenvolvimento de serviços inteiramente inovadores que utilizem os dados, nomeadamente com base em dados de vários produtos ou serviços conexos. Ao mesmo tempo, visa evitar comprometer os incentivos ao investimento para o tipo de produto a partir do qual os dados são obtidos, por exemplo, através da utilização de dados para o desenvolvimento de um produto concorrente.

(29) Um terceiro a quem sejam disponibilizados dados pode ser uma empresa, um organismo de investigação ou uma organização sem fins lucrativos. Ao disponibilizar os dados a terceiros, o detentor dos dados não deve abusar da sua posição para procurar obter uma vantagem concorrencial nos mercados em que o detentor e o terceiro possam estar em concorrência direta. Por conseguinte, o detentor dos dados não deve utilizar quaisquer dados gerados pela utilização do produto ou serviço conexo para obter informações sobre a situação económica do terceiro ou dos seus ativos ou métodos de produção, ou sobre a utilização de qualquer outra forma que possa prejudicar a posição comercial do terceiro nos mercados em que tem atividade.

(30) A utilização de um produto ou serviço conexo pode gerar dados relativos a uma pessoa singular identificada ou identificável (o titular dos dados), especialmente quando o utilizador é uma pessoa singular. O tratamento desses dados está sujeito às regras estabelecidas no Regulamento (UE) 2016/679, nomeadamente quando os dados pessoais e não pessoais de um conjunto de dados estejam indissociavelmente ligados[64]. O titular dos dados pode ser o utilizador ou outra pessoa singular. Os dados pessoais só podem ser solicitados por um responsável pelo tratamento ou por um titular dos dados. Um utilizador que seja o titular dos dados tem direito, em determinadas circunstâncias, nos termos do Regulamento (UE) 2016/679, a aceder aos dados pessoais que lhe digam respeito e esse direito não é afetado pelo presente regulamento. Nos termos do presente regulamento, o utilizador que seja uma pessoa singular tem

63 Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas.

64 JO L 303 de 28.11.2018, p. 59.

ainda o direito de aceder a todos os dados pessoais e não pessoais gerados pelo produto. Se o utilizador não for o titular dos dados, mas uma empresa, incluindo um comerciante individual, e não no caso de utilização doméstica conjunta do produto, o utilizador será um responsável pelo tratamento na aceção do Regulamento (UE) 2016/679. Por conseguinte, um utilizador que, na qualidade de responsável pelo tratamento, pretenda solicitar dados pessoais gerados pela utilização de um produto ou serviço conexo deve ter uma base jurídica para o tratamento dos dados, nos termos do artigo 6.º, n.º 1, do Regulamento (UE) 2016/679, como o consentimento do titular dos dados ou o interesse legítimo. Esse utilizador deve assegurar que o titular dos dados é devidamente informado das finalidades determinadas, explícitas e legítimas do tratamento desses dados e da forma como o titular dos dados pode exercer efetivamente os seus direitos. Caso o detentor e o utilizador dos dados sejam responsáveis conjuntos pelo tratamento na aceção do artigo 26.º do Regulamento (UE) 2016/679, devem determinar, de uma forma transparente por meio de um acordo entre si, as respetivas responsabilidades pelo cumprimento do referido regulamento. Deve entender-se que esse utilizador, depois da disponibilização dos dados, pode, por sua vez, tornar-se detentor dos dados, se satisfizer os critérios do presente regulamento e, assim, ficar sujeito às obrigações de disponibilização de dados nos termos do presente regulamento.

(31) Os dados gerados pela utilização de um produto ou serviço conexo só devem ser disponibilizados a terceiros mediante pedido do utilizador. Por conseguinte, o presente regulamento complementa o direito previsto no artigo 20.º do Regulamento (UE) 2016/679. Esse artigo prevê o direito de os titulares receberem os dados pessoais que lhes digam respeito num formato estruturado, de uso corrente e de leitura automática, e de os transferirem para outros responsáveis pelo tratamento, se o tratamento desses dados se basear no artigo 6.º, n.º 1, alínea a), ou no artigo 9.º, n.º 2, alínea a), ou num contrato nos termos do artigo 6.º, n.º 1, alínea b). Os titulares dos dados têm igualmente o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, mas unicamente caso seja tecnicamente viável. O artigo 20.º especifica que diz respeito aos dados fornecidos pelo titular, mas não especifica se tal exige um comportamento ativo por parte do titular dos dados ou se também é aplicável a situações em que um produto ou serviço conexo, pela sua conceção, regista de forma passiva o comportamento de um titular de dados ou outras informações relativas a um titular de dados. O direito conferido ao abrigo do presente regulamento complementa, de várias formas, o direito de receber e transferir dados pessoais ao abrigo do artigo 20.º do Regulamento (UE) 2016/679. Concede aos utilizadores o direito de acesso e disponibilização a terceiros de quaisquer dados gerados pela utilização de um produto ou serviço conexo, independentemente da sua natureza enquanto dados pessoais, da distinção entre dados fornecidos ativamente ou registados de forma passiva e independentemente da base jurídica do tratamento. Ao contrário das obrigações técnicas previstas no artigo 20.º do Regulamento (UE) 2016/679, o presente regulamento impõe e garante a viabilidade técnica do acesso de terceiros a todos os tipos de dados que abrange, sejam dados pessoais ou não. Possibilita igualmente ao detentor dos dados fixar uma compensação razoável a suportar por terceiros, mas não pelo utilizador, quanto a quaisquer custos incorridos com a disponibilização de acesso direto aos dados gerados pelo produto do utilizador. Se um detentor de dados e um terceiro não conseguirem chegar a acordo sobre as condições desse acesso direto, o titular dos dados não deve, de modo algum, ser impedido de exercer os direitos previstos no Regulamento (UE) 2016/679, incluindo o direito à portabilidade dos dados, através de vias de recurso nos termos do

referido regulamento. Neste contexto, deve entender-se que, em conformidade com o Regulamento (UE) 2016/679, um acordo contratual não permite o tratamento de categorias especiais de dados pessoais pelo detentor dos dados ou pelo terceiro.

(32) O acesso a quaisquer dados armazenados em equipamentos terminais, e acedidos a partir dos mesmos, está sujeito ao disposto na Diretiva 2002/58/CE e requer o consentimento do assinante ou utilizador, na aceção da referida diretiva, a menos que seja estritamente necessário para a prestação de um serviço da sociedade da informação explicitamente solicitado pelo utilizador ou assinante (ou exclusivamente para efeitos de transmissão de uma comunicação). A Diretiva 2002/58/CE («Diretiva Privacidade Eletrónica») (bem como a proposta de Regulamento Privacidade Eletrónica) protege a integridade do equipamento terminal do utilizador no que diz respeito à utilização das capacidades de tratamento e armazenamento e à recolha de informações. Os equipamentos da Internet das coisas são considerados equipamentos terminais se estiverem direta ou indiretamente ligados a uma rede pública de comunicações.

(33) A fim de impedir a exploração dos utilizadores, os terceiros a quem os dados tenham sido disponibilizados mediante pedido do utilizador só podem proceder ao tratamento dos dados para os fins acordados com o utilizador e partilhá-los com outro terceiro unicamente se tal for necessário para a prestação do serviço solicitado pelo utilizador.

(34) Em consonância com o princípio da minimização dos dados, o terceiro só deve ter acesso às informações adicionais necessárias para a prestação do serviço solicitado pelo utilizador. Tendo obtido acesso aos dados, o terceiro pode proceder ao seu tratamento exclusivamente para as finalidades acordadas com o utilizador, sem interferência do detentor dos dados. Para o utilizador, deve ser tão fácil recusar ou interromper o acesso aos dados por parte de terceiros como autorizar o acesso. O terceiro não deve coagir, enganar ou manipular o utilizador de forma alguma, subvertendo ou prejudicando a autonomia, a tomada de decisões ou as escolhas do utilizador, incluindo por meio de uma interface digital com o utilizador. Neste contexto, os terceiros não devem recorrer aos chamados «padrões obscuros» para a conceção das suas interfaces digitais. Os padrões obscuros consistem em técnicas de conceção que enganam ou induzem os consumidores em decisões que acarretam consequências negativas para os mesmos. Estas técnicas manipuladoras podem ser utilizadas para persuadir os utilizadores, em especial os consumidores vulneráveis, a adotar comportamentos indesejados, bem como para enganar os utilizadores incentivando-os a tomar decisões sobre operações de divulgação de dados ou distorcer indevidamente a tomada de decisões dos utilizadores do serviço, de uma forma que subverte e prejudica a sua autonomia, a tomada de decisões e a escolha. As práticas comerciais comuns e legítimas que estejam em conformidade com o direito da União não devem, por si só, ser consideradas padrões obscuros. Os terceiros devem cumprir as obrigações que lhes incumbem por força do direito da União aplicável, em especial os requisitos estabelecidos na Diretiva 2005/29/CE, na Diretiva 2011/83/UE, na Diretiva 2000/31/CE e na Diretiva 98/6/CE.

(35) O terceiro deve igualmente abster-se de utilizar os dados para identificar pessoas, a menos que essas atividades de tratamento sejam estritamente necessárias para a prestação do serviço solicitado pelo utilizador. O requisito de apagar os dados que já não sejam necessários para a finalidade acordada com o utilizador complementa o direito do titular dos dados ao apagamento, nos termos do artigo 17.º do Regulamento (UE) 2016/679. Caso o terceiro seja um prestador de um serviço de intermediação de dados na aceção do [Regulamento Governação de Dados], são

aplicáveis as garantias do titular dos dados previstas no referido regulamento. O terceiro pode utilizar os dados para desenvolver um produto ou um serviço conexo novo e inovador, mas não para desenvolver um produto concorrente.

(36) As empresas em fase de arranque, as pequenas e médias empresas e as empresas dos setores tradicionais com capacidades digitais menos desenvolvidas têm dificuldade em obter acesso a dados pertinentes. O presente regulamento visa facilitar o acesso destas entidades aos dados, assegurando simultaneamente que o âmbito das obrigações que lhes correspondem seja o mais proporcional possível, a fim de evitar o excesso de regulamentação. Ao mesmo tempo, surgiu um pequeno número de empresas de muito grande dimensão com um poder económico considerável na economia digital através da acumulação e da agregação de grandes volumes de dados e da infraestrutura tecnológica para os monetizar. Incluem-se nestas empresas as que prestam serviços essenciais de plataforma que controlam ecossistemas de plataforma completos na economia digital e que os operadores de mercado existentes ou novos são incapazes de desafiar ou contestar. O [Regulamento relativo à disputabilidade e equidade dos mercados no setor digital (Regulamento Mercados Digitais)] visa corrigir estas ineficiências e desequilíbrios, conferindo à Comissão o poder de designar um prestador na qualidade de «controlador de acesso» e impondo uma série de obrigações aos controladores de acesso designados, incluindo a proibição de combinar determinados dados sem consentimento e a obrigação de assegurar direitos efetivos de portabilidade dos dados nos termos do artigo 20.º do Regulamento (UE) 2016/679. Em consonância com o [Regulamento relativo à disputabilidade e equidade dos mercados no setor digital (Regulamento Mercados Digitais)], e tendo em conta a capacidade indisputada dessas empresas para obterem de dados, a inclusão dessas empresas controladoras de acesso como beneficiárias do direito de acesso aos dados não seria necessária para alcançar o objetivo do presente regulamento e, por conseguinte, seria desproporcional em relação aos detentores dos dados sujeitos a essas obrigações. Tal significa que uma empresa que preste serviços essenciais de plataforma que tenha sido designada como controladora de acesso não pode solicitar nem obter acesso aos dados dos utilizadores gerados pela utilização de um produto ou serviço conexo, ou por um assistente virtual, com base nas disposições do capítulo II do presente regulamento. Deve entender-se que uma empresa que preste serviços essenciais de plataforma designada como controladora de acesso nos termos do Regulamento Mercados Digitais inclui todas as entidades jurídicas de um grupo de empresas, caso uma entidade jurídica preste um serviço essencial de plataforma. Além disso, os terceiros a quem se disponibiliza dados mediante pedido do utilizador não podem disponibilizar os dados a um controlador de acesso designado. Por exemplo, o terceiro não pode subcontratar a prestação de serviços a um controlador de acesso. Não obstante, isso não impede que terceiros utilizem serviços de tratamento de dados prestados por um controlador de acesso designado. Esta exclusão dos controladores de acesso designados do âmbito do direito de acesso ao abrigo do presente regulamento não impede que essas empresas obtenham dados por outros meios lícitos.

(37) Tendo em conta o estado atual da tecnologia, é demasiado oneroso impor novas obrigações de conceção relativamente aos produtos fabricados ou concebidos e serviços conexos prestados por micro e pequenas empresas. Todavia, tal não é o caso quando uma micro ou pequena empresa é subcontratada para fabricar ou conceber um produto. Nessas situações, a empresa que subcontratou a micro ou a pequena empresa pode compensar adequadamente o subcontratante. Não obstante, uma micro ou pequena empresa pode estar sujeita aos requisitos estabelecidos no presente

regulamento na qualidade de detentor dos dados, caso não seja o fabricante do produto ou um prestador de serviços conexos.

(38) O presente regulamento contém regras gerais de acesso, aplicáveis sempre que um detentor de dados seja obrigado por lei a disponibilizá-los a um destinatário de dados. Esse acesso deve basear-se em condições justas, razoáveis, não discriminatórias e transparentes, a fim de assegurar a coerência das práticas em matéria de partilha de dados no mercado interno, incluindo entre setores, e de incentivar e promover práticas equitativas de partilha de dados, mesmo nos domínios em que esse direito de acesso aos dados não é concedido. Estas regras gerais de acesso não são aplicáveis às obrigações de disponibilização de dados nos termos do Regulamento (UE) 2016/679. A partilha voluntária de dados não é afetada por estas regras.

(39) Com base no princípio da liberdade contratual, as partes devem continuar a ser livres de negociar nos seus contratos as condições exatas para a disponibilização de dados, no quadro das regras gerais de acesso à disponibilização de dados.

(40) A fim de assegurar que as condições de acesso obrigatório aos dados sejam equitativas para ambas as partes, as regras gerais em matéria de direitos de acesso aos dados devem referir-se à regra relativa à prevenção de cláusulas contratuais abusivas.

(41) A fim de compensar a ausência de informações sobre as condições de diferentes contratos, o que torna difícil para o destinatário dos dados avaliar se as condições de disponibilização dos dados são não discriminatórias, deve caber ao detentor dos dados demonstrar que uma cláusula contratual não é discriminatória. Caso um detentor de dados utilize diferentes cláusulas contratuais para disponibilizar dados ou compensações diferentes, se essas diferenças forem justificadas por razões objetivas, não se trata de uma discriminação ilícita. Essas obrigações são aplicáveis sem prejuízo do disposto no Regulamento (UE) 2016/679.

(42) A fim de incentivar a continuação do investimento na geração de dados valiosos, incluindo investimentos em ferramentas técnicas pertinentes, o presente regulamento inclui o princípio de que o detentor dos dados pode solicitar uma compensação razoável quando for legalmente obrigado a disponibilizar os dados ao seu destinatário. Estas disposições não devem ser entendidas como pagamentos pelos próprios dados, mas, no caso das micro, pequenas ou médias empresas, pelos custos incorridos e pelo investimento necessário para a disponibilização dos dados.

(43) Em casos justificados, incluindo a necessidade de salvaguardar a participação dos consumidores e a concorrência ou de promover a inovação em determinados mercados, o direito da União ou a legislação nacional que transpõe o direito da União podem impor uma compensação regulamentada pela disponibilização de tipos específicos de dados.

(44) A fim de proteger as micro, pequenas ou médias empresas de encargos económicos excessivos que tornem demasiado difícil, do ponto de vista comercial, o desenvolvimento e a gestão de modelos empresariais inovadores, a compensação que têm de pagar pela disponibilização dos dados não deve exceder o custo direto da disponibilização dos dados nem ser discriminatória.

(45) Os custos diretos da disponibilização dos dados são os custos necessários para a reprodução, a difusão por meios eletrónicos e o armazenamento de dados, mas não para a sua recolha ou geração. Os custos diretos da disponibilização dos dados devem limitar-se à parte imputável aos pedidos individuais, tendo em conta que as interfaces técnicas necessárias ou o *software* e a ligação conexos terão de ser estabelecidos de

forma permanente pelo detentor dos dados. Os acordos a longo prazo entre os detentores e os destinatários dos dados, por exemplo através de um modelo de subscrição, podem reduzir os custos associados à disponibilização dos dados em operações periódicas ou repetitivas numa relação comercial.

(46) Não é necessário intervir em caso de partilha de dados entre grandes empresas, ou quando o detentor dos dados for uma pequena ou média empresa e o destinatário for uma grande empresa. Nesses casos, considera-se que as empresas são capazes de negociar qualquer compensação, se for razoável, tendo em conta fatores como o volume, o formato, a natureza, a oferta e a procura dos dados, bem como os custos de recolha e disponibilização dos dados ao seu destinatário.

(47) A transparência é um princípio importante para garantir que a compensação solicitada pelo detentor dos dados é razoável ou, caso o destinatário dos dados seja uma micro, pequena ou média empresa, que a compensação não exceda os custos diretamente relacionados com a disponibilização dos dados ao seu destinatário e seja imputável ao pedido individual. A fim de colocar o destinatário dos dados em condições de avaliar e verificar se a compensação cumpre os requisitos do presente regulamento, o detentor dos dados deve facultar ao destinatário as informações necessárias com um grau de pormenor suficiente para o cálculo da compensação.

(48) Assegurar o acesso a formas alternativas de resolução de litígios nacionais e transfronteiriços relacionados com a disponibilização de dados deve beneficiar os detentores e os destinatários dos dados e, por conseguinte, reforçar a confiança na partilha de dados. Caso as partes não cheguem a acordo quanto a condições justas, razoáveis e não discriminatórias para a disponibilização de dados, os organismos de resolução de litígios devem proporcionar às partes uma solução simples, rápida e de baixo custo.

(49) A fim de evitar que dois ou mais organismos de resolução de litígios sejam chamados a pronunciar-se sobre o mesmo litígio, em especial num contexto transfronteiriço, um organismo de resolução de litígios deve poder rejeitar um pedido de resolução de um litígio que já tenha sido submetido a outro organismo de resolução de litígios ou a um órgão jurisdicional de um Estado-Membro.

(50) As partes em processos de resolução de litígios não devem ser impedidas de exercer os seus direitos fundamentais à ação e a um tribunal imparcial. Por conseguinte, a decisão de submeter um litígio a um organismo de resolução de litígios não deve privar essas partes do seu direito de obter reparação perante um órgão jurisdicional de um Estado-Membro.

(51) Quando uma parte se encontra numa posição negocial mais forte, existe o risco de essa parte poder tirar partido dessa posição em detrimento da outra parte contratante ao negociar o acesso aos dados, tornar o acesso aos dados menos viável do ponto de vista comercial e, por vezes, economicamente proibitivo. Esses desequilíbrios contratuais prejudicam particularmente as micro, pequenas e médias empresas que não dispõem de uma capacidade significativa para negociar as condições de acesso aos dados e que podem não ter outra alternativa senão aceitar cláusulas contratuais do tipo «pegar ou largar». Por conseguinte, as cláusulas contratuais abusivas que regulam o acesso e a utilização de dados ou a responsabilidade e as vias de recurso pela violação ou cessação de obrigações relacionadas com dados não devem ser vinculativas para as micro, pequenas ou médias empresas quando lhes tenham sido impostas unilateralmente.

(52) As regras relativas às cláusulas contratuais devem ter em conta o princípio da liberdade contratual enquanto conceito essencial nas relações entre empresas. Por conseguinte, nem todas as cláusulas contratuais devem ser sujeitas a um teste do caráter abusivo, mas apenas às cláusulas impostas unilateralmente às micro, pequenas e médias empresas. Trata-se de situações do tipo «pegar ou largar», em que uma parte fornece uma determinada cláusula contratual e a micro, pequena ou média empresa não pode influenciar o teor dessa cláusula, apesar de tentar negociá-la. Uma cláusula contratual simplesmente fornecida por uma das partes e aceite pela micro, pequena ou média empresa ou uma cláusula negociada e subsequentemente acordada de forma alterada entre as partes contratantes não deve considerar-se como imposta unilateralmente.

(53) Além disso, as regras relativas às cláusulas contratuais abusivas só devem ser aplicáveis aos elementos de um contrato relacionados com a disponibilização de dados, ou seja, as cláusulas contratuais relativas ao acesso aos dados e à sua utilização, bem como à responsabilidade ou às vias de recurso em caso de violação e cessação de obrigações relacionadas com dados. As outras partes do mesmo contrato, que não estão relacionadas com a disponibilização dos dados, não devem ser sujeitas ao teste do caráter abusivo previsto no presente regulamento.

(54) Os critérios de identificação das cláusulas contratuais abusivas só devem ser aplicados a cláusulas contratuais excessivas, em caso de abuso de uma posição negocial mais forte. A grande maioria das cláusulas contratuais que são comercialmente mais favoráveis para uma parte do que para a outra, incluindo as que são normais nos contratos entre empresas, constituem uma expressão normal do princípio da liberdade contratual e continuam a ser aplicáveis.

(55) Se uma cláusula contratual não constar da lista de cláusulas que são sempre consideradas abusivas ou que se presume serem abusivas, aplica-se a disposição geral relativa ao caráter abusivo. A este respeito, as cláusulas enumeradas como cláusulas abusivas devem servir de termo de comparação para a interpretação da disposição geral relativa ao caráter abusivo. Por último, os modelos de cláusulas contratuais para os contratos de partilha de dados entre empresas a elaborar e recomendar pela Comissão podem também ser úteis para a negociação de contratos pelas partes comerciais.

(56) Em situações de necessidade excecional, pode ser necessário que os organismos do setor público ou as instituições, agências ou organismos da União utilizem dados na posse de uma empresa para dar resposta a emergências públicas ou noutros casos excecionais. Os organismos que realizam investigação e os organismos financiadores de investigação também poderão estar organizados como organismos do setor público ou organismos de direito público. A fim de limitar os encargos para as empresas, as micro e pequenas empresas devem estar isentas da obrigação de fornecer dados aos organismos do setor público e às instituições, agências ou organismos da União em situações de necessidade excecional.

(57) No caso de emergências públicas, como emergências de saúde pública, emergências resultantes da degradação ambiental e catástrofes naturais de grandes proporções, incluindo as agravadas pelas alterações climáticas, bem como catástrofes de grandes proporções de origem humana, como incidentes graves de cibersegurança, o interesse público resultante da utilização dos dados prevalecerá sobre o interesse de os detentores dos dados disporem livremente dos dados que detêm. Nesse caso, os detentores dos dados devem ser obrigados a disponibilizá-los aos organismos do setor

público ou às instituições, agências ou organismos da União, a pedido destes. A existência de uma emergência pública é determinada de acordo com os respetivos procedimentos dos Estados-Membros ou das organizações internacionais pertinentes.

(58) É possível que seja igualmente suscitada uma necessidade excecional quando um organismo do setor público puder demonstrar que os dados são necessários para prevenir uma emergência pública, ou para ajudar a recuperar de uma emergência pública, em circunstâncias razoavelmente próximas da emergência pública em questão. Caso a necessidade excecional não seja justificada pela necessidade de responder, prevenir ou apoiar a recuperação de uma emergência pública, o organismo do setor público ou a instituição, agência ou organismo da União deve demonstrar que a falta de acesso aos dados solicitados em tempo útil, bem como a não utilização dos mesmos, o impede de desempenhar eficazmente uma função específica de interesse público expressamente prevista na lei. Essa necessidade excecional pode também ocorrer noutras situações, por exemplo, em relação à compilação de estatísticas oficiais em tempo útil, quando os dados não estiverem disponíveis de outra forma ou quando os encargos para os inquiridos forem consideravelmente reduzidos. Ao mesmo tempo, o organismo do setor público ou a instituição, agência ou organismo da União deve, noutros casos que não os de resposta, prevenção ou apoio à recuperação de uma emergência pública, demonstrar que não existem meios alternativos para obter os dados solicitados e que os dados não podem ser obtidos em tempo útil através do estabelecimento das obrigações de fornecimento de dados necessárias na nova legislação.

(59) O presente regulamento não deve ser aplicável a acordos voluntários de intercâmbio de dados entre entidades privadas e públicas, nem prejudicar esses acordos. O presente regulamento não deve afetar as obrigações impostas aos detentores dos dados no sentido de os fornecerem por motivos de necessidades de natureza não excecional, nomeadamente nos casos em que a gama dos dados e dos seus detentores é conhecida e em que a utilização dos dados pode ser efetuada com periodicidade, como no caso das obrigações de comunicação de informações e das obrigações relativas ao mercado interno. O presente regulamento também não deve afetar os requisitos de acesso aos dados para a verificação do cumprimento das regras aplicáveis, incluindo nos casos em que os organismos do setor público atribuem a função de verificação da conformidade a entidades que não são organismos do setor público.

(60) No exercício das suas funções nos domínios da prevenção, investigação, deteção ou repressão de infrações penais e administrativas, da execução de sanções penais e administrativas, bem como da recolha de dados para fins fiscais ou aduaneiros, os organismos do setor público e as instituições, agências e organismos da União devem recorrer às competências que lhes são conferidas pela legislação setorial. Por conseguinte, o presente regulamento não afeta os instrumentos de partilha, acesso e utilização de dados nesses domínios.

(61) Importa estabelecer um quadro proporcional, limitado e previsível a nível da União para a disponibilização de dados pelos seus detentores, em casos de necessidades excecionais, aos organismos do setor público e às instituições, agências ou organismos da União, a fim de garantir a segurança jurídica e de minimizar os encargos administrativos que recaem sobre as empresas. Para o efeito, os pedidos de dados apresentados pelos organismos do setor público e pelas instituições, agências e organismos da União aos detentores dos dados devem ser transparentes e proporcionais em termos do seu âmbito e da sua granularidade. A finalidade do pedido e a utilização prevista dos dados solicitados devem ser específicas e claramente

explicadas, permitindo simultaneamente a flexibilidade adequada para que a entidade requerente desempenhe as suas funções de interesse público. O pedido deve igualmente respeitar os interesses legítimos das empresas às quais é apresentado. Os encargos para os detentores dos dados devem ser minimizados, obrigando-se as entidades requerentes a respeitar o princípio da declaração única, que impede que os mesmos dados sejam solicitados várias vezes por mais do que um organismo do setor público ou por uma instituição, agência ou organismo da União, caso esses dados sejam necessários para dar resposta a uma emergência pública. A fim de assegurar a transparência, os pedidos de dados apresentados por organismos do setor público e pelas instituições, agências ou organismos da União devem ser tornados públicos sem demora injustificada pela entidade que solicita os dados, devendo ser assegurada a disponibilização pública em linha de todos os pedidos justificados por uma emergência pública.

(62) O objetivo da obrigação de fornecer os dados consiste em assegurar que os organismos do setor público e as instituições, agências ou organismos da União dispõem dos conhecimentos necessários para responder, prevenir ou recuperar de emergências públicas ou para manter a capacidade de desempenhar funções específicas expressamente previstas por lei. Os dados obtidos por essas entidades podem ser comercialmente sensíveis. Por conseguinte, a Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho[65] não deve ser aplicável aos dados disponibilizados nos termos do presente regulamento nem estes devem ser considerados como dados abertos disponíveis para reutilização por terceiros. Todavia, isso não deve afetar a aplicabilidade da Diretiva (UE) 2019/1024 à reutilização de estatísticas oficiais para cuja elaboração tenham sido utilizados dados obtidos nos termos do presente regulamento, desde que a reutilização não inclua os dados subjacentes. Além disso, não deve afetar a possibilidade de partilhar dados para a realização de investigação ou para a compilação de estatísticas oficiais, desde que sejam observadas as condições estabelecidas no presente regulamento. Os organismos do setor público devem também ser autorizados a proceder ao intercâmbio de dados obtidos ao abrigo do presente regulamento com outros organismos do setor público, a fim de dar resposta às necessidades excecionais para as quais os dados tenham sido solicitados.

(63) Os detentores dos dados devem ter a possibilidade de solicitar uma alteração do pedido apresentado por um organismo do setor público ou por uma instituição, agência ou organismo da União, ou o seu cancelamento, num período de 5 ou 15 dias úteis, em função da natureza da necessidade excecional invocada no pedido. No caso de pedidos por motivos de emergência pública, devem existir motivos justificados para a não-disponibilização dos dados, se for possível demonstrar que o pedido é semelhante ou idêntico a um pedido apresentado anteriormente para o mesmo efeito por outro organismo do setor público ou por outra instituição, agência ou organismo da União. Um detentor de dados que rejeite o pedido ou solicite a sua alteração deve comunicar a justificação subjacente à recusa do pedido ao organismo do setor público ou à instituição, agência ou organismo da União que solicita os dados. Caso os direitos *sui generis* das bases de dados ao abrigo da Diretiva 96/6/CE do Parlamento Europeu e do Conselho[66] sejam aplicáveis aos conjuntos de dados solicitados, os detentores dos dados devem exercer os seus direitos de forma a não impedir o organismo do setor

---

65 Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público (JO L 172 de 26.6.2019, p. 56).

66 Diretiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de março de 1996, relativa à proteção jurídica das bases de dados (JO L 77 de 27.3.1996, p. 20).

público e as instituições, agências ou organismos da União de obter os dados ou de os partilhar, em conformidade com o presente regulamento.

(64) Caso seja estritamente necessário incluir dados pessoais nos dados disponibilizados a um organismo do setor público ou a uma instituição, agência ou organismo da União, devem ser respeitadas as regras aplicáveis em matéria de proteção de dados pessoais, devendo a disponibilização dos dados e a sua subsequente utilização ser acompanhadas de garantias relativas aos direitos e interesses das pessoas a quem esses dados dizem respeito. O organismo que solicita os dados deve demonstrar a estrita necessidade e as finalidades específicas e limitadas do tratamento. Antes de disponibilizar os dados, o detentor dos dados deve envidar esforços razoáveis para os anonimizar ou, caso essa anonimização se revele impossível, aplicar meios tecnológicos como a pseudonimização e a agregação.

(65) Os dados disponibilizados aos organismos do setor público e às instituições, agências ou organismos da União com base em necessidades excecionais só devem ser utilizados para as finalidades para as quais foram solicitados, salvo se o detentor dos dados que os disponibilizou tenha concordado expressamente que sejam utilizados para outras finalidades. Os dados devem ser destruídos quando deixarem de ser necessários para a finalidade indicada no pedido, salvo acordo em contrário, devendo o detentor dos dados ser informado desse facto.

(66) Ao reutilizar dados fornecidos pelos seus detentores, os organismos do setor público e as instituições, agências ou organismos da União devem respeitar a legislação aplicável em vigor e as obrigações contratuais às quais o detentor dos dados está sujeito. Caso a divulgação de segredos comerciais do detentor dos dados a organismos do setor público ou a instituições, agências ou organismos da União seja estritamente necessária para satisfazer a finalidade para a qual se solicitaram os dados, deve assegurar-se ao detentor dos dados a confidencialidade dessa divulgação.

(67) Quando está em causa a salvaguarda de um bem público significativo, como é o caso da resposta a emergências públicas, não se deve esperar que o organismo do setor público ou a instituição, agência ou organismo da União compense as empresas pelos dados obtidos. As emergências públicas são acontecimentos raros e nem todas essas emergências exigem a utilização de dados na posse das empresas. Por conseguinte, não é provável que as atividades comerciais dos detentores dos dados sejam afetadas negativamente em consequência do recurso ao presente regulamento pelos organismos do setor público ou pelas instituições, agências ou organismos da União. Todavia, uma vez que os casos de necessidade excecional que não sejam a resposta a uma emergência pública podem ser mais frequentes, incluindo situações de prevenção ou recuperação de uma emergência pública, os detentores dos dados devem, nesses casos, ter direito a uma compensação razoável, que não deve exceder os custos técnicos e organizativos incorridos para satisfazer o pedido e a margem razoável necessária para disponibilizar os dados ao organismo do setor público ou à instituição, agência ou organismo da União. A compensação não deve ser entendida como um pagamento pelos próprios dados nem como sendo obrigatória.

(68) O organismo do setor público ou a instituição, agência ou organismo da União pode partilhar os dados que obteve na sequência do pedido com outras entidades ou pessoas, sempre que tal seja necessário para realizar atividades analíticas ou de investigação científica que não possa realizar por si próprio. Esses dados podem também ser partilhados nas mesmas circunstâncias com os institutos nacionais de estatística e o Eurostat para a compilação de estatísticas oficiais. Essas atividades de investigação

devem, no entanto, ser compatíveis com a finalidade para a qual os dados foram solicitados e o detentor dos dados deve ser informado sobre a partilha posterior dos dados que forneceu. As pessoas singulares que realizam atividades de investigação ou as organizações de investigação com as quais estes dados sejam partilhados não devem prosseguir fins lucrativos ou devem agir no contexto de uma missão de interesse público reconhecida pelo Estado. Para efeitos do presente regulamento, não devem ser consideradas organizações de investigação as organizações sobre as quais as empresas comerciais tenham uma influência decisiva que lhes possibilite exercer controlo devido a situações estruturais, que podem resultar num acesso preferencial aos resultados da investigação.

(69) A capacidade de os clientes de serviços de tratamento de dados, incluindo serviços de computação em nuvem e periféricos, mudarem de um serviço de tratamento de dados para outro, mantendo simultaneamente uma funcionalidade mínima do serviço, é uma condição fundamental para um mercado mais competitivo, com menos obstáculos à entrada de novos prestadores de serviços.

(70) O Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho incentiva os prestadores de serviços a desenvolverem e aplicarem de forma eficaz códigos de conduta de autorregulação que abranjam as melhores práticas para, entre outros, facilitar a mudança de prestador de serviços de tratamento de dados e a portabilidade dos dados. Dada a eficácia limitada dos quadros de autorregulação desenvolvidos em resposta a essas disposições e a indisponibilidade geral de normas e interfaces abertas, importa adotar um conjunto de obrigações regulamentares mínimas para os prestadores de serviços de tratamento de dados, a fim de eliminar os obstáculos contratuais, económicos e técnicos a uma mudança eficaz entre serviços de tratamento de dados.

(71) Os serviços de tratamento de dados devem abranger serviços que possibilitem um amplo acesso remoto e a pedido de um conjunto adaptável e modulável de recursos de computação partilháveis e distribuídos. Esses recursos de computação incluem redes, servidores ou outras infraestruturas virtuais ou físicas, sistemas operativos, *software*, incluindo ferramentas de desenvolvimento de *software*, armazenamento, aplicações e serviços. A possibilidade de o cliente do serviço de tratamento de dados em nuvem gerir autónoma e unilateralmente as capacidades de computação, por exemplo o tempo de acesso ao servidor ou o armazenamento em rede, sem qualquer interação humana do prestador do serviço, pode descrever-se como administração a pedido. O termo «amplo acesso remoto» utiliza-se para descrever o facto de as capacidades de computação serem disponibilizadas por meio da rede e acedidas mediante mecanismos que promovem a utilização de diferentes plataformas para clientes «magros» (*thin client*) ou «gordos» (*thick*/*fat client*) (desde navegadores Web a dispositivos móveis e estações de trabalho). O termo «modulável» refere-se a recursos de computação atribuídos de forma flexível pelo prestador de serviços de tratamento de dados, independentemente da localização geográfica dos recursos, a fim de fazer face às flutuações da procura. O termo «conjunto adaptável» utiliza-se para descrever os recursos de computação disponibilizados e libertados em função da procura, a fim de aumentar ou diminuir rapidamente os recursos disponíveis, consoante o volume de trabalho. O termo «partilhável» utiliza-se para descrever os recursos de computação fornecidos a múltiplos utilizadores que partilham um acesso comum ao serviço, mas cujo processamento é efetuado separadamente para cada utilizador, embora o serviço seja prestado a partir do mesmo equipamento eletrónico. O termo «distribuído» utiliza-se para descrever os recursos de computação localizados em diferentes computadores

ou dispositivos ligados em rede, que comunicam e se coordenam entre si por via da transmissão de mensagens. O termo «altamente distribuído» utiliza-se para descrever os serviços de tratamento de dados que envolvem o tratamento de dados mais próximo do local onde os dados são gerados ou recolhidos, por exemplo, num dispositivo conectado de tratamento de dados. Prevê-se que a computação periférica, uma forma de tratamento altamente distribuído de dados, gere novos modelos empresariais e de prestação de serviços em nuvem, que devem ser abertos e interoperáveis desde o início.

(72) O presente regulamento visa facilitar a mudança entre serviços de tratamento de dados, que abrange todas as condições e ações necessárias para que um cliente rescinda um acordo contratual de um serviço de tratamento de dados, celebre um ou vários novos contratos com diferentes prestadores de serviços de tratamento de dados, transfira todos os seus ativos digitais, incluindo dados, para os outros prestadores em causa e continue a utilizá-los no novo ambiente, beneficiando simultaneamente de equivalência funcional. Os ativos digitais referem-se a elementos em formato digital para os quais o cliente tem o direito de utilização, incluindo dados, aplicações, máquinas virtuais e outras manifestações de tecnologias de virtualização, como *containers*. Por equivalência funcional entende-se a manutenção de um nível mínimo de funcionalidade de um serviço após a mudança entre prestadores, devendo ser considerada tecnicamente viável sempre que os serviços de tratamento de dados de origem e de destino abranjam (parcial ou totalmente) o mesmo tipo de serviço. Os metadados gerados pela utilização de um serviço pelo cliente devem também ser portáteis nos termos das disposições do presente regulamento em matéria de mudança entre prestadores.

(73) Caso os prestadores de serviços de tratamento de dados sejam, por sua vez, clientes de serviços de tratamento de dados prestados por um terceiro, beneficiarão de uma mudança mais eficaz, estando simultânea e invariavelmente vinculados às obrigações do presente regulamento no que se refere às suas próprias ofertas de serviços.

(74) Os prestadores de serviços de tratamento de dados devem ser obrigados a disponibilizar toda a assistência e o apoio necessários para que o processo de mudança seja bem-sucedido e eficaz, sem exigir que esses prestadores de serviços de tratamento de dados desenvolvam novas categorias de serviços na infraestrutura informática, ou com base na mesma, de diferentes prestadores de serviços de tratamento de dados, a fim de garantir a equivalência funcional num ambiente diferente dos seus próprios sistemas. Todavia, os prestadores de serviços são obrigados a prestar toda a assistência e o apoio necessários para tornar o processo de mudança eficaz. Os direitos vigentes relativos à rescisão de contratos, incluindo os introduzidos pelo Regulamento (UE) 2016/679 e pela Diretiva (UE) 2019/770 do Parlamento Europeu e do Conselho[67], não devem ser afetados.

(75) A fim de facilitar a mudança entre serviços de tratamento de dados, os prestadores desses serviços devem ponderar a utilização de ferramentas de execução e/ou de conformidade, nomeadamente as publicadas pela Comissão sob a forma de um conjunto de regras relativas aos serviços de computação em nuvem. Em especial, as cláusulas contratuais-tipo são benéficas para aumentar a confiança nos serviços de tratamento de dados, para criar uma relação mais equilibrada entre os utilizadores e os

[67] Diretiva (UE) 2019/770 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais (JO L 136 de 22.5.2019, p. 1).

prestadores de serviços, bem como para melhorar a segurança jurídica quanto às condições aplicáveis à mudança para outros serviços de tratamento de dados. Neste contexto, os utilizadores e os prestadores de serviços devem ponderar a utilização de cláusulas contratuais-tipo elaboradas por organismos ou grupos de peritos pertinentes criados ao abrigo do direito da União.

(76) As especificações e normas de interoperabilidade aberta elaboradas em conformidade com os pontos 3 e 4 do anexo II do Regulamento (UE) n.º 1025/2021 no domínio da interoperabilidade e da portabilidade permitem um ambiente de computação em nuvem sem descontinuidades entre vários prestadores, um requisito fundamental para a inovação aberta na economia europeia dos dados. Uma vez que os processos impulsionados pelo mercado não mostraram a capacidade de estabelecer especificações ou normas técnicas que facilitem uma interoperabilidade eficaz da computação em nuvem aos níveis da plataforma como serviço (PaaS – *Platform-as-a-Service*) e do *software* como serviço (SaaS – *Software-as-a-Service*), com base no presente regulamento e em conformidade com o Regulamento (UE) n.º 1025/2012, a Comissão deve ter a possibilidade de solicitar aos organismos europeus de normalização que elaborem essas normas, em especial para os tipos de serviços em que ainda não existam. Além disso, a Comissão incentivará as partes no mercado a elaborarem especificações pertinentes de interoperabilidade aberta. A Comissão, por meio de atos delegados, pode impor a utilização de normas europeias para a interoperabilidade ou de especificações de interoperabilidade aberta para tipos de serviços específicos, através de uma referência num repositório central de normas da União para a interoperabilidade dos serviços de tratamento de dados. As normas europeias e as especificações de interoperabilidade aberta só serão referenciadas se cumprirem os critérios especificados no presente regulamento, que têm o mesmo significado que os requisitos estabelecidos nos pontos 3 e 4 do anexo II do Regulamento (UE) n.º 1025/2021 e as facetas de interoperabilidade definidas nos termos da norma ISO/CEI 19941:2017.

(77) Os países terceiros podem aprovar leis, regulamentos e outros atos normativos que visem a transferência direta ou a concessão de acesso governamental a dados não pessoais localizados para além das fronteiras desses países, incluindo na União. As decisões de órgãos jurisdicionais ou de outras autoridades judiciais ou administrativas, incluindo as autoridades policiais de países terceiros, que exijam tal transferência ou acesso a dados não pessoais devem ser executórias com base num acordo internacional, como um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União ou um dos Estados-Membros. Noutros casos, podem surgir situações em que um pedido de transferência ou de concessão de acesso a dados não pessoais decorrente da legislação de um país terceiro colide com a obrigação de proteção desses dados por força do direito da União ou nacional, em especial no que diz respeito à proteção dos direitos fundamentais das pessoas singulares, como o direito à segurança e o direito a um recurso efetivo, ou aos interesses fundamentais de um Estado-Membro relacionados com a segurança nacional ou a defesa, bem como à proteção de dados comercialmente sensíveis, incluindo a proteção de segredos comerciais, e à proteção dos direitos de propriedade intelectual, incluindo os compromissos contratuais em matéria de confidencialidade nos termos dessa legislação. Na ausência de acordos internacionais que regulem essas matérias, a transferência ou o acesso só deve permitir-se caso se tenha verificado que a ordem jurídica do país terceiro exige que a decisão seja fundamentada, proporcional e com um caráter específico, que as objeções fundamentadas do destinatário estejam sujeitas a controlo jurisdicional no país terceiro por um tribunal competente habilitado a ter em

devida conta os interesses jurídicos relevantes do fornecedor desses dados. Sempre que possível, nos termos do pedido de acesso aos dados da autoridade do país terceiro, o prestador de serviços de tratamento de dados deve poder informar o cliente a quem se solicitam os dados, a fim de verificar a existência de um potencial conflito desse acesso com as regras da União ou nacionais, como as relativas à proteção de dados comercialmente sensíveis, incluindo a proteção dos segredos comerciais e dos direitos de propriedade intelectual, bem como os compromissos contratuais em matéria de confidencialidade.

(78) A fim de promover uma maior confiança nos dados, é importante que as garantias em relação aos cidadãos, ao setor público e às empresas da União sejam aplicadas na medida do possível, de modo a assegurar o controlo dos seus dados. Além disso, importa respeitar a legislação, os valores e as normas da União em matéria de segurança, proteção de dados e privacidade e proteção dos consumidores, entre outras. A fim de impedir o acesso ilícito a dados não pessoais, os prestadores de serviços de tratamento de dados abrangidos pelo presente instrumento, como os serviços de computação em nuvem e periféricos, devem tomar todas as medidas razoáveis para impedir o acesso aos sistemas em que se armazenam os dados não pessoais, incluindo, se for caso disso, através da cifragem dos dados, da sujeição frequente a auditorias, da adesão verificada a sistemas pertinentes de certificação da fiabilidade da segurança e da alteração das políticas empresariais.

(79) A normalização e a interoperabilidade semântica devem desempenhar um papel fundamental na disponibilização de soluções técnicas que garantam a interoperabilidade. A fim de facilitar a conformidade com os requisitos de interoperabilidade, há que conferir uma presunção de conformidade às soluções de interoperabilidade que cumprem as normas harmonizadas ou partes das mesmas, nos termos do Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho. A Comissão deve adotar especificações comuns em domínios nos quais não existam normas harmonizadas ou em que sejam insuficientes, a fim de reforçar a interoperabilidade dos espaços comuns europeus de dados, das interfaces de programação de aplicações, da computação em nuvem e dos contratos inteligentes. Além disso, podem continuar a ser adotadas especificações comuns nos diferentes setores, em conformidade com o direito setorial da União ou nacional, com base nas necessidades específicas desses setores. Os modelos (sob a forma de vocabulários de base), as ontologias, o perfil de aplicação de metadados, os dados de referência sob a forma de vocabulário de base, taxonomias, listas de códigos, quadros de autoridades, tesauros e as estruturas de dados reutilizáveis devem também fazer parte das especificações técnicas para a interoperabilidade semântica. Além disso, a Comissão deve ter a possibilidade de mandatar o desenvolvimento de normas harmonizadas para a interoperabilidade dos serviços de tratamento de dados.

(80) A fim de promover a interoperabilidade dos contratos inteligentes nas aplicações de partilha de dados, há que estabelecer requisitos essenciais para os contratos inteligentes destinados aos profissionais que criem contratos inteligentes para outros ou que integrem esses contratos inteligentes em aplicações que apoiem a execução de acordos de partilha de dados. A fim de facilitar a conformidade desses contratos inteligentes com os referidos requisitos essenciais, há que conferir uma presunção de conformidade aos contratos inteligentes que cumprem as normas harmonizadas ou partes das mesmas, nos termos do Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho.

(81) A fim de assegurar a execução efetiva do presente regulamento, os Estados-Membros devem designar uma ou várias autoridades competentes. Se um Estado-Membro designar mais do que uma autoridade competente, deve designar igualmente uma autoridade competente coordenadora. As autoridades competentes devem colaborar entre si. As autoridades responsáveis pelo controlo do cumprimento da proteção de dados e as autoridades competentes designadas ao abrigo da legislação setorial devem ser responsáveis pela execução do presente regulamento nos seus domínios de competência.

(82) A fim de fazer valer os seus direitos nos termos do presente regulamento, as pessoas singulares e coletivas devem ter o direito de obter reparação pelas violações dos seus direitos ao abrigo do presente regulamento, mediante a apresentação de reclamação às autoridades competentes. Essas autoridades devem ser obrigadas a cooperar para assegurar que a reclamação é tratada e resolvida de forma adequada. A fim de utilizar o mecanismo da rede de cooperação de defesa do consumidor e possibilitar ações coletivas, o presente regulamento altera os anexos do Regulamento (UE) 2017/2394 do Parlamento Europeu e do Conselho[68] e da Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho[69].

(83) As autoridades competentes dos Estados-Membros devem garantir o sancionamento das violações das obrigações estabelecidas no presente regulamento. Ao fazê-lo, devem considerar a natureza, a gravidade, a recorrência e a duração da violação, tendo em conta o interesse público em causa, o âmbito e o tipo de atividades exercidas, bem como a capacidade económica do infrator. Devem ter em conta se o infrator não cumpre, de forma sistemática ou recorrente, as obrigações que lhe incumbem por força do presente regulamento. A fim de ajudar as empresas a elaborar e negociar contratos, a Comissão deve desenvolver e recomendar modelos facultativos de cláusulas contratuais para os contratos de partilha de dados entre empresas, tendo em conta, se necessário, as condições em setores específicos e as práticas existentes com mecanismos voluntários de partilha de dados. Esses modelos de cláusulas contratuais devem constituir, antes de mais, um instrumento prático para ajudar, em especial, as empresas de menor dimensão a celebrar um contrato. Caso sejam utilizados de forma ampla e integral, esses modelos de cláusulas contratuais deverão também ter o efeito benéfico de influenciar a conceção dos contratos sobre o acesso e a utilização de dados e, por conseguinte, de um modo mais geral, conduzir a relações contratuais mais justas no acesso e na partilha de dados.

(84) A fim de eliminar o risco de os detentores dos dados incluídos em bases de dados, que foram obtidos ou gerados por meio de componentes físicos, por exemplo sensores, de um produto conectado e de um serviço conexo, reivindicarem o direito *sui generis* nos termos do artigo 7.º da Diretiva 96/9/CE, caso essas bases de dados não sejam elegíveis para o direito *sui generis*, prejudicando assim o exercício efetivo do direito dos utilizadores de acederem e utilizarem dados e o direito de partilharem dados com terceiros ao abrigo do presente regulamento, o presente regulamento deve clarificar

---

68 Regulamento (UE) 2017/2394 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2017, relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de proteção dos consumidores e que revoga o Regulamento (CE) n.º 2006/2004 (JO L 345 de 27.12.2017, p. 1).

69 Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho, de 25 de novembro de 2020, relativa a ações coletivas para proteção dos interesses coletivos dos consumidores e que revoga a Diretiva 2009/22/CE (JO L 409 de 4.12.2020, p. 1).

que o direito *sui generis* não é aplicável a essas bases de dados, pois os requisitos de proteção não seriam cumpridos.

(85) A fim de ter em conta os aspetos técnicos dos serviços de tratamento de dados, o poder de adotar atos nos termos do artigo 290.º do TFUE deve ser delegado na Comissão para complementar o presente regulamento, a fim de introduzir um mecanismo de controlo dos encargos de mudança impostos pelos prestadores de serviços de tratamento de dados no mercado, especificar mais pormenorizadamente os requisitos essenciais para os operadores de espaços de dados e prestadores de serviços de tratamento de dados em matéria de interoperabilidade e publicar a referência das especificações de interoperabilidade aberta e das normas europeias para a interoperabilidade dos serviços de tratamento de dados. Importa espacialmente que a Comissão proceda às consultas necessárias durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam realizadas de acordo com os princípios estabelecidos no Acordo Interinstitucional sobre Legislar Melhor, de 13 de abril de 2016[70]. Em particular, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da elaboração dos atos delegados.

(86) A fim de assegurar condições uniformes para a execução do presente regulamento, há que atribuir competências de execução à Comissão para complementar o presente regulamento, mediante a adoção de especificações comuns destinadas a assegurar a interoperabilidade dos espaços comuns europeus de dados e a partilha de dados, a mudança entre serviços de tratamento de dados, a interoperabilidade de contratos inteligentes, bem como para meios técnicos, como interfaces de programação de aplicações, com o objetivo de permitir a transmissão de dados entre as partes, incluindo de forma contínua ou em tempo real, e para vocabulários essenciais de interoperabilidade semântica, bem como para adotar especificações comuns para contratos inteligentes. Essas competências devem ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho[71].

(87) O presente regulamento não deve afetar disposições específicas dos atos da União adotados no domínio da partilha de dados entre empresas, entre empresas e consumidores e entre empresas e organismos do setor público que tenham sido adotados antes da data de adoção do presente regulamento. A fim de assegurar a coerência e o bom funcionamento do mercado interno, a Comissão deve, se for caso disso, avaliar a situação no que respeita à relação entre o presente regulamento e os atos adotados antes da sua data de adoção que regulamentam a partilha de dados, de modo a avaliar a necessidade de alinhar essas disposições específicas com o presente regulamento. O presente regulamento não deve prejudicar as regras relativas a necessidades específicas de setores ou domínios de interesse público individuais. Essas regras podem incluir requisitos adicionais sobre os aspetos técnicos do acesso aos dados, como interfaces de acesso aos dados, ou a forma como o acesso aos dados pode ser facultado, por exemplo, diretamente a partir do produto ou através de serviços de intermediação de dados. Essas regras podem também incluir limites aos direitos dos detentores dos dados no que se refere ao acesso ou à utilização dos dados dos

---

70 JO L 123 de 12.5.2016, p. 1.

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

utilizadores, ou outros aspetos para além do acesso e da utilização dos dados, por exemplo em matéria de governação. O presente regulamento também não deve prejudicar regras mais específicas no contexto do desenvolvimento de espaços comuns europeus de dados.

(88) O presente regulamento não afeta a aplicação das regras em matéria de concorrência, em particular dos artigos 101.° e 102.° do Tratado. As medidas previstas no presente regulamento não devem ser utilizadas para restringir indevidamente a concorrência de forma contrária ao Tratado.

(89) A fim de permitir que os agentes económicos se adaptem às novas regras estabelecidas no presente regulamento, estas devem ser aplicáveis a partir de um ano após a entrada em vigor do regulamento.

(90) A Autoridade Europeia para a Proteção de Dados e o Comité Europeu para a Proteção de Dados foram consultados nos termos do artigo 42.º do Regulamento (UE) 2018/1725 e emitiram um parecer conjunto em [XX.XX.2022],

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Artigo 1.º
Objeto e âmbito de aplicação

1. O presente regulamento estabelece regras harmonizadas sobre a disponibilização de dados gerados pela utilização de um produto ou serviço conexo ao utilizador desse produto ou serviço, sobre a disponibilização de dados pelos detentores dos dados aos seus destinatários e sobre a disponibilização dos dados pelos detentores a organismos do setor público ou a instituições, agências ou organismos da União, em caso de necessidade excecional, para o desempenho de uma missão de interesse público.

2. O presente regulamento é aplicável:

   a) Aos fabricantes de produtos e aos prestadores de serviços conexos colocados no mercado da União, bem como aos utilizadores desses produtos ou serviços;

   b) Aos detentores dos dados que os disponibilizam aos seus destinatários na União;

   c) Aos destinatários na União a quem os dados são disponibilizados;

   d) Aos organismos do setor público e às instituições, agências ou organismos da União que solicitam aos detentores dos dados que os disponibilizem, caso exista uma necessidade excecional desses dados para o desempenho de uma missão de interesse público, e aos detentores dos dados que os facultam em resposta a esse pedido;

   e) Aos prestadores de serviços de tratamento de dados que disponibilizam esses serviços a clientes na União.

3. O direito da União em matéria de proteção de dados pessoais, privacidade e confidencialidade das comunicações e integridade dos equipamentos terminais é aplicável aos dados pessoais tratados no âmbito dos direitos e obrigações

estabelecidos no presente regulamento. O presente regulamento não afeta a aplicabilidade do direito da União sobre a proteção dos dados pessoais, em especial o Regulamento (UE) 2016/679 e a Diretiva 2002/58/CE, incluindo os poderes e as competências das autoridades de controlo. No que diz respeito aos direitos estabelecidos no capítulo II do presente regulamento, e sempre que os utilizadores sejam titulares de dados pessoais sujeitos às obrigações e aos direitos previstos no referido capítulo, as disposições do presente regulamento complementam o direito de portabilidade dos dados previsto no artigo 20.º do Regulamento (UE) 2016/679.

4. O presente regulamento não afeta os atos jurídicos nacionais e da União que preveem a partilha, o acesso e a utilização de dados para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo o Regulamento (UE) 2021/784 do Parlamento Europeu e do Conselho[72] e as {propostas relativas às provas eletrónicas [COM(2018) 225 e 226]}, após a sua adoção, bem como a cooperação internacional nesse domínio. O presente regulamento não afeta a recolha, a partilha, o acesso e a utilização de dados nos termos da Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e do Regulamento (UE) 2015/847 do Parlamento Europeu e do Conselho relativo às informações que acompanham as transferências de fundos. O presente regulamento não afeta as competências dos Estados-Membros no que diz respeito às atividades relacionadas com a segurança pública, a defesa, a segurança nacional, a administração aduaneira e fiscal e a saúde e segurança dos cidadãos, em conformidade com o direito da União.

Artigo 2.º
Definições

Para efeitos do presente regulamento, entende-se por:

(1) «Dados», qualquer representação digital de atos, factos ou informações e qualquer compilação desses atos, factos ou informações, incluindo sob a forma de gravação sonora, visual ou audiovisual;

(2) «Produto», um bem tangível e móvel, incluindo quando incorporado num bem imóvel, que obtém, gera ou recolhe dados relativos à sua utilização ou ao seu ambiente e que é capaz de comunicar dados através de um serviço de comunicações eletrónicas publicamente disponível e cuja função principal não consiste no armazenamento e no tratamento de dados;

(3) «Serviço conexo», um serviço digital, incluindo *software*, incorporado num produto ou interligado com o mesmo de tal modo que a sua ausência impediria que o produto desempenhasse uma das suas funções;

(4) «Assistentes virtuais», *software* com capacidade para tratar de pedidos, funções ou perguntas, nomeadamente com base em sons, escritos, gestos ou movimentos, e que, com base nesses pedidos, funções ou perguntas, proporciona acesso aos seus próprios serviços e aos de terceiros ou controla os seus próprios dispositivos e os de terceiros;

(5) «Utilizador», uma pessoa singular ou coletiva que é proprietária, arrendatária ou locatária de um produto ou que recebe um serviço;

[72] Regulamento (UE) 2021/784 do Parlamento Europeu e do Conselho, de 29 de abril de 2021, relativo ao combate à difusão de conteúdos terroristas em linha (JO L 172 de 17.5.2021, p. 79).

(6) «Detentor dos dados», uma pessoa singular ou coletiva que tem o direito ou a obrigação, nos termos do presente regulamento, da legislação aplicável da União ou da legislação nacional que transpõe o direito da União, ou, no caso de dados não pessoais e através do controlo da conceção técnica do produto e dos serviços conexos, da capacidade de disponibilizar determinados dados;

(7) «Destinatário dos dados», uma pessoa singular ou coletiva que age para fins relacionados com a sua atividade comercial, empresarial, artesanal ou profissional, que não seja o utilizador de um produto ou serviço conexo, à qual o detentor dos dados disponibiliza os dados, incluindo um terceiro na sequência de um pedido do utilizador ao detentor dos dados ou em conformidade com uma obrigação legal ao abrigo do direito da União ou da legislação nacional que transpõe o direito da União;

(8) «Empresa», uma pessoa singular ou coletiva que, no que respeita às práticas e aos contratos abrangidos pelo presente regulamento, age para fins relacionados com a sua atividade comercial, empresarial, artesanal ou profissional;

(9) «Organismo do setor público», as autoridades nacionais, regionais ou locais dos Estados-Membros e os organismos de direito público dos Estados-Membros ou as associações formadas por uma ou várias dessas autoridades ou por um ou vários desses organismos;

(10) «Emergência pública», uma situação excecional que afeta negativamente a população da União, de um Estado-Membro ou de parte dele, com o risco de repercussões graves e duradouras nas condições de vida ou na estabilidade económica, ou de degradação significativa dos ativos económicos da União ou dos Estados-Membros em causa;

(11) «Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados ou conjuntos de dados em formato eletrónico, através de procedimentos automatizados ou não automatizados, como, por exemplo, a recolha, o registo, a organização, a estruturação, o armazenamento, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, a difusão ou qualquer outra forma de disponibilização, o alinhamento ou a combinação, a limitação, o apagamento ou a destruição;

(12) «Serviço de tratamento de dados», um serviço digital que não seja um serviço de conteúdos em linha na aceção do artigo 2.º, n.º 5, do Regulamento (UE) 2017/1128, prestado a um cliente, que permite a administração a pedido e um amplo acesso remoto a um conjunto modulável e adaptável de recursos de computação partilháveis de natureza centralizada, distribuída ou altamente distribuída;

(13) «Tipo de serviço», um conjunto de serviços de tratamento de dados que partilham o mesmo objetivo principal e o mesmo modelo de serviço de tratamento de dados de base;

(14) «Equivalência funcional», a manutenção de um nível mínimo de funcionalidade no ambiente de um novo serviço de tratamento de dados após o processo de mudança, de tal modo que, em resposta a uma ação de introdução realizada pelo utilizador em elementos essenciais do serviço, o serviço de destino produzirá o mesmo resultado com o mesmo desempenho e com o mesmo nível de segurança, resiliência operacional e qualidade do serviço que o serviço de origem no momento da rescisão do contrato;

(15) «Especificações de interoperabilidade aberta», as especificações técnicas no domínio das TIC, conforme definidas no Regulamento (UE) n.º 1025/2012, que são orientadas para a consecução da interoperabilidade entre serviços de tratamento de dados;

(16) «Contrato inteligente», um programa informático armazenado num sistema de livro-razão eletrónico em que o resultado da execução do programa é registado no livro-razão eletrónico;

(17) «Livro-razão eletrónico», um livro-razão eletrónico na aceção do artigo 3.º, ponto 53, do Regulamento (UE) n.º 910/2014;

(18) «Especificações comuns», um documento, que não uma norma, que contém soluções técnicas que proporcionam um meio para cumprir certos requisitos e obrigações estabelecidas no presente regulamento;

(19) «Interoperabilidade», a capacidade de dois ou mais espaços de dados ou redes de comunicações, sistemas, dispositivos, aplicações ou componentes, procederem ao intercâmbio de dados e utilizarem-nos, de modo a desempenharem as suas funções;

(20) «Norma harmonizada», uma norma harmonizada tal como definida no artigo 2.º, ponto 1, alínea c), do Regulamento (UE) n.º 1025/2012.

CAPÍTULO II
PARTILHA DE DADOS ENTRE EMPRESAS E CONSUMIDORES E ENTRE EMPRESAS

Artigo 3.º
Obrigação de tornar acessíveis os dados gerados pela utilização de produtos ou serviços conexos

1. Os produtos devem ser concebidos e fabricados e os serviços conexos prestados de modo a que os dados gerados pela sua utilização sejam, por defeito, fáceis, seguros e, se for caso disso, diretamente acessíveis ao utilizador.

2. Antes da celebração de um contrato de compra, aluguer ou locação de um produto ou serviço conexo, devem ser facultadas ao utilizador, num formato claro e compreensível, pelo menos as seguintes informações:

   a) A natureza e o volume dos dados suscetíveis de serem gerados pela utilização do produto ou serviço conexo;

   b) A probabilidade de os dados serem gerados continuamente e em tempo real;

   c) A forma como o utilizador pode aceder a esses dados;

   d) Se o fabricante que fornece o produto ou o prestador do serviço conexo tenciona utilizar ele próprio os dados ou permitir que terceiros os utilizem e, em caso afirmativo, as finalidades para as quais esses dados serão utilizados;

   e) Se o vendedor, o arrendatário ou o locador é o detentor dos dados e, em caso negativo, a identidade do detentor dos dados, como a sua designação social e o endereço geográfico em que está estabelecido;

   f) Os meios de comunicação que permitem ao utilizador contactar rapidamente o detentor dos dados e comunicar eficazmente com o mesmo;

   g) A forma como o utilizador pode solicitar que os dados sejam partilhados com um terceiro;

h) O direito do utilizador de apresentar uma reclamação, alegando uma violação das disposições do presente capítulo, à autoridade competente a que se refere o artigo 31.º.

Artigo 4.º
O direito dos utilizadores de acederem e utilizarem os dados gerados pela utilização de produtos ou serviços conexos

1. Caso o utilizador não possa aceder diretamente aos dados a partir do produto, o detentor dos dados deve disponibilizar ao utilizador os dados gerados pela sua utilização de um produto ou serviço conexo, sem demora injustificada, gratuitamente e, se for caso disso, de forma contínua e em tempo real, com base num simples pedido por via eletrónica, caso seja tecnicamente viável.

2. O detentor dos dados não pode exigir que o utilizador faculte quaisquer informações para além das necessárias para verificar a qualidade de utilizador nos termos do n.º 1. O detentor dos dados não pode conservar quaisquer informações sobre o acesso do utilizador aos dados solicitados para além das necessárias para a boa execução do pedido de acesso do utilizador e para a segurança e manutenção da infraestrutura de dados.

3. Os segredos comerciais só podem ser divulgados se forem tomadas todas as medidas específicas necessárias para preservar a confidencialidade dos segredos comerciais, em especial no que diz respeito a terceiros. O detentor dos dados e o utilizador podem acordar medidas para preservar a confidencialidade dos dados partilhados, em especial em relação a terceiros.

4. O utilizador não pode utilizar os dados obtidos na sequência de um pedido a que se refere o n.º 1 para desenvolver um produto que concorra com o produto do qual provêm os dados.

5. Caso o utilizador não seja titular dos dados, quaisquer dados pessoais gerados pela utilização de um produto ou serviço conexo só podem ser disponibilizados pelo titular dos dados ao utilizador se existir uma base jurídica válida nos termos do artigo 6.º, n.º 1, do Regulamento (UE) 2016/679 e, se for caso disso, estiverem preenchidas as condições do artigo 9.º do referido regulamento.

6. O detentor dos dados só pode utilizar quaisquer dados não pessoais gerados pela utilização de um produto ou serviço conexo com base num acordo contratual com o utilizador. O detentor dos dados não pode utilizar esses dados gerados pela utilização do produto ou serviço conexo para obter informações sobre a situação económica, os ativos e os métodos de produção do utilizador, ou a sua utilização, que possam prejudicar a posição comercial do utilizador nos mercados nos quais exerce a sua atividade.

Artigo 5.º
Direito de partilhar dados com terceiros

1. A pedido de um utilizador, ou de uma parte que atue por conta de um utilizador, o detentor dos dados deve disponibilizar a terceiros, sem demora injustificada e a título gratuito, os dados gerados pela utilização de um produto ou serviço conexo, com a mesma qualidade que está disponível para o detentor dos dados e, se for caso disso, de forma contínua e em tempo real.

2. Qualquer empresa que preste serviços essenciais de plataforma para os quais um ou vários desses serviços foram designados como controladores de acesso, nos termos do artigo [...] do [Regulamento XXX relativo à disputabilidade e equidade dos mercados no setor digital (Regulamento Mercados Digitais)[73]], não é um terceiro elegível nos termos do presente artigo e, por conseguinte, não pode:

   a) Solicitar ou incentivar comercialmente um utilizador, de qualquer forma, nomeadamente através do fornecimento de compensações pecuniárias ou de qualquer outra natureza, que disponibilize a um dos seus serviços os dados que o utilizador obteve na sequência de um pedido nos termos do artigo 4.º, n.º 1;

   b) Solicitar ou incentivar comercialmente um utilizador a solicitar ao detentor dos dados que os disponibilize a um dos seus serviços, nos termos do n.º 1 do presente artigo;

   c) Receber dados de um utilizador que este obteve na sequência de um pedido de acordo com o artigo 4.º, n.º 1.

3. Não pode exigir-se ao utilizador ou ao terceiro que faculte quaisquer informações para além do necessário para verificar a qualidade de utilizador ou de terceiro nos termos do n.º 1. O detentor dos dados não pode conservar quaisquer informações sobre o acesso do terceiro aos dados solicitados para além das necessárias para a boa execução do pedido de acesso do terceiro e para a segurança e manutenção da infraestrutura de dados.

4. O terceiro não pode recorrer a meios coercivos nem utilizar abusivamente lacunas evidentes na infraestrutura técnica do detentor dos dados destinada a proteger os dados, a fim de obter acesso aos mesmos.

5. O detentor dos dados não pode utilizar dados não pessoais gerados pela utilização do produto ou serviço conexo para obter informações sobre a situação económica, os ativos e os métodos de produção do terceiro, ou a sua utilização, que possam prejudicar a posição comercial do terceiro nos mercados nos quais exerce a sua atividade, a menos que o terceiro tenha consentido essa utilização e tenha a possibilidade técnica de retirar esse consentimento a qualquer momento.

6. Caso o utilizador não seja titular dos dados, quaisquer dados pessoais gerados pela utilização de um produto ou serviço conexo só podem ser disponibilizados se existir uma base jurídica válida nos termos do artigo 6.º, n.º 1, do Regulamento (UE) 2016/679 e, se for caso disso, forem cumpridas as condições do artigo 9.º do referido regulamento.

7. O facto de o detentor dos dados e o terceiro não chegarem a acordo sobre as modalidades de transmissão dos dados não pode prejudicar, impedir ou dificultar o exercício dos direitos do titular dos dados nos termos do Regulamento (UE) 2016/679 e, em especial, com o direito à portabilidade dos dados previsto no artigo 20.º do referido regulamento.

8. Os segredos comerciais só podem ser divulgados a terceiros na medida em que sejam estritamente necessários para cumprir a finalidade acordada entre o utilizador e o terceiro e que todas as medidas específicas necessárias acordadas entre o detentor dos dados e o terceiro sejam adotadas por este último a fim de preservar a confidencialidade do segredo comercial. Nesse caso, a natureza dos dados enquanto

[73] JO […].

segredos comerciais e as medidas destinadas a preservar a confidencialidade devem ser especificadas no acordo entre o detentor dos dados e o terceiro.

9. O direito a que se refere o n.º 1 não pode prejudicar os direitos de proteção de dados de terceiros.

Artigo 6.º

Obrigações dos terceiros que recebem dados a pedido do utilizador

1. Um terceiro deve tratar os dados que lhe foram disponibilizados nos termos do artigo 5.º unicamente para as finalidades e nas condições acordadas com o utilizador, e sob reserva dos direitos do titular dos dados no que se refere aos dados pessoais, devendo apagá-los quando já não sejam necessários para a finalidade acordada.

2. O terceiro não pode:

   a) Coagir, enganar ou manipular o utilizador de qualquer forma, subvertendo ou prejudicando a autonomia, a tomada de decisões ou as escolhas do utilizador, nomeadamente através de uma interface digital com o utilizador;

   b) Utilizar os dados que recebe para a definição de perfis de pessoas singulares, na aceção do artigo 4.º, n.º 4, do Regulamento (UE) 2016/679, a menos que tal seja necessário para prestar o serviço solicitado pelo utilizador;

   c) Disponibilizar os dados que recebe a terceiros, em bruto, agregados ou num formato derivado, a menos que tal seja necessário para prestar o serviço solicitado pelo utilizador;

   d) Disponibilizar os dados que recebe a uma empresa que preste serviços essenciais de plataforma para os quais um ou vários desses serviços tenham sido designados como controladores de acesso, nos termos do artigo [...] do [Regulamento relativo à disputabilidade e equidade dos mercados no setor digital (Regulamento Mercados Digitais)];

   e) Utilizar os dados que recebe para desenvolver um produto que concorra com o produto do qual os dados acedidos são provenientes ou partilhar os dados com outro terceiro para essa finalidade;

   f) Impedir o utilizador, nomeadamente através de compromissos contratuais, de disponibilizar os dados que recebe a outras partes.

Artigo 7.º

Âmbito das obrigações de partilha de dados entre empresas e consumidores e entre empresas

1. As obrigações do presente capítulo não são aplicáveis aos dados gerados pela utilização de produtos fabricados ou serviços conexos prestados por empresas que sejam consideradas micro ou pequenas empresas, na aceção do artigo 2.º do anexo da Recomendação 2003/361/CE, desde que essas empresas não tenham empresas parceiras ou associadas, na aceção do artigo 3.º do anexo da Recomendação 2003/361/CE, que não sejam consideradas micro ou pequenas empresas.

2. Caso o presente regulamento se refira a produtos ou serviços conexos, entende-se igualmente que essa referência inclui os assistentes virtuais, na medida em que sejam utilizados para aceder ou controlar um produto ou serviço conexo.

CAPÍTULO III
OBRIGAÇÕES DOS DETENTORES DOS DADOS LEGALMENTE OBRIGADOS A DISPONIBILIZAR OS DADOS

Artigo 8.º

Condições em que os detentores dos dados disponibilizam os dados aos seus destinatários

1. Caso um detentor de dados seja obrigado a disponibilizar os dados a um destinatário nos termos do artigo 5.º ou de outra legislação da União ou da legislação nacional que transpõe o direito da União, deve fazê-lo em condições justas, razoáveis e não discriminatórias e de forma transparente, em conformidade com o disposto no presente capítulo e no capítulo IV.

2. Um detentor de dados deve chegar a acordo com o destinatário dos dados no que se refere às condições da respetiva disponibilização. Uma cláusula contratual relativa ao acesso aos dados e à sua utilização ou à responsabilidade e às vias de recurso pela violação ou cessação de obrigações relacionadas com os dados não é vinculativa se cumprir as condições do artigo 13.º ou se excluir a aplicação dos direitos do utilizador nos termos do capítulo II, constituir uma derrogação dos mesmos ou alterar os seus efeitos.

3. Ao disponibilizar os dados, o detentor dos dados não pode discriminar entre categorias comparáveis de destinatários dos dados, incluindo empresas parceiras ou empresas associadas, na aceção do artigo 3.º do anexo da Recomendação 2003/361/CE. Caso um destinatário de dados considere discriminatórias as condições em que os dados lhe foram disponibilizados, cabe ao detentor dos dados demonstrar que não houve discriminação.

4. Um detentor de dados não pode disponibilizar os dados a um destinatário de dados em regime de exclusividade, a menos que o utilizador o solicite nos termos do capítulo II.

5. Os detentores e os destinatários dos dados não podem ser obrigados a facultar quaisquer informações para além das necessárias com vista à verificação do cumprimento das condições contratuais acordadas para a disponibilização dos dados ou das suas obrigações nos termos do presente regulamento ou de outra legislação da União aplicável ou da legislação nacional que transpõe o direito da União.

6. Salvo disposição em contrário do direito da União, incluindo o artigo 6.º do presente regulamento, ou da legislação nacional que transpõe o direito da União, a obrigação de disponibilização dos dados a um destinatário não obriga à divulgação de segredos comerciais na aceção da Diretiva (UE) 2016/943.

Artigo 9.º

Compensação pela disponibilização de dados

1. Qualquer compensação acordada entre o detentor e o destinatário dos dados pela disponibilização dos dados deve ser razoável.

2. Caso o destinatário dos dados seja uma micro, pequena ou média empresa, na aceção do artigo 2.º do anexo da Recomendação 2003/361/CE, qualquer compensação acordada não pode exceder os custos diretamente associados à disponibilização dos

dados ao seu destinatário e que são imputáveis ao pedido. O artigo 8.°, n.º 3, aplica-se em conformidade.

3. O presente artigo não pode obstar a que outra legislação da União ou legislação nacional que transpõe o direito da União exclua a compensação pela disponibilização de dados ou que preveja uma compensação inferior.

4. O detentor dos dados deve facultar ao destinatário dos dados informações sobre a base de cálculo da compensação de forma suficientemente pormenorizada para que o destinatário dos dados possa verificar o cumprimento dos requisitos do n.º 1 e, se for caso disso, do n.º 2.

Artigo 10.º
Resolução de litígios

1. Os detentores e os destinatários dos dados devem ter acesso aos organismos de resolução de litígios, certificados nos termos do n.º 2 do presente artigo, para resolver litígios relacionados com a determinação de condições justas, razoáveis e não discriminatórias para a disponibilização dos dados, e com a forma transparente de o fazer, em conformidade com os artigos 8.º e 9.º.

2. O Estado-Membro em que está estabelecido o organismo de resolução de litígios deve certificá-lo, a pedido desse organismo, sempre que este tenha demonstrado que preenche todas as condições seguintes:

   a) Ser imparcial e independente e adotar as suas decisões de acordo com regras processuais claras e justas;

   b) Dispor dos conhecimentos especializados necessários no que respeita à determinação de condições justas, razoáveis e não discriminatórias para a disponibilização dos dados, e à forma transparente de o fazer, permitindo ao organismo determinar efetivamente esses termos;

   c) Estar facilmente acessível através das tecnologias de comunicação eletrónica;

   d) Ser capaz de adotar as suas decisões de forma rápida, eficiente e eficaz em termos de custos e em, pelo menos, uma língua oficial da União.

   Se não houver nenhum organismo de resolução de litígios certificado num Estado-Membro até [data de aplicação do presente regulamento], esse Estado-Membro deve criar e certificar um organismo de resolução de litígios que cumpra as condições estabelecidas nas alíneas a) a d) do presente número.

3. Os Estados-Membros devem notificar à Comissão os organismos de resolução de litígios certificados em conformidade com o n.º 2. A Comissão deve publicar uma lista desses organismos num sítio Web específico e mantê-la atualizada.

4. Os organismos de resolução de litígios devem comunicar as taxas, ou os mecanismos utilizados para as determinar, às partes em causa antes de estas solicitarem uma decisão.

5. Os organismos de resolução de litígios devem recusar-se a tratar um pedido de resolução de um litígio que já tenha sido submetido a outro organismo de resolução de litígios ou a um órgão jurisdicional de um Estado-Membro.

6. Os organismos de resolução de litígios devem conceder às partes a possibilidade de, num prazo razoável, manifestarem o seu ponto de vista sobre as questões que essas partes apresentaram a esses organismos. Nesse contexto, os organismos de resolução

de litígios devem facultar a essas partes as observações da outra parte e quaisquer declarações de peritos. Esses organismos devem conceder às partes a possibilidade de apresentarem observações sobre essas informações e declarações.

7. Os organismos de resolução de litígios devem adotar qualquer decisão sobre as questões submetidas à sua apreciação no prazo de 90 dias a contar da apresentação do pedido de decisão. Essas decisões devem ser tomadas por escrito ou num suporte duradouro e ser acompanhadas de uma fundamentação da decisão.

8. A decisão do organismo de resolução de litígios só é vinculativa para as partes se estas tiverem dado o seu consentimento explícito à sua natureza vinculativa antes do início do processo de resolução de litígios.

9. O presente artigo não afeta o direito de as partes interporem um recurso efetivo perante um órgão jurisdicional de um Estado-Membro.

Artigo 11.º

Medidas técnicas de proteção e disposições relativas à utilização ou à divulgação não autorizadas de dados

1. O detentor dos dados pode aplicar medidas adequadas de proteção técnica, incluindo contratos inteligentes, a fim de impedir o acesso não autorizado aos dados e assegurar o cumprimento dos artigos 5.º, 6.º, 9.º e 10.º, bem como das condições contratuais acordadas para a disponibilização dos dados. Essas medidas técnicas de proteção não podem ser utilizadas para prejudicar o direito do utilizador de efetivamente facultar dados a terceiros nos termos do artigo 5.º, ou qualquer direito de terceiros ao abrigo do direito da União ou da legislação nacional que transpõe o direito da União, conforme referido no artigo 8.º, n.º 1.

2. Um destinatário de dados que, para efeitos da obtenção de dados, tenha facultado ao detentor dos dados informações inexatas ou falsas, tenha utilizado meios enganosos ou coercivos ou tenha recorrido abusivamente a lacunas evidentes na infraestrutura técnica do detentor dos dados destinadas a protegê-los, tenha utilizado os dados disponibilizados para finalidades não autorizadas ou divulgado esses dados a outra parte sem a autorização do seu detentor, deve, sem demora injustificada, a menos que o detentor ou o utilizador dos dados dê instruções em contrário:

   a) Destruir os dados disponibilizados pelo seu detentor, bem como quaisquer cópias dos mesmos;

   b) Pôr termo à produção, oferta, colocação no mercado ou utilização de bens, serviços ou dados derivados produzidos com base em conhecimentos obtidos através desses dados, ou a importação, a exportação ou o armazenamento de bens em infração para essas finalidades, bem como destruir quaisquer bens em infração.

3. O disposto no n.º 2, alínea b), não é aplicável em nenhum dos seguintes casos:

   a) A utilização dos dados não causou danos significativos ao seu detentor;

   b) Seria desproporcional à luz dos interesses do detentor dos dados.

Artigo 12.º

Âmbito das obrigações dos detentores dos dados legalmente obrigados a disponibilizar os dados

1. O presente capítulo é aplicável sempre que um detentor de dados seja obrigado, nos termos do artigo 5.º, ou por força do direito da União ou da legislação nacional que transpõe o direito da União, a disponibilizar os dados a um destinatário.

2. Qualquer cláusula contratual num acordo de partilha de dados que, em detrimento de uma parte ou, se for caso disso, em detrimento do utilizador, exclua a aplicação do presente capítulo, constitua uma derrogação do mesmo ou altere os seus efeitos, não é vinculativa para essa parte.

3. O presente capítulo é unicamente aplicável às obrigações de disponibilização de dados nos termos do direito da União ou da legislação nacional que transpõe o direito da União, que entrem em vigor após [data de aplicação do presente regulamento].

CAPÍTULO IV
CLÁUSULAS ABUSIVAS RELATIVAS AO ACESSO AOS DADOS E À SUA UTILIZAÇÃO ENTRE EMPRESAS

Artigo 13.º

Cláusulas contratuais abusivas impostas unilateralmente a uma micro, pequena ou média empresa

1. Uma cláusula contratual relativa ao acesso aos dados e à sua utilização ou à responsabilidade e às vias de recurso pela violação ou cessação de obrigações relacionadas com os dados que tenha sido imposta unilateralmente por uma empresa a uma micro, pequena ou média empresa, na aceção do artigo 2.º do anexo da Recomendação 2003/361/CE, não é vinculativa para esta última, caso seja abusiva.

2. Uma cláusula contratual é abusiva se for de tal natureza que a sua utilização se desvie manifestamente das boas práticas comerciais em matéria de acesso e utilização de dados, contrariamente à boa-fé e às práticas comerciais leais.

3. Para efeitos do presente artigo, uma cláusula contratual é considerada abusiva se tiver por objeto ou efeito:

   a) Excluir ou limitar a responsabilidade da parte que impôs unilateralmente a cláusula por atos intencionais ou negligência grosseira;

   b) Excluir as vias de recurso à disposição da parte à qual a cláusula foi imposta unilateralmente em caso de incumprimento de obrigações contratuais ou a responsabilidade da parte que impôs unilateralmente a cláusula em caso de violação dessas obrigações;

   c) Conferir à parte que impôs unilateralmente a cláusula o direito exclusivo de determinar se os dados facultados estão em conformidade com o contrato ou de interpretar qualquer cláusula do contrato.

4. Para efeitos do presente artigo, uma cláusula contratual presume-se abusiva se tiver por objeto ou efeito:

a) Limitar de forma inadequada as vias de recurso em caso de incumprimento das obrigações contratuais ou a responsabilidade em caso de violação dessas obrigações;

b) Permitir que a parte que impôs unilateralmente a cláusula aceda aos dados da outra parte contratante e os utilize de uma forma que prejudique significativamente os interesses legítimos desta última;

c) Impedir a parte a quem a cláusula foi imposta unilateralmente de utilizar os dados facultados ou gerados por essa parte durante a vigência do contrato, ou limitar a utilização desses dados, na medida em que essa parte não tenha o direito de os utilizar, recolher, aceder ou controlar, ou explorar o valor dos mesmos de forma proporcional;

d) Impedir a parte a quem a cláusula foi imposta unilateralmente de obter uma cópia dos dados facultados ou gerados por essa parte durante a vigência do contrato ou num prazo razoável após a rescisão do mesmo;

e) Permitir que a parte que impôs unilateralmente a cláusula rescinda o contrato com um pré-aviso injustificadamente curto, tendo em conta as possibilidades razoáveis da outra parte contratante de mudar para um serviço alternativo e comparável, bem como o prejuízo financeiro causado por essa rescisão, exceto quando existam motivos sérios para o fazer.

5. Considera-se que uma cláusula contratual é imposta unilateralmente, na aceção do presente artigo, se tiver sido facultada por uma parte contratante e a outra parte contratante não tiver podido influenciar o seu teor, apesar de ter tentado negociá-la. Recai sobre a parte contratante que facultou uma cláusula contratual o ónus da prova de que essa cláusula não foi imposta unilateralmente.

6. Caso a cláusula contratual abusiva seja dissociável das restantes cláusulas, estas últimas continuam a ser vinculativas.

7. O presente artigo não é aplicável às cláusulas contratuais que definem o objeto principal do contrato, nem às cláusulas contratuais que determinam o preço a pagar.

8. As partes num contrato a que se refere o n.º 1 não podem excluir a aplicação do presente artigo, constituir uma derrogação do mesmo, nem alterar os seus efeitos.

CAPÍTULO V
DISPONIBILIZAÇÃO DE DADOS AOS ORGANISMOS DO SETOR PÚBLICO E ÀS INSTITUIÇÕES, AGÊNCIAS OU ORGANISMOS DA UNIÃO COM FUNDAMENTO EM NECESSIDADES EXCECIONAIS

Artigo 14.º

Obrigação de disponibilização de dados com fundamento em necessidades excecionais

1. Mediante pedido, o detentor dos dados deve disponibilizá-los a um organismo do setor público ou a uma instituição, agência ou organismo da União que demonstre a necessidade excecional de utilizar os dados solicitados.

2. O presente capítulo não é aplicável às micro e pequenas empresas na aceção do artigo 2.º do anexo da Recomendação 2003/361/CE.

Artigo 15.º
Necessidade excecional de utilizar dados

Considera-se que existe uma necessidade excecional de utilizar dados na aceção do presente capítulo em qualquer das seguintes circunstâncias:

a) Caso os dados solicitados sejam necessários para dar resposta a uma emergência pública;

b) Caso o pedido de dados seja limitado no tempo e no âmbito e necessário para prevenir uma emergência pública ou para apoiar a recuperação de uma emergência pública;

c) Caso a ausência de dados disponíveis impeça o organismo do setor público ou a instituição, agência ou organismo da União de desempenhar uma função específica de interesse público expressamente prevista por lei; e

(1) Não tenha sido possível ao organismo do setor público ou à instituição, agência ou organismo da União obter esses dados por meios alternativos, nomeadamente através da aquisição de dados no mercado a taxas de mercado ou com recurso às obrigações existentes de disponibilização de dados, e a adoção de novas medidas legislativas não possa assegurar a disponibilidade atempada dos mesmos; ou

(2) A obtenção dos dados em conformidade com o procedimento estabelecido no presente capítulo reduza substancialmente os encargos administrativos para os detentores dos dados ou outras empresas.

Artigo 16.º
Relação com outras obrigações de disponibilização de dados aos organismos do setor público e às instituições, agências ou organismos da União

1. O presente capítulo não afeta as obrigações estabelecidas no direito da União ou no direito nacional para efeitos de comunicação, cumprimento dos pedidos de informação ou demonstração ou verificação do cumprimento das obrigações legais.

2. Os direitos previstos no presente capítulo não podem ser exercidos pelos organismos do setor público nem pelas instituições, agências ou organismos da União para o exercício de atividades de prevenção, investigação, deteção ou repressão de infrações penais ou administrativas ou de execução de sanções penais, nem para a administração aduaneira ou fiscal. O presente capítulo não afeta o direito da União nem o direito nacional aplicável em matéria de prevenção, investigação, deteção ou repressão de infrações penais ou administrativas ou de execução de sanções penais ou administrativas, ou de administração aduaneira ou fiscal.

Artigo 17.º
Pedidos de disponibilização de dados

1. Ao solicitar dados nos termos do artigo 14.º, n.º 1, um organismo do setor público ou uma instituição, agência ou organismo da União deve:

a) Especificar os dados que são necessários;

b) Demonstrar a necessidade excecional para a qual se solicitam os dados;

c) Explicar a finalidade do pedido, a utilização prevista dos dados solicitados e a duração dessa utilização;

d) Indicar a base jurídica para o pedido dos dados;

e) Especificar o prazo em que os dados devem ser disponibilizados ou no qual o seu detentor pode solicitar ao organismo do setor público ou à instituição, agência ou organismo da União que altere ou retire o pedido.

2. Um pedido de dados apresentado nos termos do n.º 1 do presente artigo deve:

a) Ser formulado em linguagem clara, concisa e simples, compreensível pelo detentor dos dados;

b) Ser proporcional à necessidade excecional, em termos de granularidade e volume dos dados solicitados e à frequência de acesso aos mesmos;

c) Respeitar os objetivos legítimos do detentor dos dados, tendo em conta a proteção dos segredos comerciais e os custos e esforços necessários para os disponibilizar;

d) Dizer respeito, na medida do possível, a dados não pessoais;

e) Informar o detentor dos dados quanto às sanções impostas nos termos do artigo 33.º por uma autoridade competente a que se refere o artigo 31.º em caso de incumprimento do pedido;

f) Ser publicado em linha, sem demora injustificada.

3. Um organismo do setor público ou uma instituição, agência ou organismo da União não pode disponibilizar os dados obtidos nos termos do presente capítulo para reutilização, na aceção da Diretiva (UE) 2019/1024. A referida diretiva não é aplicável aos dados na posse de organismos do setor público que foram obtidos nos termos do presente capítulo.

4. O disposto no n.º 3 não obsta a que um organismo do setor público ou uma instituição, agência ou organismo da União proceda ao intercâmbio de dados obtidos nos termos do presente capítulo com outro organismo do setor público ou com uma instituição, agência ou organismo da União, tendo em vista o desempenho das funções previstas no artigo 15.º, ou que disponibilizem os dados a terceiros nos casos em que tenham subcontratado, por meio de um acordo publicamente disponível, inspeções técnicas ou outras funções a esse terceiro. São aplicáveis as obrigações dos organismos do setor público e das instituições, agências ou organismos da União nos termos do artigo 19.º.

Caso um organismo do setor público ou uma instituição, agência ou organismo da União transmita ou disponibilize dados nos termos do presente número, deve notificar o detentor que os enviou.

Artigo 18.º
Cumprimento dos pedidos de dados

1. Um detentor de dados que receba um pedido de acesso a dados nos termos do presente capítulo deve disponibilizá-los ao organismo do setor público ou a uma instituição, agência ou organismo da União requerente sem demora injustificada.

2. Sem prejuízo das necessidades específicas relativas à disponibilidade de dados definidas na legislação setorial, o detentor dos dados pode recusar ou solicitar a

alteração do pedido no prazo de cinco dias úteis a contar da receção de um pedido de dados necessários para dar resposta a uma emergência pública e no prazo de 15 dias úteis noutros casos de necessidade excecional, por um dos seguintes motivos:

a) Os dados não estão disponíveis;

b) O pedido não cumpre as condições estabelecidas no artigo 17.º, n.os 1 e 2.

3. No caso de um pedido de dados necessários para dar resposta a uma emergência pública, o detentor dos dados pode também recusar ou solicitar a alteração do pedido se o titular dos dados já tiver facultado os dados solicitados em resposta a um pedido anteriormente apresentado para a mesma finalidade por outro organismo do setor público ou por uma instituição, agência ou organismo da União e o detentor dos dados não tiver sido notificado da destruição dos dados nos termos do artigo 19.º, n.º 1, alínea c).

4. Se o detentor dos dados decidir recusar o pedido ou solicitar a sua alteração em conformidade com o n.º 3, deve indicar a identidade do organismo do setor público ou da instituição, agência ou organismo da União que apresentou anteriormente um pedido para a mesma finalidade.

5. Caso o cumprimento do pedido de disponibilização de dados a um organismo do setor público ou a uma instituição, agência ou organismo da União exija a divulgação de dados pessoais, o seu detentor deve envidar esforços razoáveis para os pseudonimizar, na medida em que o pedido possa ser satisfeito com dados pseudonimizados.

6. Caso o organismo do setor público ou a instituição, agência ou organismo da União pretenda contestar a recusa de um detentor dos dados em facultar os dados solicitados ou o facto de solicitar a alteração do pedido, ou caso o detentor dos dados pretenda contestar o pedido, a matéria deve ser sujeita à apreciação da autoridade competente a que se refere o artigo 31.º.

Artigo 19.º

Obrigações dos organismos do setor público e das instituições, agências ou organismos da União

1. Um organismo do setor público ou uma instituição, agência ou organismo da União que tenha recebido dados na sequência de um pedido apresentado nos termos do artigo 14.º:

a) Não pode utilizar os dados de forma incompatível com a finalidade para a qual foram solicitados;

b) Deve aplicar, na medida em que o tratamento de dados pessoais seja necessário, medidas técnicas e organizativas que salvaguardem os direitos e liberdades dos titulares dos dados;

c) Deve destruir os dados quando já não sejam necessários para a finalidade indicada e informar o detentor dos dados de que os mesmos foram destruídos.

2. A divulgação de segredos comerciais, ou de alegados segredos comerciais, a um organismo do setor público ou a uma instituição, agência ou organismo da União só pode ser exigida na medida do estritamente necessário para a consecução do objetivo do pedido. Nesse caso, o organismo do setor público ou a instituição, agência ou

organismo da União toma as medidas adequadas para preservar a confidencialidade desses segredos comerciais.

Artigo 20.º
Compensação em caso de necessidade excecional

1. Os dados disponibilizados para dar resposta a uma emergência pública nos termos do artigo 15.º, alínea a), devem ser facultados a título gratuito.

2. Caso o detentor dos dados solicite uma compensação pela disponibilização dos mesmos em conformidade com um pedido apresentado nos termos do artigo 15.º, alíneas b) ou c), essa compensação não pode exceder os custos técnicos e organizativos incorridos para dar cumprimento ao pedido, incluindo, se necessário, os custos de anonimização e de adaptação técnica, acrescidos de uma margem razoável. A pedido do organismo do setor público ou da instituição, agência ou organismo da União que solicita os dados, o detentor dos dados deve facultar informações sobre a base de cálculo dos custos e da margem razoável.

Artigo 21.º
Contribuição das organizações de investigação ou dos organismos de estatística no contexto de necessidades excecionais

1. Um organismo do setor público ou uma instituição, agência ou organismo da União tem o direito de partilhar os dados recebidos nos termos do presente capítulo com pessoas singulares ou organizações, com vista à realização de investigações ou análises científicas compatíveis com a finalidade para a qual os dados foram solicitados, ou com os institutos nacionais de estatística e o Eurostat para a compilação de estatísticas oficiais.

2. As pessoas ou as organizações que recebam os dados nos termos do n.º 1 devem prosseguir fins não lucrativos ou agir no contexto de uma missão de interesse público reconhecida pelo direito da União ou dos Estados-Membros. Não podem incluir organizações sobre as quais empresas comerciais tenham uma influência decisiva ou que possam dar origem a um acesso preferencial aos resultados da investigação.

3. As pessoas ou as organizações que recebem os dados nos termos do n.º 1 devem cumprir o disposto no artigo 17.º, n.º 3, e no artigo 19.º.

4. Caso um organismo do setor público ou uma instituição, agência ou organismo da União transmita ou disponibilize dados nos termos do n.º 1, deve notificar o detentor que os enviou.

Artigo 22.º
Assistência mútua e cooperação transfronteiriça

1. Os organismos do setor público e as instituições, agências ou organismos da União devem cooperar e prestar assistência mútua, a fim de aplicar o presente capítulo de forma coerente.

2. Os dados objeto de intercâmbio no contexto de um pedido e da prestação de assistência nos termos do n.º 1 não podem ser utilizados de um modo incompatível com a finalidade para a qual foram solicitados.

3. Caso um organismo do setor público pretenda solicitar dados a um detentor estabelecido noutro Estado-Membro, deve notificar previamente dessa intenção a

autoridade competente desse Estado-Membro, conforme referido no artigo 31.º. Este requisito é igualmente aplicável aos pedidos apresentados pelas instituições, agências ou organismos da União.

4. Após ter sido notificada nos termos do n.º 3, a autoridade competente deve aconselhar o organismo do setor público requerente sobre a eventual necessidade de cooperar com os organismos do setor público do Estado-Membro em que o detentor dos dados está estabelecido, com o objetivo de reduzir os encargos administrativos que recaem sobre o detentor dos dados ao satisfazer o pedido. O organismo do setor público requerente deve ter em consideração o aconselhamento da autoridade competente.

CAPÍTULO VI

MUDANÇA ENTRE SERVIÇOS DE TRATAMENTO DE DADOS

Artigo 23.º

Eliminar os obstáculos à mudança eficaz entre prestadores de serviços de tratamento de dados

1. Os prestadores de um serviço de tratamento de dados devem tomar as medidas previstas nos artigos 24.º, 25.º e 26.º, a fim de garantir que os clientes do seu serviço possam mudar para outro serviço de tratamento de dados, que abranja o mesmo tipo de serviço, disponibilizado por outro prestador de serviços. Em especial, os prestadores de serviços de tratamento de dados devem eliminar os obstáculos comerciais, técnicos, contratuais e organizativos que impedem os clientes de:

   a) Rescindir o acordo contratual do serviço, após um período máximo de pré-aviso de 30 dias consecutivos;

   b) Celebrar novos acordos contratuais com outro prestador de serviços de tratamento de dados que abranjam o mesmo tipo de serviço;

   c) Transferir os seus dados, aplicações e outros ativos digitais para outro prestador de serviços de tratamento de dados;

   d) Manter a equivalência funcional do serviço no ambiente informático do outro ou dos outros prestadores de serviços de tratamento de dados que abranjam o mesmo tipo de serviço, em conformidade com o artigo 26.º.

2. O n.º 1 é unicamente aplicável aos obstáculos relacionados com os serviços, os acordos contratuais ou as práticas comerciais disponibilizados pelo prestador inicial.

Artigo 24.º

Cláusulas contratuais relativas à mudança de prestador de serviços de tratamento de dados

1. Os direitos do cliente e as obrigações do prestador de um serviço de tratamento de dados em relação à mudança de prestador desses serviços devem ser estabelecidos de forma clara num contrato escrito. Sem prejuízo do disposto na Diretiva (UE) 2019/770, esse contrato deve incluir, pelo menos, os seguintes elementos:

a) Cláusulas que permitam ao cliente, mediante pedido, mudar para um serviço de tratamento de dados disponibilizado por outro prestador de serviços de tratamento de dados ou transferir todos os dados, aplicações e ativos digitais gerados direta ou indiretamente pelo cliente para um sistema local, em especial o estabelecimento de um período de transição máximo obrigatório de 30 dias consecutivos, durante o qual o prestador de serviços de tratamento de dados:

   1) Deve prestar assistência e, caso seja tecnicamente viável, conclui o processo de mudança;

   2) Deve assegurar a plena continuidade da prestação das respetivas funções ou serviços;

b) Uma especificação exaustiva de todas as categorias de dados e aplicações que podem ser exportadas durante o processo de mudança, incluindo, no mínimo, todos os dados importados pelo cliente no início do contrato de prestação do serviço e todos os dados e metadados criados pelo cliente e pela utilização do serviço durante o período em que o serviço foi prestado, incluindo, entre outros, parâmetros de configuração, parâmetros de segurança, direitos de acesso e registos de acesso ao serviço;

c) Um período mínimo de recuperação de dados de, pelo menos, 30 dias consecutivos, com início após o termo do período de transição acordado entre o cliente e o prestador de serviços, em conformidade com o n.º 1, alínea a), e o n.º 2.

2. Caso o período de transição obrigatório fixado no n.º 1, alíneas a) e c), do presente artigo seja tecnicamente inviável, o prestador de serviços de tratamento de dados deve notificar o cliente no prazo de sete dias úteis a contar da apresentação do pedido de mudança, fundamentando devidamente a inviabilidade técnica com um relatório pormenorizado e indicando um período de transição alternativo, que não pode ser superior a seis meses. Em conformidade com o n.º 1 do presente artigo, deve assegurar a plena continuidade do serviço durante todo o período de transição alternativo, mediante encargos reduzidos, aos quais se refere o artigo 25.º, n.º 2.

Artigo 25.º

Supressão gradual dos encargos decorrentes da mudança

1. A partir de [data X + três anos], os prestadores de serviços de tratamento de dados não podem impor quaisquer encargos ao cliente pelo processo de mudança.

2. A partir de [data X, a data de entrada em vigor do Regulamento Dados] até [data X + três anos], os prestadores de serviços de tratamento de dados podem impor encargos reduzidos ao cliente decorrentes do processo de mudança.

3. Os encargos a que se refere o n.º 2 não podem exceder os custos incorridos pelo prestador de serviços de tratamento de dados diretamente relacionados com o processo de mudança em causa.

4. A Comissão fica habilitada a adotar atos delegados em conformidade com o artigo 38.º que complementem o presente regulamento, a fim de introduzir um mecanismo de controlo que lhe permita fazer o acompanhamento dos encargos de mudança impostos pelos prestadores de serviços de tratamento de dados no mercado, de modo a assegurar que a supressão dos encargos decorrentes da mudança,

conforme descrita no n.º 1 do presente artigo, é alcançada no prazo previsto no mesmo número.

Artigo 26.º
Aspetos técnicos da mudança de prestador

1. Os prestadores de serviços de tratamento de dados que digam respeito a recursos de computação moduláveis e adaptáveis limitados a elementos infraestruturais, como servidores, redes e recursos virtuais necessários para o funcionamento da infraestrutura, mas que não facultem acesso às aplicações, ao *software* e aos serviços operacionais armazenados, tratados ou implantados nesses elementos infraestruturais, devem assegurar que o cliente, após ter mudado para um serviço que abranja o mesmo tipo de serviço disponibilizado por outro prestador de serviços de tratamento de dados, goza de equivalência funcional na utilização do novo serviço.
2. No caso de serviços de tratamento de dados não abrangidos pelo n.º 1, os prestadores de serviços de tratamento de dados devem disponibilizar ao público interfaces abertas, a título gratuito.
3. No caso de serviços de tratamento de dados não abrangidos pelo n.º 1, os prestadores de serviços de tratamento de dados devem assegurar a compatibilidade com as especificações de interoperabilidade aberta ou com as normas europeias de interoperabilidade identificadas em conformidade com o artigo 29.º, n.º 5, do presente regulamento.
4. Caso não existam especificações de interoperabilidade aberta ou normas europeias a que se refere o n.º 3 para o tipo de serviço em causa, o prestador de serviços de tratamento de dados, a pedido do cliente, deve exportar todos os dados gerados ou cogerados, incluindo os formatos de dados e as estruturas de dados pertinentes, num formato estruturado, de uso corrente e de leitura automática.

CAPÍTULO VII
GARANTIAS PARA OS DADOS NÃO PESSOAIS EM CONTEXTOS INTERNACIONAIS

Artigo 27.º
Acesso e transferência internacionais

1. Os prestadores de serviços de tratamento de dados devem tomar todas as medidas técnicas, jurídicas e organizativas razoáveis, incluindo disposições contratuais, a fim de impedir transferências internacionais ou o acesso governamental a dados não pessoais detidos na União, caso essa transferência ou esse acesso seja suscetível de criar um conflito com o direito da União ou o direito nacional do Estado-Membro pertinente, sem prejuízo do disposto nos n.ºs 2 ou 3.
2. Qualquer decisão de órgãos jurisdicionais ou de outras autoridades judiciais ou administrativas de um país terceiro que exija que um prestador de serviços de tratamento de dados transfira dados não pessoais detidos na União e que sejam abrangidos pelo âmbito do presente regulamento, ou que conceda acesso aos mesmos, só pode ser reconhecida ou executada se tiver por base um acordo internacional, como, por exemplo, um acordo de assistência judiciária mútua, em

vigor entre o país terceiro em causa e a União ou entre esse país terceiro e um Estado-Membro.

3. Na ausência de tal acordo internacional, caso um prestador de serviços de tratamento de dados seja o destinatário de uma decisão de órgãos jurisdicionais ou de outras autoridades judiciais ou administrativas de um país terceiro para que transfira dados não pessoais detidos na União e que sejam abrangidos pelo âmbito do presente regulamento, ou que conceda acesso aos mesmos, e caso o cumprimento dessa decisão seja suscetível de colocar o destinatário em conflito com o direito da União ou com o direito nacional do Estado-Membro pertinente, a transferência dos dados para essa autoridade do país terceiro, bem como o acesso aos dados pela mesma, só podem ocorrer:

   a) Caso o sistema do país terceiro exija o estabelecimento dos motivos e da proporcionalidade da decisão ou da sentença, bem como que essa decisão ou sentença, consoante o caso, tenha um caráter específico, por exemplo, ao estabelecer uma ligação suficiente a determinados suspeitos ou infrações;

   b) Caso a objeção fundamentada do destinatário esteja sujeita a controlo no país terceiro por um órgão jurisdicional competente; e

   c) Caso o órgão jurisdicional competente que proferiu a decisão ou sentença ou que aprecia a decisão de uma autoridade administrativa esteja habilitado, nos termos do direito desse país, a ter devidamente em conta os interesses jurídicos pertinentes do fornecedor dos dados protegidos pelo direito da União ou pelo direito nacional do Estado-Membro pertinente.

O destinatário da decisão pode solicitar o parecer dos organismos ou das autoridades competentes, nos termos do presente regulamento, a fim de determinar se essas condições são cumpridas, nomeadamente quando considerar que a decisão pode dizer respeito a dados comercialmente sensíveis, ou pode colidir com os interesses de segurança nacional ou de defesa da União ou dos seus Estados-Membros.

O Conselho Europeu da Inovação de Dados, criado ao abrigo do Regulamento [xxx – Regulamento Governação de Dados], presta aconselhamento e assistência à Comissão na elaboração de diretrizes sobre a avaliação do cumprimento destas condições.

4. Se as condições previstas nos n.os 2 ou 3 forem cumpridas, o prestador de serviços de tratamento de dados deve facultar a quantidade mínima e admissível de dados em resposta a um pedido, com base numa interpretação razoável do mesmo.

5. O prestador de serviços de tratamento de dados deve informar o detentor dos dados da existência de um pedido de acesso aos seus dados apresentado por uma autoridade administrativa de um país terceiro, antes de satisfazer o seu pedido, exceto nos casos em que o pedido vise finalidades de fiscalização do cumprimento da lei e enquanto tal for necessário para preservar a eficácia dessas atividades.

CAPÍTULO VIII
INTEROPERABILIDADE

Artigo 28.º
Requisitos essenciais em matéria de interoperabilidade

1. Os operadores de espaços de dados devem cumprir os seguintes requisitos essenciais a fim de facilitar a interoperabilidade dos dados, dos serviços e dos mecanismos de partilha de dados:

   a) O conteúdo do conjunto de dados, as restrições de utilização, as licenças, a metodologia de recolha de dados, a qualidade e a incerteza dos dados devem ser suficientemente descritos para possibilitar que o destinatário encontre os dados, a eles aceda e os utilize;

   b) As estruturas de dados, os formatos dos dados, os vocabulários, os sistemas de classificação, as taxonomias e as listas de códigos devem ser descritos de forma coerente e acessível ao público;

   c) Os meios técnicos de acesso aos dados, como as interfaces de programação de aplicações, bem como as respetivas condições de utilização e a qualidade do serviço devem ser suficientemente descritos para possibilitar o acesso e a transmissão automáticos de dados entre as partes, incluindo continuamente ou em tempo real num formato de leitura automática;

   d) Devem ser disponibilizados os meios para permitir a interoperabilidade dos contratos inteligentes no âmbito dos seus serviços e atividades.

Estes requisitos podem revestir-se de uma natureza genérica ou dizer respeito a setores específicos, tendo plenamente em conta a inter-relação com os requisitos provenientes de outra legislação setorial nacional ou da União.

2. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 38.º para completar o presente regulamento mediante uma maior especificação dos requisitos essenciais a que se refere o n.º 1.

3. Presume-se que os operadores de espaços de dados que cumprem as normas harmonizadas, ou partes das mesmas, publicadas por referência no *Jornal Oficial da União Europeia* estão em conformidade com os requisitos essenciais a que se refere o n.º 1 do presente artigo, na medida em que essas normas abranjam esses requisitos.

4. A Comissão, em conformidade com o artigo 10.º do Regulamento (UE) n.º 1025/2012, pode solicitar a uma ou várias organizações europeias de normalização que elaborem normas harmonizadas que satisfaçam os requisitos essenciais previstos no n.º 1 do presente artigo.

5. Caso não existam as normas harmonizadas a que se refere o n.º 4 do presente artigo, ou caso considere que as normas harmonizadas aplicáveis são insuficientes para garantir a conformidade com os requisitos essenciais previstos no n.º 1 do presente artigo, se for caso disso e por meio de atos de execução, a Comissão deve adotar especificações comuns no que diz respeito a alguns ou a todos os requisitos estabelecidos no n.º 1 do presente artigo. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2.

6. A Comissão pode adotar diretrizes que estabeleçam especificações de interoperabilidade para o funcionamento de espaços comuns europeus de dados,

como modelos de arquitetura e normas técnicas de execução de regras jurídicas e acordos entre as partes que promovam a partilha de dados, nomeadamente no que diz respeito aos direitos de acesso e tradução técnica do consentimento ou da autorização.

Artigo 29.º
Interoperabilidade dos serviços de tratamento de dados

1. As especificações de interoperabilidade aberta e as normas europeias de interoperabilidade dos serviços de tratamento de dados devem:

   a) Ser orientadas para a interoperabilidade entre diferentes serviços de tratamento de dados que abranjam o mesmo tipo de serviço;

   b) Melhorar a portabilidade dos ativos digitais entre diferentes serviços de tratamento de dados que abranjam o mesmo tipo de serviço;

   c) Garantir, caso seja tecnicamente viável, a equivalência funcional entre os diferentes serviços de tratamento de dados que abranjam o mesmo tipo de serviço.

2. As especificações de interoperabilidade aberta e as normas europeias de interoperabilidade dos serviços de tratamento de dados têm de abordar:

   a) Os aspetos da interoperabilidade da computação em nuvem da interoperabilidade dos transportes, da interoperabilidade sintática, da interoperabilidade semântica dos dados, da interoperabilidade comportamental e da interoperabilidade das políticas;

   b) Os aspetos da portabilidade dos dados em nuvem da portabilidade sintática dos dados, da portabilidade semântica dos dados e da portabilidade das políticas de dados;

   c) Os aspetos da aplicação em nuvem da portabilidade sintática das aplicações, da portabilidade das instruções das aplicações, da portabilidade dos metadados das aplicações, da portabilidade do comportamento das aplicações e da portabilidade das políticas de aplicação.

3. As especificações de interoperabilidade aberta devem cumprir o disposto nos pontos 3 e 4 do anexo II do Regulamento (UE) n.º 1025/2012.

4. A Comissão, em conformidade com o artigo 10.º do Regulamento (UE) n.º 1025/2012, pode solicitar a uma ou várias organizações europeias de normalização que elaborem normas europeias aplicáveis a tipos específicos de serviços de tratamento de dados.

5. Para efeitos do artigo 26.º, n.º 3, do presente regulamento, a Comissão fica habilitada a adotar atos delegados, nos termos do artigo 38.º, para publicar a referência das especificações de interoperabilidade aberta e das normas europeias para a interoperabilidade dos serviços de tratamento de dados no repositório central de normas da União, com vista à interoperabilidade dos serviços de tratamento de dados, caso estes cumpram os critérios especificados nos n.os 1 e 2 do presente artigo.

Artigo 30.º

Requisitos essenciais em matéria de contratos inteligentes de partilha de dados

1. O vendedor de uma aplicação que utilize contratos inteligentes ou, na sua ausência, a pessoa cuja atividade comercial, empresarial ou profissional implique a implantação de contratos inteligentes para terceiros no contexto de um acordo de disponibilização de dados, deve cumprir os seguintes requisitos essenciais:

   a) Solidez: assegurar que o contrato inteligente foi concebido de modo a proporcionar um elevado grau de solidez, a fim de evitar erros funcionais e resistir à manipulação por terceiros;

   b) Cessação e interrupção seguras: assegurar a existência de um mecanismo para pôr termo à execução continuada das operações — o contrato inteligente deve incluir funções internas que permitam redefinir ou dar instruções ao contrato de modo a parar ou interromper a operação, a fim de evitar futuras execuções (acidentais);

   c) Arquivo e continuidade dos dados: se um contrato inteligente tiver de ser rescindido ou desativado, prever a possibilidade de arquivar dados sobre as transações, a lógica do contrato inteligente e o código, a fim de conservar o registo das operações realizadas anteriormente nos dados (auditabilidade); e

   d) Controlo do acesso: os contratos inteligentes devem ser protegidos através de mecanismos rigorosos de controlo do acesso ao nível da governação e dos contratos inteligentes.

2. O vendedor de um contrato inteligente ou, na sua ausência, a pessoa cuja atividade comercial, empresarial ou profissional implique a implantação de contratos inteligentes para terceiros no contexto de um acordo de disponibilização de dados deve efetuar uma avaliação da conformidade com vista ao cumprimento dos requisitos essenciais estabelecidos no n.º 1 e, no que respeita ao cumprimento dos requisitos, emitir uma declaração de conformidade UE.

3. Ao elaborar a declaração de conformidade UE, o vendedor de uma aplicação que utilize contratos inteligentes ou, na sua ausência, a pessoa cuja atividade comercial, empresarial ou profissional implique a implantação de contratos inteligentes para terceiros no contexto de um acordo de disponibilização de dados é responsável pelo cumprimento dos requisitos previstos no n.º 1.

4. Presume-se que um contrato inteligente que cumpre as normas harmonizadas, ou as partes pertinentes das mesmas, elaboradas e publicadas no *Jornal Oficial da União Europeia* está em conformidade com os requisitos essenciais estabelecidos no n.º 1 do presente artigo, na medida em que essas normas abranjam esses requisitos.

5. A Comissão, em conformidade com o artigo 10.º do Regulamento (UE) n.º 1025/2012, pode solicitar a uma ou várias organizações europeias de normalização que elaborem normas harmonizadas que satisfaçam os requisitos essenciais previstos no n.º 1 do presente artigo.

6. Na ausência das normas harmonizadas a que se refere o n.º 4 do presente artigo ou caso a Comissão considere que as normas harmonizadas existentes são insuficientes para assegurar a conformidade com os requisitos essenciais estabelecidos no n.º 1 do presente artigo num contexto transfronteiriço, a Comissão pode, por meio de atos de execução, adotar especificações comuns relativas aos requisitos essenciais

estabelecidos no n.º 1 do presente artigo. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2.

CAPÍTULO IX
EXECUÇÃO E FISCALIZAÇÃO DO CUMPRIMENTO

Artigo 31.º
Autoridades competentes

1. Cada Estado-Membro designa uma ou mais autoridades competentes responsáveis pela execução e fiscalização do cumprimento do presente regulamento. Os Estados-Membros podem criar uma ou várias novas autoridades ou recorrer às existentes.

2. Sem prejuízo do disposto no n.º 1 do presente artigo:

   a) As autoridades de controlo independentes responsáveis pelo controlo da aplicação do Regulamento (UE) 2016/679 são responsáveis pelo controlo da aplicação do presente regulamento no que diz respeito à proteção dos dados pessoais. Os capítulos VI e VII do Regulamento (UE) 2016/679 são aplicáveis com as devidas adaptações. As funções e as competências das autoridades de controlo devem ser exercidas no que diz respeito ao tratamento de dados pessoais;

   b) No caso de questões específicas de intercâmbio setorial de dados a respeito da aplicação do presente regulamento, a competência das autoridades setoriais deve ser respeitada;

   c) A autoridade nacional competente responsável pela execução e fiscalização do cumprimento do disposto no capítulo VI do presente regulamento deve ter experiência no domínio dos serviços de comunicações eletrónicas e dados.

3. Os Estados-Membros devem assegurar que as funções e competências das autoridades competentes designadas nos termos do n.º 1 do presente artigo são claramente definidas e incluem:

   a) A promoção da sensibilização dos utilizadores e das entidades abrangidas pelo âmbito do presente regulamento no que se refere aos direitos e às obrigações estabelecidos no presente regulamento;

   b) O tratamento das reclamações decorrentes de alegadas violações do presente regulamento, a investigação, na medida do necessário, do conteúdo das reclamações, e prestação de informações aos seus autores sobre o andamento e o resultado das investigações num prazo razoável, em especial se for necessário realizar atividades de investigação ou de coordenação complementares com outras autoridades competentes;

   c) A realização de investigações em matérias relativas à aplicação do presente regulamento, nomeadamente com base em informações recebidas de outras autoridades competentes ou de outras autoridades públicas;

   d) A imposição, por meio de procedimentos administrativos, de sanções financeiras dissuasivas, que podem incluir sanções periódicas e sanções com efeitos retroativos, ou a instauração de processos judiciais para a aplicação de coimas;

e) O acompanhamento da evolução tecnológica pertinente para a disponibilização e a utilização dos dados;

f) A cooperação com as autoridades competentes de outros Estados-Membros, a fim de assegurar a aplicação coerente do presente regulamento, incluindo o intercâmbio de todas as informações pertinentes por via eletrónica, sem demora injustificada;

g) A garantia da disponibilização pública em linha dos pedidos de acesso aos dados, apresentados por organismos do setor público em caso de emergência pública ao abrigo do capítulo V;

h) A cooperação com todas as autoridades competentes, a fim de assegurar que as obrigações previstas no capítulo VI são aplicadas de forma coerente com outra legislação da União e com a autorregulação aplicável aos prestadores de serviços de tratamento de dados;

i) A garantia da supressão dos encargos pela mudança de prestador de serviços de tratamento de dados, em conformidade com o artigo 25.º.

4. Caso um Estado-Membro designe mais do que uma autoridade competente, as autoridades competentes, no exercício das funções e competências que lhes são conferidas nos termos do n.º 3 do presente artigo, devem cooperar entre si, incluindo, se for caso disso, com a autoridade de controlo responsável pelo controlo da aplicação do Regulamento (UE) 2016/679, a fim de assegurar a aplicação coerente do presente regulamento. Nesses casos, os Estados-Membros devem designar uma autoridade competente coordenadora.

5. Os Estados-Membros devem comunicar à Comissão o nome das autoridades competentes designadas e as respetivas funções e competências e, se for caso disso, o nome da autoridade competente coordenadora. A Comissão deve manter um registo público dessas autoridades.

6. No desempenho das suas funções e no exercício das suas competências em conformidade com o presente regulamento, as autoridades competentes devem estar livres de qualquer influência externa, direta ou indireta, e não solicitar nem aceitar instruções de qualquer outra autoridade pública ou de qualquer entidade privada.

7. Os Estados-Membros devem assegurar que as autoridades competentes designadas dispõem dos recursos necessários para desempenhar adequadamente as suas funções em conformidade com o presente regulamento.

Artigo 32.º
Direito de apresentar reclamações a uma autoridade competente

1. Sem prejuízo de qualquer outra via de recurso administrativa ou judicial, as pessoas singulares e coletivas têm o direito de apresentar reclamações, a título individual ou, se for caso disso, coletivamente, a uma autoridade competente do Estado-Membro da sua residência habitual, do seu local de trabalho ou do seu estabelecimento, se considerarem que os seus direitos ao abrigo do presente regulamento foram violados.

2. A autoridade competente à qual tenha sido apresentada uma reclamação informa o autor da reclamação quanto à evolução do processo e à decisão tomada.

3. As autoridades competentes devem cooperar com vista ao tratamento e resolução das reclamações, incluindo pelo intercâmbio de todas as informações pertinentes por via

eletrónica, sem demora injustificada. Essa cooperação não afeta o mecanismo específico de cooperação previsto nos capítulos VI e VII do Regulamento (UE) 2016/679.

Artigo 33.º
Sanções

1. Os Estados-Membros devem estabelecer as regras relativas às sanções aplicáveis em caso de violação do disposto no presente regulamento e tomar todas as medidas necessárias para garantir a sua aplicação. As sanções previstas têm de ser efetivas, proporcionais e dissuasivas.
2. Os Estados-Membros devem notificar a Comissão dessas regras e dessas medidas até [data de aplicação do presente regulamento] e de qualquer alteração posterior das mesmas no mais breve prazo possível.
3. Em caso de violação das obrigações estabelecidas nos capítulos II, III e V do presente regulamento, as autoridades de controlo a que se refere o artigo 51.º do Regulamento (UE) 2016/679 podem, no âmbito das suas competências, aplicar coimas em conformidade com o artigo 83.º do Regulamento (UE) 2016/679, até ao montante referido no artigo 83.º, n.º 5, do mesmo regulamento.
4. Em caso de violação das obrigações estabelecidas no capítulo V do presente regulamento, a autoridade de controlo a que se refere o artigo 52.º do Regulamento (UE) 2018/1725 pode aplicar, no âmbito das suas competências, coimas em consonância com o artigo 66.º do Regulamento (UE) 2018/1725, até ao montante referido no artigo 66.º, n.º 3, do mesmo regulamento.

Artigo 34.º
Modelos de cláusulas contratuais

A Comissão deve elaborar e recomendar modelos de cláusulas contratuais não vinculativos sobre o acesso e a utilização dos dados, a fim de prestar assistência às partes na elaboração e na negociação de contratos equilibrados em termos de direitos e obrigações.

CAPÍTULO X
DIREITO *SUI GENERIS* NOS TERMOS DA DIRETIVA 96/9/CE

Artigo 35.º
Bases de dados que contêm determinados dados

A fim de não impedir o exercício do direito dos utilizadores de acederem e utilizarem esses dados, em conformidade com o artigo 4.º do presente regulamento, ou do direito de partilharem esses dados com terceiros, nos termos do artigo 5.º do presente regulamento, o direito *sui generis* previsto no artigo 7.º da Diretiva 96/9/CE não é aplicável às bases de dados que contenham dados obtidos ou gerados pela utilização de um produto ou serviço conexo.

CAPÍTULO XI
DISPOSIÇÕES FINAIS

Artigo 36.º
Alteração do Regulamento (UE) 2017/2394

Ao anexo do Regulamento (UE) 2017/2394, é aditado o seguinte ponto:

«29. [Regulamento (UE) XXXX/XXX do Parlamento Europeu e do Conselho (Regulamento Dados)]».

Artigo 37.º
Alteração da Diretiva (UE) 2020/1828

Ao anexo da Diretiva (UE) 2020/1828, é aditado o seguinte ponto:

«67. [Regulamento (UE) XXXX/XXX do Parlamento Europeu e do Conselho (Regulamento Dados)]».

Artigo 38.º
Exercício da delegação

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

2. O poder de adotar atos delegados a que se referem o artigo 25.º, n.º 4, o artigo 28.º, n.º 2, e o artigo 29.º, n.º 5, é conferido à Comissão por tempo indeterminado, a partir de [...].

3. A delegação de poderes prevista no artigo 25.º, n.º 4, no artigo 28.º, n.º 2, e no artigo 29.º, n.º 5, pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.

4. Antes de adotar um ato delegado, a Comissão deve consultar os peritos designados por cada Estado-Membro, em conformidade com os princípios estabelecidos no Acordo Interinstitucional sobre Legislar Melhor, de 13 de abril de 2016.

5. Assim que adotar um ato delegado, a Comissão deve notificá-lo simultaneamente ao Parlamento Europeu e ao Conselho.

6. Os atos delegados adotados nos termos do artigo 25.º, n.º 4, do artigo 28.º, n.º 2, e do artigo 29.º, n.º 5, só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de três meses a contar da notificação do ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. O referido prazo é prorrogável por três meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 39.º
Procedimento de comité

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

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

Artigo 40.º
Outros atos jurídicos da União que regem os direitos e as obrigações em matéria de acesso e utilização de dados

1. Não são afetadas as obrigações específicas relativas à disponibilização de dados entre empresas, entre empresas e consumidores e, a título excecional, entre empresas e organismos públicos, constantes dos atos jurídicos da União que entraram em vigor em [xx XXX xxx] ou antes dessa data, nem dos atos delegados ou de execução que se baseiam nos mesmos.

2. O presente regulamento não prejudica a legislação da União que especifique requisitos adicionais, em função das necessidades de um setor, de um espaço europeu comum de dados ou de um domínio de interesse público, em especial no que diz respeito:

   (a) Aos aspetos técnicos do acesso aos dados;

   (b) Aos limites dos direitos dos detentores de dados de acederem ou utilizarem determinados dados facultados pelos utilizadores;

   (c) Aos aspetos que vão além do acesso e da utilização dos dados.

Artigo 41.º
Avaliação e revisão

Até [*dois anos após a data de aplicação do presente regulamento*], a Comissão deve avaliar o presente regulamento e apresentar um relatório com as suas principais conclusões ao Parlamento Europeu e ao Conselho, bem como ao Comité Económico e Social Europeu. Essa avaliação deve incidir, em especial, nos seguintes aspetos:

a) Outras categorias ou tipos de dados a tornar acessíveis;

b) A exclusão de determinadas categorias de empresas da qualidade de beneficiárias nos termos do artigo 5.º;

c) Outras situações a considerar como necessidades excecionais para efeitos do artigo 15.º;

d) Alterações das práticas contratuais dos prestadores de serviços de tratamento de dados e se tal resulta no cumprimento suficiente do artigo 24.º;

e) Redução dos encargos impostos pelos prestadores de serviços de tratamento de dados devido ao processo de mudança, em consonância com a supressão gradual dos encargos decorrentes da mudança nos termos do artigo 25.º.

Artigo 42.º
Entrada em vigor e aplicação

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

É aplicável a partir de [12 meses após a data de entrada em vigor do presente regulamento].

Feito em Bruxelas, em

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