REGULAMENTO (UE) 2018/1807 DO PARLAMENTO EUROPEU E DO CONSELHO

de 14 de novembro de 2018

relativo a um regime para o livre fluxo de dados não pessoais na União Europeia

(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 ([1]),

Após consulta ao Comité das Regiões,

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

Considerando o seguinte:

(1) A digitalização da economia tem vindo a acelerar-se. O setor das tecnologias da informação e das comunicações deixou de ser um setor específico, passando a ser a base de todos os sistemas económicos e de todas as sociedades modernas e inovadoras. Os dados eletrónicos são um elemento central desses sistemas e podem gerar muito valor quando analisados ou combinados com serviços e produtos. Por outro lado, o rápido desenvolvimento da economia dos dados e das tecnologias emergentes, como a inteligência artificial, os produtos e serviços ligados à internet das coisas, os sistemas autónomos e a 5G, suscitam novos problemas jurídicos em torno das questões do acesso aos dados, da reutilização dos dados, da responsabilidade, da ética e da solidariedade. Deverá dar-se atenção à questão da imputação de responsabilidade, nomeadamente aplicando códigos de autorregulação e outras boas práticas, tendo em conta as recomendações, as decisões e as ações feitas, tomadas e realizadas sem interação humana ao longo de toda a cadeia de valor do tratamento de dados. Essas atividades poderão incluir também mecanismos adequados para determinar a imputação de responsabilidade, para transferir responsabilidades entre os serviços que colaboram entre si, para os seguros e para a auditoria.

(2) As cadeias de valor de dados assentam em diferentes atividades relacionadas com os dados: criação e recolha de dados; agregação e organização de dados; tratamento de dados; análise, comercialização e distribuição de dados; utilização e reutilização de dados. O funcionamento eficaz e eficiente do tratamento de dados constitui um alicerce fundamental em todas as cadeias de valor de dados. No entanto, esse funcionamento eficaz e eficiente e o desenvolvimento da economia dos dados na União são postos em causa, em particular, por dois tipos de obstáculos à mobilidade dos dados e ao mercado interno: os requisitos de localização de dados estabelecidos pelas autoridades dos Estados-Membros e as práticas de vinculação a um prestador no setor privado.

(3) A liberdade de estabelecimento e a livre prestação de serviços, consagradas no Tratado sobre o Funcionamento da União Europeia (TFUE), aplicam-se aos serviços de tratamento de dados. Todavia, a prestação destes serviços é dificultada ou, nalguns casos, impedida por determinadas disposições nacionais, regionais ou locais que exigem que os dados estejam localizados num território específico.

(4) Os referidos obstáculos à livre circulação de serviços de tratamento de dados, bem como ao direito de estabelecimento de prestadores de serviços, têm origem nas disposições legislativas nacionais que exigem que os dados estejam localizados numa zona geográfica ou território específico para efeitos de tratamento de dados. Outras regras ou práticas administrativas têm efeitos equivalentes, ao imporem requisitos específicos que tornam mais difícil o tratamento dos dados fora de uma zona geográfica ou território específico na União: por exemplo, a obrigação de utilizar meios tecnológicos certificados ou aprovados num determinado Estado-Membro. As incertezas jurídicas quanto ao alcance dos requisitos legítimos e ilegítimos em matéria de localização dos dados restringem ainda mais as opções disponíveis para os intervenientes no mercado e o setor público, no que se refere à localização do tratamento dos dados. O presente regulamento não limita de forma alguma a liberdade de as empresas poderem celebrar contratos em que especifiquem o sítio onde os dados devem ficar localizados. O presente regulamento destina-se meramente a salvaguardar essa liberdade, assegurando que uma localização acordada possa estar situada em qualquer ponto da União.

([1]) JO C 227 de 28.6.2018, p. 78.
([2]) Posição do Parlamento Europeu de 4 de outubro de 2018 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 6 de novembro de 2018.

(5) Ao mesmo tempo, a mobilidade de dados na União é afetada por restrições de natureza privada: aspetos jurídicos, contratuais e técnicos que prejudicam ou impedem os utilizadores de serviços de tratamento de dados de aplicarem a portabilidade dos seus dados de um prestador de serviços para outro ou novamente para os seus próprios sistemas informáticos, isto pelo menos até à cessação do seu contrato com um prestador de serviços.

(6) A combinação desses obstáculos levou à falta de concorrência entre os prestadores de serviços em nuvem na União, a diversos problemas de vinculação a um prestador e a uma grave carência ao nível da mobilidade de dados. Do mesmo modo, as políticas de localização de dados comprometeram a capacidade das empresas de investigação e desenvolvimento de facilitarem a colaboração entre empresas, universidades e outras organizações de investigação para estimularem a inovação.

(7) Por motivos de segurança jurídica e devido à necessidade de condições concorrenciais equitativas na União, a existência de um conjunto único de regras para todos os participantes no mercado é um elemento-chave para o funcionamento do mercado interno. A fim de eliminar os obstáculos ao comércio e as distorções da concorrência resultantes de divergências entre as legislações nacionais e evitar o provável surgimento de novos obstáculos ao comércio e de distorções significativas da concorrência, é necessário adotar regras uniformes aplicáveis em todos os Estados-Membros.

(8) O regime jurídico sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e sobre o respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas, nomeadamente o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([1]) e as Diretivas (UE) 2016/680 ([2]) e 2002/58/CE ([3]) do Parlamento Europeu e do Conselho, não são afetados pelo presente regulamento.

(9) A internet das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão, representam grandes fontes de dados não pessoais, por exemplo, em consequência da sua utilização em processos automatizados de produção industrial. Exemplos concretos de dados não pessoais incluem conjuntos de dados agregados e anonimizados utilizados para a análise de grandes volumes de dados, os dados relativos à agricultura de precisão que podem ajudar a controlar e a otimizar a utilização de pesticidas e de água ou ainda dados sobre as necessidades de manutenção de máquinas industriais. Se os progressos tecnológicos permitirem transformar dados anonimizados em dados pessoais, esses dados devem ser tratados como dados pessoais, e o Regulamento (UE) 2016/679 deve ser aplicado em conformidade.

(10) Nos termos do Regulamento (UE) 2016/679, os Estados-Membros não podem restringir nem proibir a livre circulação de dados pessoais no interior da União por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais. O presente regulamento estabelece o mesmo princípio de livre circulação no interior da União relativamente aos dados não pessoais, com exceção dos casos em que se justifique uma restrição ou uma proibição por motivos de segurança pública. O Regulamento (UE) 2016/679 e o presente regulamento estabelecem um conjunto coerente de regras que preveem a livre circulação de diferentes tipos de dados. Por outro lado, o presente regulamento não impõe a obrigação de armazenar separadamente os diferentes tipos de dados.

(11) A fim de criar um regime para o livre fluxo de dados não pessoais na União, e as bases para desenvolver a economia dos dados e para reforçar a competitividade da indústria da União, é necessário estabelecer um regime jurídico claro, abrangente e previsível para o tratamento dos dados, que não sejam dados pessoais, no mercado interno. Uma abordagem baseada em princípios, que permita a cooperação entre os Estados-Membros e a autorregulação, deverá assegurar que esse regime seja suficientemente flexível para ter em conta a evolução das necessidades dos utilizadores, dos prestadores de serviços e das autoridades nacionais na União. A fim de evitar o risco de sobreposições com os mecanismos em vigor, evitando assim uma maior sobrecarga tanto para os Estados-Membros como para as empresas, não deverão definir-se normas técnicas pormenorizadas.

(12) O presente regulamento não deverá afetar o tratamento de dados, na medida em que esse tratamento seja realizado como parte de uma atividade fora do âmbito de aplicação do direito da União. Deverá ter-se presente, em especial, que, nos termos do artigo 4.º do Tratado da União Europeia (TUE), a segurança nacional é da exclusiva responsabilidade de cada Estado-Membro.

([1]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

([2]) Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, p. 89).

([3]) Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

(13) O livre fluxo de dados na União desempenhará um papel fundamental para se conseguir um crescimento e uma inovação assentes em dados. Tal como as empresas e os consumidores, as autoridades públicas e os organismos regidos pelo direito público dos Estados-Membros podem beneficiar de uma maior liberdade de escolha em relação aos prestadores de serviços de dados, a preços mais competitivos e a uma prestação de serviços aos cidadãos mais eficaz. Tendo em conta a grande quantidade de dados tratados pelas autoridades públicas e pelos organismos regidos pelo direito público, é da maior importância que estes deem o exemplo aderindo a serviços de tratamento de dados e abstendo-se de impor restrições à localização de dados quando recorrem a serviços de tratamento de dados. Por conseguinte, as autoridades públicas e os organismos regidos pelo direito público deverão ser abrangidos pelo presente regulamento. Neste sentido, o princípio do livre fluxo de dados não pessoais previsto pelo presente regulamento deverá aplicar-se também a práticas administrativas gerais e coerentes e a outros requisitos de localização de dados no domínio dos contratos públicos, sem prejuízo do disposto na Diretiva 2014/24/UE do Parlamento Europeu e do Conselho ([1]).

(14) À semelhança da Diretiva 2014/24/UE, o presente regulamento é aplicável sem prejuízo das disposições legislativas, regulamentares e administrativas relativas à organização interna dos Estados-Membros e que atribuem às autoridades públicas e aos organismos regidos pelo direito público poderes e responsabilidades para o tratamento de dados, sem remuneração contratual do setor privado, nem das disposições legislativas, regulamentares e administrativas dos Estados-Membros que preveem a aplicação desses poderes e dessas responsabilidades. Embora as autoridades públicas e os organismos regidos pelo direito público sejam encorajados a ter em conta os benefícios económicos e os outros benefícios da externalização para prestadores de serviços externos, essas autoridades e esses organismos podem ter razões legítimas para escolher prestar eles próprios os serviços ou para os internalizar. Assim, não há nada no presente regulamento que obrigue os Estados-Membros a subcontratar ou a externalizar a prestação de serviços que os próprios pretendem prestar ou organizar por meios que não contratos públicos.

(15) O presente regulamento deverá aplicar-se às pessoas singulares ou coletivas que prestam serviços de tratamento de dados a utilizadores residentes ou estabelecidos na União, incluindo as pessoas que prestam serviços de tratamento de dados na União sem estarem estabelecidas na União. Por conseguinte, o presente regulamento não deverá aplicar-se a serviços de tratamento de dados executados fora da União, nem aos requisitos de localização de dados relativos a esses dados.

(16) O presente regulamento não estabelece regras relativas à determinação da lei aplicável em matéria comercial e, por conseguinte, é aplicável sem prejuízo do Regulamento (CE) n.º 593/2008 do Parlamento Europeu e do Conselho ([2]). Em especial, na medida em que a lei aplicável a um contrato não tenha sido escolhida nos termos desse regulamento, os contratos de prestação de serviços são, em princípio, regidos pela lei do país da residência habitual do prestador de serviços.

(17) O presente regulamento deverá aplicar-se ao tratamento de dados no sentido mais lato, englobando a utilização de todos os tipos de sistemas informáticos, tanto localizados nas instalações do utilizador como externalizados a um prestador de serviços. O presente regulamento deverá abranger o tratamento de dados em diferentes níveis de intensidade, desde o armazenamento (infraestrutura como serviço, ou IaaS – do inglês *Infrastructure-as-a-Service*) até ao tratamento por meio de plataformas (plataforma como serviço, ou PaaS – *Platform-as-a-Service*) ou aplicações (software como serviço, ou SaaS – *Software-as-a-Service*).

(18) Os requisitos de localização dos dados representam um obstáculo manifesto à livre prestação de serviços de tratamento de dados em toda a União e ao mercado interno. Como tal, deverão ser excluídos, salvo quando se justifiquem por razões de segurança pública, tal como definida no direito da União, nomeadamente na aceção do artigo 52.º do TFUE, e deverão respeitar o princípio da proporcionalidade consagrado no artigo 5.º do TUE. A fim de tornar efetivo o princípio do livre fluxo de dados não pessoais além-fronteiras, de eliminar atempadamente os requisitos de localização de dados e de permitir, por motivos de natureza operacional, o tratamento de dados em múltiplas localizações em toda a União, e tendo em conta que o presente regulamento prevê medidas destinadas a assegurar a disponibilidade dos dados para fins de controlo regulamentar, os Estados-Membros só deverão poder invocar a segurança pública como justificação para requisitos de localização de dados.

(19) Na aceção do artigo 52.º do TFUE, e tal como interpretado pelo Tribunal de Justiça, o conceito de «segurança pública» abrange tanto a segurança interna como a segurança externa de um Estado-Membro, bem como questões atinentes à proteção pública, nomeadamente a fim de facilitar a investigação, a deteção e a repressão de infrações penais. O conceito de «segurança pública» pressupõe a existência de uma ameaça real e suficientemente grave que afete um interesse essencial da sociedade, como, por exemplo, uma ameaça ao funcionamento das instituições e serviços públicos essenciais e à sobrevivência da população, assim como o risco de uma perturbação grave das relações externas ou da coexistência pacífica das nações, ou um risco para os interesses militares. Em conformidade com o princípio da proporcionalidade, os requisitos de localização de dados que se justifiquem por razões de segurança pública deverão ser adequados à realização do objetivo pretendido, e não deverão exceder o necessário para alcançar esse objetivo.

([1]) Diretiva 2014/24/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à decisão europeia de investigação em matéria penal (JO L 94 de 28.3.2014, p. 65).

([2]) Regulamento (CE) n.º 593/2008 do Parlamento Europeu e do Conselho, de 17 de junho de 2008, sobre a lei aplicável às obrigações contratuais (Roma I) (JO L 177 de 4.7.2008, p. 6).

(20) A fim de garantir a aplicação efetiva do princípio do livre fluxo de dados não pessoais além-fronteiras e de prevenir o surgimento de novos obstáculos ao bom funcionamento do mercado interno, os Estados-Membros deverão comunicar imediatamente à Comissão qualquer projeto de ato que introduza um novo requisito de localização dos dados ou que modifique um requisito existente de localização dos dados. Esses projetos de ato deverão ser apresentados e avaliados nos termos da Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho ([1]).

(21) Além disso, a fim de suprimir os obstáculos que possam existir atualmente, os Estados-Membros deverão proceder a um exame, durante um período de transição de 24 meses a contar da data de aplicação do presente regulamento, das disposições legislativas, regulamentares ou administrativas de natureza geral que estabelecem requisitos de localização dos dados, e comunicar à Comissão os requisitos de localização dos dados que considerem em conformidade com o presente regulamento, juntamente com uma justificação. Isto deverá permitir à Comissão examinar a conformidade dos requisitos remanescentes de localização dos dados. A Comissão deverá poder fazer comentários, se for caso disso, dirigidos ao Estado-Membro em questão. Esses comentários poderão incluir uma recomendação para alterar ou revogar o requisito de localização dos dados.

(22) As obrigações estabelecidas no presente regulamento de comunicar à Comissão os requisitos existentes de localização de dados e os projetos de atos deverão aplicar-se aos requisitos regulamentares de localização de dados e aos projetos de atos de caráter geral, mas não às decisões que tenham por destinatário uma pessoa singular ou coletiva determinada.

(23) A fim de assegurar a transparência dos requisitos de localização de dados impostos em disposições legislativas, regulamentares ou administrativas de caráter geral nos Estados-Membros às pessoas singulares e coletivas, designadamente prestadores de serviços e utilizadores de serviços de tratamento de dados, os Estados-Membros deverão publicar e atualizar periodicamente as informações sobre esses requisitos num ponto de informação nacional em linha único. Em alternativa, os Estados-Membros deverão fornecer informação atualizada sobre esses requisitos a um ponto de informação central criado ao abrigo de outro ato da União. A fim de prestar informações adequadas às pessoas singulares e coletivas sobre os requisitos de localização de dados em toda a União, os Estados-Membros deverão notificar à Comissão os endereços dos referidos pontos de informação únicos. A Comissão deverá publicar essas informações no seu próprio sítio Web, juntamente com uma lista consolidada dos requisitos de localização de dados em vigor nos Estados-Membros, incluindo informações sintetizadas sobre esses requisitos.

(24) Os requisitos de localização de dados resultam frequentemente de uma falta de confiança no tratamento transfronteiriço de dados, tendo origem numa presunção de indisponibilidade dos dados para os fins das autoridades competentes dos Estados-Membros, designadamente a realização de inspeções e auditorias no âmbito de controlos regulamentares ou de supervisão. A nulidade das condições contratuais que proíbem o acesso legal aos dados pelas autoridades competentes para o desempenho das suas obrigações oficiais não é suficiente para colmatar essa falta de confiança. Por conseguinte, o presente regulamento deverá indicar expressamente que não afeta os poderes das autoridades competentes de requererem ou de obterem acesso a dados nos termos do direito da União ou do direito nacional, e que o acesso aos dados por parte das autoridades competentes não pode ser recusado a pretexto de os dados serem tratados noutro Estado-Membro. As autoridades competentes podem impor requisitos funcionais para apoiar o acesso a dados, como, por exemplo, exigir que a descrição do sistema seja mantida no Estado-Membro em questão.

(25) As pessoas singulares ou coletivas sujeitas à obrigação de fornecer dados às autoridades competentes podem cumprir essa obrigação concedendo e garantindo às autoridades competentes um acesso efetivo e oportuno aos dados por via eletrónica, independentemente do Estado-Membro em cujo território os dados são tratados. Esse acesso pode ser assegurado mediante cláusulas concretas nos contratos entre, por um lado, as pessoas singulares ou coletivas sujeitas à obrigação de conceder acesso e, por outro, os prestadores de serviços.

(26) Se uma pessoa singular ou coletiva obrigada a fornecer dados não cumprir essa obrigação, a autoridade competente deverá poder pedir assistência às autoridades competentes de outros Estados-Membros. Nestes casos, as autoridades competentes deverão recorrer a instrumentos de cooperação específicos previstos no direito da União ou em convenções internacionais, consoante o objeto do caso em apreço, tais como, nos domínios da cooperação policial, da justiça penal ou civil ou em questões administrativas, respetivamente, a Decisão-Quadro

([1]) Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação (JO L 241 de 17.9.2015, p. 1).

2006/960/JAI do Conselho ([1]), a Diretiva 2014/41/UE do Parlamento Europeu e do Conselho ([2]), a Convenção do Conselho da Europa sobre o Cibercrime ([3]), o Regulamento (CE) n.º 1206/2001 do Conselho ([4]), a Diretiva 2006/112/CE do Conselho ([5]) e o Regulamento (UE) n.º 904/2010 do Conselho ([6]). Na falta de mecanismos de cooperação específicos, as autoridades competentes deverão colaborar entre si para facultar acesso aos dados solicitados, por intermédio de pontos de contacto únicos designados.

(27) Caso um pedido de assistência implique a obtenção do acesso da autoridade requerida às instalações de uma pessoa singular ou coletiva, incluindo equipamentos e meios de tratamento de dados, esse acesso deverá estar em conformidade com o direito da União ou com o direito processual nacional, designadamente a obrigação de obter uma autorização judicial prévia.

(28) O presente regulamento não deverá permitir que os utilizadores tentem subtrair-se à aplicação do direito nacional. Por conseguinte, o presente regulamento deverá prever disposições que permitam a aplicação pelos Estados-Membros de sanções efetivas, proporcionadas e dissuasivas aos utilizadores que impeçam as autoridades competentes de aceder aos seus dados necessários para o cumprimento das obrigações oficiais das autoridades competentes ao abrigo do direito da União e do direito nacional. Em casos urgentes, caso um utilizador abuse do seu direito, os Estados-Membros deverão poder aplicar medidas provisórias estritamente proporcionadas. Qualquer medida provisória que exija a relocalização dos dados por um período superior a 180 dias a contar da relocalização contrariaria o princípio da livre circulação de dados durante um período significativo, pelo que deverá ser comunicada à Comissão para exame da sua compatibilidade com o direito da União.

(29) A capacidade de aplicar a portabilidade de dados sem entraves é um fator essencial para facilitar a escolha do utilizador e a concorrência efetiva nos mercados dos serviços de tratamento de dados. As dificuldades, reais ou sentidas, em aplicar a portabilidade transfronteiriça de dados também afeta a confiança dos utilizadores profissionais na aceitação de ofertas transfronteiriças e, portanto, a sua confiança no mercado interno. Embora os consumidores individuais beneficiem do direito da União em vigor, a possibilidade de mudar de prestador de serviços não é facilitada aos utilizadores no exercício das suas atividades comerciais ou profissionais. A existência de requisitos técnicos coerentes em toda a União, de uma harmonização técnica, de reconhecimento mútuo ou de harmonização voluntária, contribui também para o desenvolvimento de um mercado interno competitivo de serviços de tratamento de dados.

(30) A fim de tirar o máximo partido do ambiente concorrencial, os utilizadores profissionais deverão ter a possibilidade de efetuar escolhas fundamentadas e de comparar facilmente as componentes individuais dos vários serviços de tratamento de dados oferecidos no mercado interno, inclusive no que se refere às condições contratuais da portabilidade dos dados na cessação de um contrato. Para corresponder ao potencial de inovação do mercado e ter em conta a experiência e os conhecimentos dos prestadores de serviços e dos utilizadores profissionais de serviços de tratamento de dados, os requisitos pormenorizados de informação e funcionamento relativos à portabilidade dos dados deverão ser definidos pelos intervenientes no mercado através de autorregulação, com o apoio, a mediação e o acompanhamento da Comissão, sob a forma de códigos de conduta da União que poderão incluir modelos de cláusulas contratuais.

(31) Para que possa ser eficaz e para facilitar a mudança entre prestadores de serviços e a portabilidade dos dados, os códigos de conduta supracitados deverão ser abrangentes e deverão incluir, pelo menos, alguns aspetos fundamentais importantes durante o processo de portabilidade dos dados, tal como os processos usados para as cópias de segurança de dados e a localização das mesmas; os formatos e os suportes de dados disponíveis; a configuração informática e a largura mínima de banda da rede; o tempo mínimo necessário antes de iniciar o processo de portabilidade e o período durante o qual os dados continuarão disponíveis para a portabilidade dos dados; assim como as garantias de acesso aos dados em caso de falência do prestador de serviços. Os códigos de conduta deverão, por outro lado, deixar claro que a vinculação a um prestador não é uma prática comercial aceitável, deverão prever tecnologias que reforcem a confiança e deverão ser atualizados com regularidade para poderem acompanhar a evolução tecnológica. A Comissão deverá garantir que todas as partes interessadas pertinentes, incluindo as associações de pequenas e médias empresas (PME) e as empresas em fase de arranque, os utilizadores e os prestadores de serviços em nuvem, sejam consultadas ao longo do processo. A Comissão deverá avaliar o desenvolvimento e a aplicação efetiva desses códigos de conduta.

([1]) Decisão-Quadro 2006/960/JAI do Conselho, de 18 de dezembro de 2006, relativa à simplificação do intercâmbio de dados e informações entre as autoridades de aplicação da lei dos Estados-Membros da União Europeia (JO L 386 de 29.12.2006, p. 89).

([2]) Diretiva 2014/41/UE do Parlamento Europeu e do Conselho, de 3 de abril de 2014, relativa à decisão europeia de investigação em matéria penal (JO L 130 de 1.5.2014, p. 1).

([3]) Convenção do Conselho da Europa sobre o Cibercrime, STCE n.º 185.

([4]) Regulamento (CE) n.º 1206/2001 do Conselho, de 28 de maio de 2001, relativo à cooperação entre os tribunais dos Estados-Membros no domínio da obtenção de provas em matéria civil ou comercial (JO L 174 de 27.6.2001, p. 1).

([5]) Diretiva 2006/112/CE do Conselho, de 28 de novembro de 2006, relativa ao sistema comum do imposto sobre o valor acrescentado (JO L 347 de 11.12.2006, p. 1).

([6]) Regulamento (UE) n.º 904/2010 do Conselho, de 7 de outubro de 2010, relativo à cooperação administrativa e à luta contra a fraude no domínio do imposto sobre o valor acrescentado (JO L 268 de 12.10.2010, p. 1).

(32) Caso uma autoridade competente de um Estado-Membro peça a assistência de outro Estado-Membro para obter acesso a dados nos termos do presente regulamento, deverá apresentar ao ponto de contacto único designado do segundo Estado-Membro, através de um ponto de contacto único designado, um pedido devidamente fundamentado que inclua uma exposição escrita dos motivos e das bases jurídicas para solicitar acesso aos dados. O ponto de contacto único designado pelo Estado-Membro ao qual é pedida assistência deverá viabilizar a transmissão entre as autoridades, identificando e transmitindo o pedido à autoridade competente do Estado-Membro requerido. A fim de assegurar uma cooperação eficaz, a autoridade à qual é transmitido um pedido deverá, sem demora indevida, prestar assistência em resposta a um pedido ou fornecer informações sobre as dificuldades para satisfazer esse pedido, ou sobre os motivos que a levaram a indeferi-lo.

(33) A promoção da confiança na segurança do tratamento de dados a nível transfronteiriço deverá reduzir a tendência dos intervenientes no mercado e do setor público para utilizarem a localização dos dados como fator de salvaguarda da segurança dos dados. Deverá também melhorar a segurança jurídica das empresas em relação aos requisitos de segurança aplicáveis, quando da externalização das suas atividades de tratamento de dados, inclusive para prestadores de serviços localizados noutros Estados-Membros.

(34) Todos os requisitos de segurança relativos ao tratamento de dados que sejam aplicados de modo justificado e proporcionado, com base no direito da União ou no direito nacional, em conformidade com o direito da União, no Estado-Membro de residência ou de estabelecimento das pessoas singulares ou coletivas às quais os dados dizem respeito deverão continuar a aplicar-se ao tratamento desses dados noutro Estado-Membro. Essas pessoas singulares ou coletivas deverão poder satisfazer os requisitos em causa por si próprias ou mediante cláusulas contratuais nos contratos com os prestadores.

(35) Os requisitos de segurança estabelecidos ao nível nacional deverão ser necessários e proporcionados aos riscos para a segurança do tratamento de dados no domínio abrangido pelo direito nacional no âmbito do qual os requisitos são definidos.

(36) A Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho ([1]) prevê medidas jurídicas para reforçar o nível geral de cibersegurança na União. Os serviços de tratamento de dados constituem uma das categorias de serviços digitais abrangidos por esta diretiva. Nos termos dessa diretiva, os Estados-Membros têm de assegurar que os prestadores de serviços digitais identifiquem os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam e tomem medidas técnicas e organizativas adequadas e proporcionadas para gerir esses riscos. Estas medidas deverão garantir um nível de segurança adequado ao risco em causa, e ter em conta a segurança dos sistemas e das instalações, o tratamento dos incidentes, a gestão da continuidade das atividades, o acompanhamento, a auditoria e os testes realizados, bem como a conformidade com as normas internacionais. A Comissão deve especificar estes elementos de forma mais pormenorizada através de atos de execução ao abrigo dessa diretiva.

(37) A Comissão deverá apresentar um relatório sobre a execução do presente regulamento, nomeadamente para decidir da eventual necessidade de alterações à luz da evolução tecnológica ou do mercado. Esse relatório deverá avaliar, nomeadamente, o presente regulamento, em especial a sua aplicação aos conjuntos de dados compostos por dados pessoais e não pessoais, e a aplicação da exceção de segurança pública. Antes de o presente regulamento começar a aplicar-se, a Comissão deverá também publicar orientações informativas, nomeadamente sobre a forma como lidar com conjuntos de dados compostos por dados pessoais e não pessoais, para que as empresas, incluindo as PME, consigam ter um melhor entendimento da interação entre o presente regulamento e o Regulamento (UE) 2016/679, e para assegurar que ambos os regulamentos sejam cumpridos.

(38) O presente regulamento respeita os direitos fundamentais e observa os princípios reconhecidos, designadamente, na Carta dos Direitos Fundamentais da União Europeia, e deverá ser interpretado e aplicado em conformidade com esses direitos e princípios, incluindo os direitos à proteção dos dados pessoais, a liberdade de expressão e de informação e a liberdade de empresa.

(39) Atendendo a que o objetivo do presente regulamento, a saber, assegurar o livre fluxo de dados que não sejam dados pessoais na União, não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, devido à sua dimensão e aos seus efeitos, ser mais bem alcançado ao nível da União, a União pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do TUE. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para alcançar esse objetivo,

([1]) Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (JO L 194 de 19.7.2016, p. 1).

ADOTARAM O PRESENTE REGULAMENTO:

Artigo 1.º

Objeto

O presente regulamento destina-se a assegurar o livre fluxo de dados que não sejam dados pessoais na União, estabelecendo as regras relativas aos requisitos de localização dos dados, à disponibilidade dos dados para as autoridades competentes e à portabilidade dos dados para os utilizadores profissionais.

Artigo 2.º

Âmbito de aplicação

1. O presente regulamento aplica-se ao tratamento de dados eletrónicos que não sejam dados pessoais na União:

a) Prestado como um serviço a utilizadores residentes ou estabelecidos na União, independentemente de o prestador de serviços estar ou não estabelecido na União; ou

b) Realizado por uma pessoa singular ou coletiva com residência ou estabelecimento na União para as suas necessidades próprias.

2. No caso de um conjunto de dados compostos por dados pessoais e não pessoais, o presente regulamento aplica-se aos dados não pessoais do conjunto de dados. Caso os dados pessoais e não pessoais de um conjunto de dados estejam indissociavelmente ligados, o presente regulamento não prejudica a aplicação do Regulamento (UE) 2016/679.

3. O presente regulamento não se aplica a atividades não abrangidas pelo âmbito de aplicação do direito da União.

O presente regulamento é aplicável sem prejuízo das disposições legislativas, regulamentares e administrativas relativas à organização interna dos Estados-Membros e que atribuem às autoridades públicas e aos organismos regidos pelo direito público definidos no artigo 2.º, n.º 1, ponto 4, da Diretiva 2014/24/UE poderes e responsabilidades para o tratamento de dados sem remuneração contratual do setor privado, nem das disposições legislativas, regulamentares e administrativas dos Estados-Membros que preveem a aplicação desses poderes e dessas responsabilidades.

Artigo 3.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Dados», os dados que não sejam dados pessoais na aceção do artigo 4.º, ponto 1, do Regulamento (UE) 2016/679;

2) «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;

3) «Projeto de ato», um texto redigido com o objetivo de vir a ser adotado como uma disposição legislativa, regulamentar ou administrativa de caráter geral, na fase de elaboração que permite ainda a introdução de alterações substanciais;

4) «Prestador de serviços», uma pessoa singular ou coletiva que presta serviços de tratamento de dados;

5) «Requisito de localização de dados», uma obrigação, proibição, condição, limitação ou outra exigência, prevista nas disposições legislativas, regulamentares ou administrativas de um Estado-Membro, ou resultante de práticas administrativas gerais e coerentes de um Estado-Membro e de organismos regidos pelo direito público, nomeadamente no domínio dos contratos públicos, sem prejuízo do disposto na Diretiva 2014/24/UE, que exige o tratamento de dados no território de um Estado-Membro específico ou restringe o tratamento de dados em qualquer outro Estado-Membro;

6) «Autoridade competente», uma autoridade de um Estado-Membro, ou qualquer outra entidade autorizada pelo direito nacional a desempenhar uma função pública ou a exercer um poder público, habilitada a obter acesso aos dados tratados por pessoas singulares ou coletivas para efeitos do exercício das suas funções oficiais, nos termos do direito da União ou do direito nacional;

7) «Utilizador», uma pessoa singular ou coletiva, incluindo uma autoridade pública ou um organismo regido pelo direito público, que utiliza ou solicita um serviço de tratamento de dados;

8) «Utilizador profissional», uma pessoa singular ou coletiva, incluindo uma autoridade pública ou um organismo regido pelo direito público, que utiliza ou solicita um serviço de tratamento de dados para fins relacionados com as suas atividades comerciais, empresariais ou artesanais, ou com as suas tarefas profissionais.

Artigo 4.º

Livre circulação de dados na União

1. Os requisitos de localização de dados são proibidos, salvo quando justificados por motivos de segurança pública e no respeito do princípio da proporcionalidade.

O primeiro parágrafo do presente número é aplicável sem prejuízo do n.º 3 e dos requisitos de localização de dados estabelecidos com base no direito em vigor da União.

2. Os Estados-Membros comunicam imediatamente à Comissão os projetos de atos que introduzam um novo requisito de localização de dados ou que modifiquem um requisito existente de localização de dados, pelos procedimentos previstos nos artigos 5.º, 6.º e 7.º da Diretiva (UE) 2015/1535.

3. Até 30 de maio de 2021, os Estados-Membros asseguram a revogação de todos os requisitos vigentes de localização de dados, estabelecidos em disposições legislativas, regulamentares ou administrativas de caráter geral, que não cumpram o n.º 1 do presente artigo.

Até 30 de maio de 2021, se um Estado-Membro considerar que uma medida vigente que inclua um requisito de localização de dados cumpre o n.º 1 do presente artigo e pode, por conseguinte, permanecer em vigor, comunica essa medida à Comissão, juntamente com uma justificação para manter o requisito em vigor. Sem prejuízo do artigo 258.º do TFUE, a Comissão examina, no prazo de seis meses a contar da data de receção dessa comunicação, a conformidade dessa medida com o n.º 1 do presente artigo e, se for caso disso, faz comentários dirigidos ao Estado-Membro em causa, incluindo, se necessário, uma recomendação de alteração ou de revogação da medida.

4. Os Estados-Membros disponibilizam publicamente, através de um ponto de informação nacional em linha único, que devem manter atualizado, informações pormenorizadas sobre qualquer requisito de localização de dados aplicável no seu território, estabelecido em disposições legislativas, regulamentares ou administrativas de caráter geral, ou fornecem informações atualizadas sobre esse requisito de localização de dados a um ponto de informação central estabelecido ao abrigo de outro ato da União.

5. Os Estados-Membros comunicam à Comissão o endereço do respetivo ponto de informação único a que se refere o n.º 4. A Comissão publica no seu sítio Web hiperligações para os referidos pontos de informação, juntamente com uma lista consolidada e periodicamente atualizada de todos os requisitos de localização de dados referidos no n.º 4, incluindo informações sintéticas sobre esses requisitos.

Artigo 5.º

Disponibilidade dos dados para as autoridades competentes

1. O presente regulamento não afeta os poderes das autoridades competentes de requererem ou obterem acesso a dados para o desempenho das suas obrigações oficiais, nos termos do direito da União ou do direito nacional. O acesso das autoridades competentes aos dados não pode ser recusado a pretexto de que os dados são tratados noutro Estado-Membro.

2. Caso uma autoridade competente, após ter pedido acesso aos dados de um utilizador, não obtenha acesso a esses dados, e se não existir um mecanismo específico de cooperação ao abrigo do direito da União ou de convenções internacionais relativamente ao intercâmbio de dados entre autoridades competentes de diferentes Estados-Membros, pode pedir a assistência de uma autoridade competente de outro Estado-Membro, pelo procedimento estabelecido no artigo 7.º.

3. Caso um pedido de assistência implique a obtenção do acesso da autoridade requerida às instalações de uma pessoa singular ou coletiva, incluindo equipamentos e meios de tratamento de dados, esse acesso deve estar em conformidade com o direito da União ou com o direito processual nacional.

4. Os Estados-Membros podem impor sanções efetivas, proporcionadas e dissuasivas em caso de incumprimento da obrigação de fornecer dados, nos termos do direito da União e do direito nacional.

Em caso de abuso de direito por um utilizador, um Estado-Membro pode aplicar medidas provisórias estritamente proporcionadas a esse utilizador, sempre que tal se justifique pela urgência em aceder aos dados, tendo em consideração os interesses das partes em causa. Caso uma medida provisória imponha a relocalização dos dados por um período superior a 180 dias a contar da relocalização, deve ser comunicada à Comissão dentro desse prazo de 180 dias. A Comissão examina no mais curto prazo possível a medida e a sua compatibilidade com o direito da União e, se for caso disso, toma as medidas necessárias. A Comissão procede ao intercâmbio de informações com os pontos de contacto únicos dos Estados-Membros referidos no artigo 7.º sobre a experiência adquirida a esse respeito.

Artigo 6.º

Portabilidade dos dados

1. A Comissão deve incentivar e viabilizar a elaboração de códigos de conduta de autorregulação ao nível da União («códigos de conduta»), a fim de contribuir para uma economia dos dados competitiva assente nos princípios da transparência e da interoperabilidade, e tendo devidamente em conta as normas abertas, incluindo, nomeadamente, os seguintes aspetos:

a) Melhores práticas para facilitar a mudança de prestador de serviços e a portabilidade dos dados num formato estruturado, comum e de leitura automática, incluindo formatos normalizados abertos quando requerido ou solicitado pelo prestador de serviços que recebe os dados;

b) Requisitos mínimos de informação para garantir que os utilizadores profissionais recebam, antes de assinarem um contrato de tratamento de dados, informações suficientemente pormenorizadas, claras e transparentes relativamente aos processos, requisitos técnicos, prazos e encargos aplicáveis no caso de um utilizador profissional pretender mudar para outro prestador de serviços ou aplicar a portabilidade dos dados para os seus próprios sistemas informáticos;

c) Abordagens relativas a sistemas de certificação que facilitem a comparação de produtos e serviços de tratamento de dados para os utilizadores profissionais, tendo em conta as normas nacionais ou internacionais estabelecidas, para facilitar a comparabilidade desses produtos e serviços. Essas abordagens podem dizer respeito, nomeadamente, à gestão da qualidade, à gestão da segurança da informação, à gestão da continuidade das atividades e à gestão ambiental;

d) Roteiros de comunicação com uma abordagem multidisciplinar visando uma sensibilização das partes interessadas para os códigos de conduta.

2. A Comissão assegura que os códigos de conduta sejam elaborados em estreita cooperação com todas as partes interessadas relevantes, incluindo as associações de PME e as empresas em fase de arranque, os utilizadores e os prestadores de serviços em nuvem.

3. A Comissão deve incentivar os prestadores de serviços a terminarem a elaboração dos códigos de conduta até 29 de novembro de 2019 e a aplicarem-nos efetivamente até 29 de maio de 2020.

Artigo 7.º

Procedimento para a cooperação entre as autoridades

1. Cada Estado-Membro deve designar um ponto de contacto único que servirá de elo de ligação com os pontos de contacto únicos dos demais Estados-Membros e com a Comissão no atinente à aplicação do presente regulamento. Os Estados-Membros devem notificar à Comissão os pontos de contacto únicos designados e quaisquer posteriores alterações dos mesmos.

2. Caso uma autoridade competente num Estado-Membro peça a assistência de outro Estado-Membro, nos termos do artigo 5.º, n.º 2, a fim de obter acesso a dados, deve apresentar um pedido devidamente fundamentado ao ponto de contacto único designado do segundo Estado-Membro. O pedido deve incluir uma exposição escrita dos motivos e das bases jurídicas para solicitar acesso aos dados.

3. O ponto de contacto único deve identificar a autoridade competente relevante do respetivo Estado-Membro e transmitir o pedido recebido nos termos do n.º 2 a essa autoridade competente.

4. A autoridade competente relevante à qual é feito o pedido deve fornecer, sem demora indevida e num prazo proporcionado em relação à urgência do pedido, uma resposta comunicando os dados solicitados ou informando a autoridade competente requerente que considera que as condições para requerer a assistência ao abrigo do presente regulamento não foram cumpridas.

5. As informações partilhadas no contexto de um pedido e da prestação de assistência nos termos do artigo 5.º, n.º 2, devem destinar-se exclusivamente aos fins para os quais são solicitadas.

6. Os pontos de contacto únicos devem fornecer aos utilizadores informações gerais sobre o presente regulamento, nomeadamente sobre os códigos de conduta.

Artigo 8.º

Avaliação e revisão

1. Até 29 de novembro de 2022, a Comissão apresenta um relatório ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu em que avalia a execução do presente regulamento, nomeadamente no que se refere:

a) À aplicação do presente regulamento, em especial a sua aplicação aos conjuntos de dados compostos por dados pessoais e não pessoais, à luz das evoluções tecnológicas e do mercado, que possam alargar as possibilidades de tornar os dados não anónimos;

b) À execução do artigo 4.º, n.º 1, pelos Estados-Membros, nomeadamente a exceção de segurança pública; e

c) À elaboração e à aplicação efetiva dos códigos de conduta e à disponibilização efetiva de informações pelos prestadores de serviços.

2. Os Estados-Membros fornecem à Comissão as informações necessárias para a elaboração do relatório referido no n.º 1.

3. Até 29 de maio de 2019, a Comissão publica orientações sobre a interação do presente regulamento com o Regulamento (UE) 2016/679, nomeadamente no que se refere aos conjuntos compostos por dados pessoais e não pessoais.

Artigo 9.º

Disposições finais

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

O presente regulamento é aplicável seis meses após a sua publicação.

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

Feito em Estrasburgo, em 14 de novembro de 2018.

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*A Presidente*
A. TAJANI	K. EDTSTADLER