Conselho da
União Europeia

**Bruxelas, 8 de abril de 2016**
**(OR. en)**

**5419/1/16**
**REV 1 ADD 1**

**Dossiê interinstitucional:**
**2012/0011 (COD)**

**DATAPROTECT 2**
**JAI 38**
**MI 25**
**DIGIT 21**
**DAPIX 9**
**FREMP 4**
**CODEC 52**
**PARLNAT 83**

**NOTA JUSTIFICATIVA DO CONSELHO**

| | |
|---|---|
| Assunto: | Posição do Conselho em primeira leitura com vista à adoção do REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)<br>– Nota justificativa do Conselho<br>– Adotada pelo Conselho em 8 de abril de 2016 |

## I. INTRODUÇÃO

Em 25 de janeiro de 2012, Comissão propôs uma reforma global para a proteção de dados, que compreendia:

- a proposta de Regulamento Geral sobre a Proteção de Dados referida em epígrafe, que visa substituir a Diretiva Proteção de Dados de 1995 (antigo primeiro pilar);
- uma proposta de diretiva relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados, que visa substituir a Decisão-Quadro Proteção de Dados de 2008 (antigo terceiro pilar).

Em 12 de março de 2014, o Parlamento Europeu adotou a sua posição em primeira leitura em relação à proposta de Regulamento Geral sobre a Proteção de Dados (7427/14).

Em 15 de junho de 2015, o Conselho chegou a acordo sobre uma orientação geral, conferindo desse modo à Presidência um mandato de negociação para encetar os trílogos com o Parlamento Europeu (9565/15).

O Parlamento Europeu e o Conselho a nível, respetivamente, da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos e do Comité de Representantes Permanentes, confirmaram o acordo sobre o texto de compromisso resultante das negociações nos trílogos de 17 e 18 de dezembro de 2015, respetivamente.

Na sua reunião de 12 de fevereiro de 2016, o Conselho alcançou um acordo político sobre o projeto de Regulamento (5455/15). Em 8 de abril de 2016, o Conselho adotou a sua posição em primeira leitura, que está plenamente em consonância com o texto de compromisso sobre o regulamento que foi acordado nas negociações informais entre o Conselho e o Parlamento Europeu.

O Comité Económico e Social emitiu parecer sobre o regulamento em 2012 (JO C 229, de 31.07.2012, p. 90).

O Comité das Regiões emitiu parecer sobre o Regulamento ( JO C 391, de 18.12.2012, p. 127).

A Autoridade Europeia para a Proteção de Dados foi consultada e emitiu um primeiro parecer em 2012 (JO C 192, de 30.6.2012, p. 7) e um segundo parecer em 2015 (JO C 301, de 12.09.2015, p. 1-8).

A Agência dos Direitos Fundamentais da União Europeia emitiu parecer em 1 de outubro de 2012.

## II. OBJETIVO

O Regulamento Geral sobre a Proteção de Dados harmoniza as normas em matéria de proteção de dados na União Europeia. O regulamento tem por objetivos reforçar os direitos das pessoas singulares em matéria de proteção de dados, facilitar a livre circulação de dados pessoais no mercado único digital e reduzir os encargos administrativos.

## III. ANÁLISE DA POSIÇÃO DO CONSELHO EM PRIMEIRA LEITURA

### A. Observações genéricas

Atendendo ao objetivo do Conselho Europeu de alcançar um acordo sobre a reforma da proteção de dados até ao final de 2015, o Parlamento Europeu e o Conselho conduziram negociações informais para aproximarem as respetivas posições. O texto da posição do Conselho em primeira leitura relativa ao Regulamento Geral sobre a Proteção de Dados reflete inteiramente o compromisso alcançado entre os dois colegisladores, assistidos pela Comissão Europeia.

A posição do Conselho em primeira leitura mantém os objetivos da Diretiva 95/46/CE: a preservação dos direitos de proteção dos dados e a livre circulação dos dados. Ao mesmo tempo, procura adaptar as normas em matéria de proteção de dados atualmente em vigor, tendo em conta o volume crescente de dados pessoais que são tratados como resultado da evolução tecnológica e da globalização. Com vista a adequar o regulamento às exigências do futuro, as normas de proteção de dados da posição do Conselho em primeira leitura são tecnologicamente neutras.

A fim de assegurar um nível coerente de proteção das pessoas singulares em toda a União e evitar divergências que impeçam a livre circulação de dados pessoais no mercado interno, a posição do Conselho em primeira leitura prevê, em grande medida, um conjunto único de normas que é diretamente aplicável em toda a União. Esta harmonização eliminará a fragmentação decorrente das diferentes legislações dos Estados-Membros que transpõem a Diretiva 95/46. Todavia, para ter em conta os requisitos de situações específicas em matéria de tratamento dos dados, nomeadamente no setor público, a posição do Conselho em primeira leitura permite que os Estados-Membros especifiquem mais pormenorizadamente na sua legislação nacional a aplicação das regras de proteção de dados previstas no regulamento.

A proteção dos dados de caráter pessoal é um direito fundamental consagrado no artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia. Além disso, o artigo 16.º do Tratado sobre o Funcionamento da União Europeia estabelece que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito, independentemente da nacionalidade ou residência, e que devem ser estabelecidas normas para esse efeito e para efeitos da livre circulação de dados pessoais. Nessa base, a posição do Conselho em primeira leitura estabelece os princípios e as normas em matéria de proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais.

A fim de atingir os objetivos do regulamento, a posição do Conselho em primeira leitura reforça a responsabilização dos responsáveis pelo tratamento de dados (responsáveis por determinar as finalidades e os meios do tratamento de dados pessoais) e dos subcontratantes (responsáveis pelo tratamento de dados pessoais em nome do responsável pelo tratamento), por forma a promover uma verdadeira cultura de proteção de dados. Neste contexto, é introduzida ao longo de todo o regulamento uma abordagem baseada no risco que permite a modulação das obrigações do responsável pelo tratamento e do subcontratante em função do risco do tratamento de dados que efetuam. Além disso, os códigos de conduta e os procedimentos de certificação contribuem para a conformidade com as normas de proteção de dados. Esta abordagem evita normas excessivamente prescritivas e reduz os encargos administrativos, sem no entanto enfraquecer o cumprimento das normas. Além disso, o caráter dissuasivo das sanções possíveis que podem ser impostas cria incentivos para que os responsáveis pelo tratamento atuem em conformidade com o regulamento.

As novas normas sobre proteção de dados estabelecidas na posição do Conselho em primeira leitura também preveem direitos reforçados e suscetíveis de proteção judicial para os cidadãos. Tal permite que as pessoas singulares controlem melhor os seus dados pessoais, aumentando a confiança nos serviços fornecidos por via eletrónica a uma escala transfronteiras, o que irá estimular o mercado único digital. As crianças merecem proteção especial, uma vez que podem estar menos cientes dos riscos relacionados com o tratamento de dados pessoais, bem como dos seus direitos.

A posição do Conselho em primeira leitura reforça ainda a independência das autoridades de controlo, ao mesmo tempo que harmoniza as suas funções e competências. As regras para a cooperação entre autoridades de controlo e, se for caso disso, com a Comissão nos casos com dimensão transfronteiras – o procedimento de controlo da coerência – contribuirão para a aplicação coerente do presente regulamento em toda a União Europeia. Tal reforçará a segurança jurídica e reduzirá os encargos administrativos. Além disso, o mecanismo de balcão único prevê um único interlocutor para os responsáveis pelo tratamento e os subcontratantes em relação ao seu tratamento transfronteiras, incluindo as decisões vinculativas tomadas pelo recém-criado Comité Europeu para a Proteção de Dados em caso de litígio. Como resultado deste mecanismo, será assegurada uma aplicação mais coerente do regulamento. Além disso, tal reforçará a segurança jurídica e reduzirá os encargos administrativos.

Por último, a posição do Conselho em primeira leitura estabelece um quadro abrangente para as transferências de dados pessoais a partir da União Europeia para destinatários em países terceiros ou em organizações internacionais, que prevê novos instrumentos relativamente à Diretiva 95/46/CE.

## B. Elementos essenciais

Nas negociações informais, o Conselho e o Parlamento Europeu, assistidos pela Comissão Europeia, aproximaram as suas posições estabelecidas, respetivamente, na orientação geral do Conselho e na posição do Parlamento em primeira leitura. A posição do Conselho em primeira leitura relativa ao Regulamento Geral sobre a Proteção de dados reflete plenamente os compromissos acordados. Os aspetos principais da posição do Conselho em primeira leitura são indicados a seguir.

## 1. Âmbito de aplicação

### 1.1. Âmbito de aplicação material do regulamento e articulação com a Diretiva sobre a Proteção de Dados

A posição do Conselho em primeira leitura prevê que o Regulamento Geral sobre a Proteção de Dados se aplica ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais que façam parte de qualquer conjunto estruturado de dados pessoais acessíveis segundo critérios específicos, ou que se destinem a fazer parte de tal conjunto estruturado. O âmbito de aplicação material do Regulamento Geral sobre a Proteção de Dados e o âmbito de aplicação da Diretiva sobre a Proteção de Dados excluem-se mutuamente. É especificado que o regulamento não se aplica ao tratamento de dados pessoais efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Esta diferenciação permite que as autoridades responsáveis pela aplicação da lei, em especial a polícia, apliquem, por norma, o regime de proteção de dados da diretiva e, ao mesmo tempo, assegura um nível elevado e coerente de proteção dos dados pessoais das pessoas singulares que são objeto de operações policiais.

### 1.2. Instituições e órgãos da UE

Com vista a assegurar uma proteção uniforme e coerente dos titulares de dados relativamente ao tratamento dos seus dados pessoais, a posição do Conselho em primeira leitura indica que as adaptações necessárias do Regulamento (CE) n.º 45/2001 aplicável às instituições, órgãos, organismos e agências da UE deverão ter lugar após a adoção do Regulamento Geral sobre a Proteção de Dados, de modo a que possam ser aplicáveis ao mesmo tempo que o Regulamento Geral sobre a Proteção de Dados.

### 1.3. Isenção doméstica

A fim de evitar a fixação de normas que criariam encargos desnecessários para as pessoas singulares, a posição do Conselho em primeira leitura prevê que o regulamento não é aplicável ao tratamento de dados pessoais efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas, ou seja, sem qualquer ligação com uma atividade profissional ou comercial.

1.4. Âmbito de aplicação territorial

A posição do Conselho em primeira leitura cria condições de igualdade para os responsáveis pelo tratamento e os subcontratantes em termos de âmbito de aplicação territorial, englobando todos os responsáveis pelo tratamento e os subcontratantes, independentemente de estarem ou não estabelecidos na União.

Em primeiro lugar, o regulamento determina que as regras em matéria de proteção de dados se aplicam ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União. Em segundo lugar, a fim de assegurar que as pessoas singulares não sejam privadas da proteção dos seus dados, o regulamento aplica-se ao tratamento de dados pessoais de titulares de dados residentes no território da União, mesmo que os responsáveis pelo tratamento ou os subcontratantes não estejam estabelecidos na União, quando as atividades de tratamento estejam relacionadas com a oferta de bens ou serviços a esses titulares de dados na União, bem como com o controlo do seu comportamento, desde que esse comportamento tenha lugar na União Europeia. Além disso, este modo de determinação do âmbito de aplicação aumenta a segurança jurídica para os responsáveis pelo tratamento e os titulares de dados (as pessoas singulares cujos dados pessoais são tratados).

A posição do Conselho em primeira leitura assegura também que os titulares dos dados e as autoridades de controlo dispõem de um ponto de contacto na UE no caso de os responsáveis pelo tratamento e os subcontratantes não estarem estabelecidos na União, mas serem abrangidos pelo âmbito de aplicação do regulamento: têm de designar por escrito um representante seu na União. A fim de evitar encargos administrativos desnecessários, esta obrigação não é aplicável ao tratamento que não seja suscetível de implicar riscos para os direitos e liberdades individuais, nem ao tratamento efetuado por uma autoridade ou organismo público do país terceiro.

## 2. Princípios relativos ao tratamento de dados pessoais

Os princípios da proteção de dados aplicam-se a quaisquer informações relativas a uma pessoa singular identificada ou identificável, incluindo informações que deixaram de poder ser atribuídas a um determinado titular de dados sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável (pseudonimização). Em relação à Diretiva 95/46, o regulamento prevê, em grande medida, a continuidade no que respeita aos princípios subjacentes ao tratamento de dados pessoais. Ao mesmo tempo, o princípio da "minimização dos dados" foi adaptado de forma a ter em conta a realidade digital e com vista a estabelecer um equilíbrio entre, por um lado, a proteção dos dados pessoais e, por outro, as possibilidades de os responsáveis pelo tratamento tratarem os dados.

## 3. Licitude do tratamento

### 3.1. Condições de licitude

A fim de garantir a segurança jurídica, a posição do Conselho em primeira leitura assenta na Diretiva 95/46, ao especificar que o tratamento de dados pessoais só é lícito se forem preenchidas pelo menos uma das condições seguintes:

- o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
- o tratamento for necessário para a execução de um contrato;
- o tratamento for necessário para o cumprimento de uma obrigação jurídica;
- o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
- o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
- o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros.

Convém aprofundar duas condições: o consentimento e os interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros.

*3.1.1. Consentimento*

A fim de permitir o tratamento dos seus dados pessoais, o titular dos dados pode dar o seu consentimento ao tratamento através de um ato positivo inequívoco que constitua uma manifestação de vontade livre, específica, informada e inequívoca do seu acordo para que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. Esse consentimento abrange todas as atividades de tratamento realizadas com a mesma finalidade ou finalidades. Nos casos em que o tratamento sirva várias finalidades, deve ser dado o consentimento para todas as finalidades. Além disso, o responsável pelo tratamento deve ser capaz de demonstrar que o titular dos dados deu o seu consentimento para a operação de tratamento. O silêncio, as opções pré-validadas ou a omissão não constituem, por conseguinte, um consentimento. A definição do conceito de consentimento assegura a continuidade com o acervo que tem vindo a desenvolver-se no que respeita à utilização deste conceito com base na Diretiva 95/46/CE, contribuindo ao mesmo tempo para um entendimento e aplicação comuns da noção de consentimento em toda a União Europeia.

Por outro lado, a fim de proteger os direitos de proteção dos dados pessoais do titular dos dados, é especificado que, se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, qualquer parte dessa declaração que constitua uma violação do regulamento não é vinculativa. Além disso, ao avaliar se o consentimento é dado de livre vontade, há que verificar com a máxima atenção se, designadamente, a execução de um contrato depende do consentimento para se efetuar um tratamento que não é necessário para a execução desse contrato.

Por último, a fim de permitir derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, a posição do Conselho em primeira leitura prevê um limiar mais elevado do que para outros tratamentos, uma vez que o titular dos dados deve dar o seu consentimento explícito para o tratamento desses dados pessoais sensíveis.

No que toca às crianças, a posição do Conselho em primeira leitura prevê um regime específico de proteção para o consentimento das crianças em relação à oferta de serviços da sociedade da informação. O tratamento dos dados pessoais de crianças de menos de 16 anos é considerado lícito se puder ser razoavelmente verificado, tendo em conta os meios tecnológicos disponíveis, que o consentimento foi dado ou autorizado pelo titular da responsabilidade parental da criança. Os Estados-Membros que considerem mais adequado prever uma idade mais baixa são autorizados a fixar uma idade máxima inferior, mas não abaixo dos 13 anos.

*3.1.2. Interesse legítimo do responsável pelo tratamento*

O tratamento de dados pessoais pode ser considerado lícito se o tratamento for necessário para efeitos dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros. No entanto, esses interesses legítimos não constituem fundamento suficiente para o tratamento lícito nos casos em que prevaleçam interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

A existência de um interesse legítimo requer uma avaliação, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que estes poderão vir a ser tratados com essa finalidade. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta. Dado que incumbe ao legislador prever por lei a base jurídica para autorizar as autoridades a procederem ao tratamento de dados pessoais, o interesse legítimo não é aplicável aos tratamentos de dados pessoais efetuados pelas autoridades públicas no exercício das suas funções.

3.2. Regras dos Estados-Membros que adaptam a aplicação do regulamento

A posição do Conselho em primeira leitura permite que os Estados-Membros mantenham ou introduzam disposições mais específicas para adaptar a aplicação das regras do regulamento, caso os dados pessoais sejam tratados para o cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento As derrogações, requisitos específicos e outras medidas encontram-se também previstos em relação a operações de tratamento específicas em que os Estados-Membros conciliam o direito à proteção dos dados pessoais com o direito à liberdade de expressão e de informação, o acesso do público aos documentos oficiais, o tratamento dos números de identificação nacionais, o tratamento de dados no contexto laboral e o tratamento para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos.

3.3. Tratamento posterior

A posição do Conselho em primeira leitura prevê que o tratamento para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos só é lícito se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente objeto de tratamento. Todavia, quando o titular dos dados tiver dado o seu consentimento ou quando o tratamento se basear em disposições do direito da União ou de um Estado-Membro que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar, em especial, os importantes objetivos de interesse público geral, o responsável pelo tratamento está autorizado a proceder ao tratamento posterior dos dados pessoais, independentemente da compatibilidade das finalidades. Os direitos do titular de dados foram reforçados em caso de tratamento posterior, nomeadamente no que se refere ao direito à informação e ao direito de se opor a esse tratamento posterior quando tal tratamento não for necessário para a execução de uma missão efetuada por motivos de interesse público.

A fim de apurar se a finalidade de uma nova operação de tratamento é ou não compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento tem de ter em atenção, entre outros aspetos, a existência de uma ligação entre a primeira finalidade e aquela a que se destina a nova operação de tratamento que se pretende efetuar, o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, baseadas na sua relação com o responsável pelo tratamento, a natureza dos dados pessoais, as consequências que o posterior tratamento dos dados pode ter para o seu titular e a existência de garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas.

3.4. Tratamento de categorias especiais de dados pessoais

Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis, dado que o contexto do tratamento desses dados pode implicar riscos importantes para os direitos e liberdades fundamentais das pessoas singulares. Por essa razão, a posição do Conselho em primeira leitura mantém, regra geral, a abordagem da Diretiva 95/46 ao proibir o tratamento de categorias especiais de dados pessoais.

Em derrogação a esta regra, em certos casos exaustivamente enumerados, o tratamento de dados sensíveis é permitido, por exemplo, quando o titular dos dados tiver dado o seu consentimento explícito, quando o tratamento for necessário por motivos de interesse público importante, ou quando o tratamento for necessário para outros fins, designadamente no domínio da saúde.

Por fim, a posição do Conselho em primeira leitura prevê que os Estados-Membros possam manter ou introduzir outras condições, incluindo limitações, no que diz respeito ao tratamento de dados genéticos, biométricos ou de dados relativos à saúde. No entanto, essas outras condições não podem prejudicar a livre circulação de dados na União.

## 4. Atribuição de poderes aos titulares dos dados

### 4.1. Introdução

A posição do Conselho em primeira leitura confere poderes aos titulares de dados, atribuindo--lhes direitos reforçados de proteção de dados e incumbindo obrigações aos responsáveis pelo tratamento. Os direitos do titular de dados englobam o direito à informação, ao acesso aos dados pessoais, à retificação, ao apagamento dos dados pessoais, incluindo o "direito a ser esquecido", à limitação do tratamento, à portabilidade dos dados, de oposição e a não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis. Os direitos que sofreram importantes alterações em relação à Diretiva 95/46 são indicado em seguida.

Os responsáveis pelo tratamento são obrigados a facilitar o exercício dos direitos pelos titulares de dados e a efetuar o tratamento de dados pessoais em conformidade com o princípio de transparência, facultando, designadamente, informações sobre o tratamento dos dados pessoais que efetuam.

No entanto, se os dados pessoais tratados por um responsável pelo tratamento não lhe permitirem identificar um titular de dados, esse responsável pelo tratamento não é obrigado a obter informações suplementares para identificar o titular dos dados com o único objetivo de dar cumprimento a uma disposição do presente regulamento.

Sem prejuízo dos direitos dos titulares de dados e das obrigações dos responsáveis pelo tratamento, a posição do Conselho em primeira leitura mantém a abordagem da Diretiva 95/46 e prevê restrições aos princípios gerais e aos direitos das pessoas singulares desde que essa restrição se baseie no direito da União ou dos Estados-Membros. Essas restrições têm de respeitar o conteúdo essencial dos direitos e das liberdades fundamentais e devem ser necessárias e proporcionadas numa sociedade democrática para salvaguardar determinados interesses públicos.

4.2. Transparência

Em conformidade com o princípio da transparência, os responsáveis pelo tratamento devem fornecer informações e enviar comunicações relativas ao tratamento de dados pessoais de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações se destinam a crianças. As informações têm de ser prestadas por escrito ou por outros meios, e por via eletrónica sempre que for adequado.

A posição do Conselho em primeira leitura fixa ainda os prazos para os pedidos de informação, apresentação de comunicações ou qualquer outra ação por parte do responsável pelo tratamento, aos quais, por norma, deve ser dado seguimento a título gratuito. Todavia, se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, em especial devido ao seu caráter repetitivo, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável, tendo em conta os custos administrativos resultantes do fornecimento das informações ou da comunicação ou adoção da medida solicitada, ou pode recusar-se a dar seguimento ao pedido. Nesses casos, cabe ao responsável pelo tratamento demonstrar o caráter manifestamente infundado ou excessivo do pedido.

4.3. Informações e comunicações a fornecer pelo responsável pelo tratamento

Com vista a encontrar um equilíbrio entre, por um lado, a prestação de informações suficientes aos titulares dos dados sobre o tratamento dos seus dados pessoais e, por outro, evitar obrigações onerosas para os responsáveis pelo tratamento, a posição do Conselho em primeira leitura estabelece uma abordagem em duas fases para assegurar que os titulares dos dados são devidamente informados, tanto nos casos em que os dados pessoais tenham sido recolhidos junto do titular dos dados, como nos casos em que os dados pessoais não tenham sido obtidos junto do titular dos dados. Numa primeira fase, aquando da recolha dos dados pessoais, o responsável pelo tratamento é obrigado a fornecer ao titular dos dados as informações previstas no regulamento. Numa segunda fase, o responsável pelo tratamento deve fornecer informações adicionais previstas no regulamento, necessárias para garantir um tratamento equitativo e transparente. Os responsáveis pelo tratamento devem também informar os titulares de dados quando pretendam prosseguir o tratamento dos dados pessoais com uma finalidade diferente daquela para a qual os dados pessoais foram inicialmente recolhidos.

O responsável pelo tratamento não é obrigado a fornecer as informações enumeradas na primeira ou na segunda fase quando o titular dos dados já dispuser das informações. Sempre que os dados pessoais não tenham sido obtidos junto do titular de dados, o responsável pelo tratamento não faculta quaisquer informações ao titular dos dados, caso o registo ou a comunicação dos dados pessoais a terceiros forem expressamente previstos por lei, ou se a informação ao titular dos dados se revelar impossível de concretizar ou se implicar esforços desproporcionados.

Por último, os responsáveis pelo tratamento dos dados são obrigados a comunicar a cada destinatário a quem os dados tenham sido transmitidos qualquer retificação, apagamento ou limitação do tratamento dos dados a que se tenha procedido, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. Além disso, se o titular dos dados o solicitar, o responsável pelo tratamento tem de lhe fornecer informações sobre os referidos destinatários.

4.4. Ícones

Os princípios do tratamento transparente exigem que o titular dos dados seja informado do tratamento de dados e das suas finalidades. Neste contexto, a posição do Conselho em primeira leitura prevê que as informações possam ser fornecida aos titulares de dados em combinação com ícones normalizados. Os responsáveis pelo tratamento podem decidir, numa base voluntária, se a utilização desses ícones normalizados será útil para o tratamento dos dados pessoais que efetuam. Os ícones deverão dar, de forma facilmente visível, inteligível e claramente legível, uma útil perspetiva geral do tratamento previsto. Os ícones devem ser fornecidos ao mesmo tempo que as informações. Se forem apresentados por via eletrónica, os ícones devem ser de leitura automática. Com vista a contribuir para a utilização de ícones normalizados na UE, o regulamento habilita a Comissão a adotar atos delegados a fim de determinar quais as informações a fornecer por meio dos ícones e os procedimentos aplicáveis ao fornecimento de ícones normalizados. O Comité Europeu para a Proteção de Dados tem de dar parecer sobre os ícones propostos pela Comissão. A possibilidade de adotar atos delegados não impede o Comité Europeu para a Proteção de Dados de emitir diretrizes, opiniões e boas práticas sobre os ícones.

4.5. Direito de acesso

O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito estão ou não a ser objeto de tratamento e, se assim for, o titular tem o direito de aceder às informações enumeradas no regulamento. Em relação a este aspeto, o regulamento determina que o responsável pelo tratamento deve fornecer, a título gratuito, uma cópia dos dados pessoais em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. O direito de obter uma cópia não deve prejudicar os direitos e as liberdades de terceiros.

4.6. Direito ao apagamento dos dados ("direito a ser esquecido")

A posição do Conselho em primeira leitura permite que os titulares de dados tenham o direito ao apagamento dos dados pessoais que lhes digam respeito quando o tratamento desses dados não cumprir o disposto no regulamento ou no direito da União ou do Estado-Membro ao qual o responsável pelo tratamento está sujeito.

A referência ao "direito a ser esquecido" reconhece a necessidade de adaptar o direito ao apagamento dos dados, em especial num contexto digital. Os responsáveis pelo tratamento que tenham tornado públicos os dados pessoais em relação aos quais o respetivo titular pretende exercer o seu direito ao esquecimento, tem de tomar as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento desses dados pessoais do pedido de apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos, apresentado pelo titular dos dados. O Comité Europeu para a Proteção de Dados pode emitir diretrizes, recomendações e boas práticas para os procedimentos de apagamento de ligações para dados pessoais, bem como de cópias ou reproduções desses dados existentes em serviços de comunicação acessíveis ao público.

O direito ao apagamento e a obrigação de o responsável pelo tratamento informar outros responsáveis pelo tratamento do pedido de apagamento não se aplicam na medida em que esse tratamento de dados pessoais seja necessário para as finalidades exaustivamente enumeradas no regulamento, tais como o direito à liberdade de expressão e de informação.

4.7. Direito à portabilidade dos dados

A posição do Conselho em primeira leitura estabelece que sempre que o tratamento de dados pessoais for automatizado, os titulares dos dados têm o direito de receber os dados pessoais que lhes digam respeito e que forneceram a um responsável pelo tratamento, num formato estruturado, de uso corrente, de leitura automática e interoperável, bem como a transmitir esses dados a outro responsável. Além disso, é especificado que, sempre que seja tecnicamente possível, os titulares dos dados têm o direito de transmitir diretamente os dados pessoais a outro responsável pelo tratamento. Tal reforça ainda mais o controlo dos titulares de dados sobre os seus próprios dados, bem como incentiva a concorrência entre responsáveis pelo tratamento.

No entanto, o direito à portabilidade dos dados não se aplica ao tratamento necessário para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento. Além disso, quando um determinado conjunto de dados pessoais disser respeito a mais de um titular, o direito de um dos titulares de dados a receber os dados pessoais não prejudica os direitos e liberdades dos outros titulares.

4.8. Direito de oposição

Nos casos em que os dados pessoais possam ser licitamente tratados pelo facto de o tratamento ser necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, ou ainda por motivos de interesse legítimo do responsável pelo tratamento ou de terceiros, o titular dos dados tem o direito de se opor ao tratamento de quaisquer dados pessoais que digam respeito à sua situação específica. Nesse caso, o responsável pelo tratamento deixa de poder tratar os dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Neste contexto, é especificado que, sempre que os dados pessoais sejam tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor em qualquer momento ao tratamento dos dados pessoais que lhe digam respeito. Tal inclui a definição de perfis, na medida em que esteja relacionada com essa comercialização direta. A definição de perfis é definida como qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados para avaliar certos aspetos pessoais de uma pessoa singular, em especial para analisar ou prever aspetos relacionados com o seu desempenho profissional, situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações. Sempre que o titular dos dados se oponha ao tratamento de dados pessoais para efeitos de comercialização direta, estes deixam de poder ser tratados para esse fim. Além disso, esse direito deve ser explícita e claramente levado ao conhecimento do titular dos dados, o mais tardar no momento da primeira comunicação do responsável pelo tratamento com o titular dos dados.

A posição do Conselho em primeira leitura inclui ainda uma referência à função disponível por via eletrónica denominada "não rastrear" (*do-not-track*), especificando que, no contexto da utilização de serviços da sociedade da informação, o titular dos dados pode exercer o direito de se opor por meios automatizados, utilizando especificações técnicas.

4.9. Decisões individuais automatizadas, incluindo definição de perfis

O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado que avalie aspetos pessoais com ele relacionados e que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. São disso exemplos a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana. Tal tratamento automatizado pode incluir a definição de perfis. No entanto, este direito de não ficar sujeito a um tratamento automatizado não se aplica:

– quando for necessário para a celebração ou a execução de um contrato entre o titular dos dados e o responsável pelo tratamento;

– quando for autorizado pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e no qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular, como o controlo da fraude e da evasão fiscal; ou

– quando for baseado no consentimento explícito do titular dos dados.

Com exceção do segundo caso relacionado com o tratamento autorizado pelo direito da União ou dos Estados-Membros, o responsável pelo tratamento que efetua o tratamento automatizado deve aplicar salvaguardas adequadas para os direitos, as liberdades e os interesses legítimos dos titulares dos dados. Essas medidas de salvaguarda devem incluir, pelo menos, o direito de obter uma intervenção humana por parte do responsável pelo tratamento e a possibilidade de o titular dos dados manifestar o seu ponto de vista e contestar a decisão. Além disso, a fim de garantir um tratamento equitativo e transparente, os responsáveis pelo tratamento deverão utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis e medidas que minimizem os riscos potenciais para os interesses dos titulares dos dados.

Ao titular de dados são atribuídos poderes reforçados, dado que o responsável pelo tratamento está obrigado a fornecer-lhe, quando tal é necessário para assegurar um tratamento equitativo e transparente, informações sobre a existência de decisões automatizadas, incluindo a definição de perfis, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como à importância e às consequências previstas desse tratamento para o titular dos dados.

Por último, a decisão e definição de perfis automatizadas com base em categorias especiais de dados pessoais só poderão ser permitidas em condições específicas, incluindo o direito do titular de dados se opor ao tratamento quando os dados pessoais são objeto de um tratamento posterior para fins de investigação científica ou histórica ou para fins estatísticos, a menos que o tratamento seja necessário para a execução de uma missão de interesse público.

O Comité Europeu para a Proteção de Dados pode emitir diretrizes, recomendações e boas práticas para especificar mais em detalhe os critérios e as condições aplicáveis a decisões baseadas na definição de perfis.

## 5. Responsável pelo tratamento e subcontratante

### 5.1. Introdução

A posição do Conselho em primeira leitura estabelece o quadro jurídico para a responsabilidade por qualquer tratamento de dados pessoais realizado por um responsável pelo tratamento ou, por sua conta, por um subcontratante. Em consonância com o princípio da responsabilidade, o responsável pelo tratamento é obrigado a aplicar medidas técnicas e organizativas adequadas e ser capaz de demonstrar a conformidade das suas operações de tratamento com o regulamento. Nesse contexto, o regulamento estabelece regras aplicáveis às responsabilidades do responsável pelo tratamento no que diz respeito às avaliações de impacto, à manutenção de registos de tratamento, às violações de dados, à designação de um encarregado da proteção de dados e aos códigos de conduta e procedimentos de certificação.

### 5.2. Avaliações de impacto

Cabe ao responsável pelo tratamento efetuar uma avaliação de impacto sobre a proteção de dados a fim de determinar os casos em que o tratamento é suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares. A posição do Conselho em primeira leitura estabelece os casos específicos em que é exigida uma avaliação de impacto sobre a proteção de dados, como sejam certas operações específicas de tratamento de grande escala. No caso de tal avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não pode atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, impõe-se consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais. A autoridade de controlo pode então dar orientações ao responsável pelo tratamento e recorrer a todos os seus poderes.

O Comité Europeu para a Proteção de Dados pode emitir igualmente orientações sobre operações de tratamento que sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares e indicar quais as medidas adequadas em tais casos para responder a esse risco potencial.

5.3. Registos das atividades de tratamento

A fim de permitir que a autoridade de controlo efetue controlos *ex post*, o responsável pelo tratamento ou, caso exista, o seu representante, ou o subcontratante, tem que manter registos das atividades de tratamento realizadas sob a sua autoridade, incluindo as atinentes a violações de dados. Com vista a reduzir a carga administrativa, a obrigação de registo não se aplica às empresas ou organizações com menos de 250 assalariados, a menos que o tratamento por elas efetuado seja suscetível de implicar um risco para os direitos e liberdades dos titulares dos dados, não seja ocasional ou abranja dados sensíveis ou dados relativos a condenações e infrações penais.

5.4. Violações de dados

A violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social. A posição do Conselho em primeira leitura estabelece que os responsáveis pelo tratamento têm que notificar as violações de dados às autoridades de controlo, a menos que a violação não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Os responsáveis pelo tratamento têm também que comunicar aos titulares dos dados em causa as violações suscetíveis de apresentar um risco elevado. A notificação às autoridades de controlo permitir-lhes-á intervir, se necessário. Além disso, a comunicação aos titulares dos dados em causa permitir-lhes-á tomar medidas cautelares.

Com vista a reduzir a carga administrativa, a posição do Conselho em primeira leitura aplica diferentes limiares para as notificações à autoridade de controlo e as comunicações aos titulares dos dados em causa, com um limiar mais elevado para a comunicação do que para a notificação. Mal tenham conhecimento de uma violação de dados pessoais, os responsáveis pelo tratamento são obrigados a notificá-la à autoridade de controlo competente sem demora injustificada e, se possível, no prazo de 72 horas após terem tido conhecimento do ocorrido. No entanto, os responsáveis pelo tratamento podem prescindir da notificação se puderem demonstrar que a violação dos dados pessoais não é suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Tirando algumas exceções, os responsáveis pelo tratamento são obrigados a comunicar as violações de dados aos titulares dos dados em causa, sem demora injustificada, quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades desses titulares.

O Comité Europeu para a Proteção de Dados pode emitir diretrizes, recomendações e melhores práticas para o estabelecimento das violações de dados e a determinação da demora injustificada depois de o responsável pelo tratamento ter tido conhecimento da violação, para as circunstâncias particulares em que o responsável pelo tratamento é obrigado a notificar a violação de dados pessoais, bem como para as circunstâncias em que essa violação é suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares.

5.5. Encarregado da proteção de dados

O objetivo de designar um encarregado da proteção de dados é melhorar a conformidade com o regulamento. Por conseguinte, o encarregado da proteção de dados tem que ser uma pessoa com um conhecimento especializado da legislação e das práticas de proteção de dados, cabendo-lhe prestar assistência ao responsável pelo tratamento ou ao subcontratante para controlar o cumprimento do presente regulamento a nível interno. O encarregado da proteção de dados pode pertencer ao pessoal do responsável pelo tratamento dos dados ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviços. Pode designar-se um único encarregado da proteção de dados para um grupo de empresas ou caso o responsável pelo tratamento ou o subcontratante seja uma autoridade pública. A posição do Conselho em primeira leitura prevê a designação obrigatória de um encarregado da proteção de dados sempre que:

– o tratamento seja efetuado por uma autoridade pública, excetuando os tribunais ou autoridades judiciais independentes quando atuem no exercício das sua funções jurisdicionais,

– as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala, ou

– as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de dados sensíveis e de dados relacionados com condenações e infrações penais.

5.6. Códigos de conduta e procedimentos de certificação

A posição do Conselho em primeira leitura incentiva a aplicação de códigos de conduta e promove uma utilização mais ampla de procedimentos de certificação em matéria de proteção de dados, bem como de selos e marcas de proteção de dados. Tais iniciativas contribuem para o cumprimento das regras de proteção de dados, evitando ao mesmo tempo regras excessivamente prescritivas e reduzindo os custos para as autoridades públicas responsáveis pela sua aplicação. Além disso, os códigos de conduta podem atender às características específicas do tratamento efetuado em certos setores, bem como às necessidades das micro, pequenas e médias empresas. Por sua vez, os procedimentos de certificação e os selos e marcas de proteção de dados contribuem para o cumprimento do regulamento, uma vez que permitem aos titulares dos dados avaliar facilmente o nível de proteção de dados proporcionado pelos produtos e serviços pertinentes.

A posição do Conselho em primeira leitura inclui um conjunto elaborado de regras no que diz respeito aos códigos de conduta e aos procedimentos de certificação, assim como aos selos e marcas de proteção de dados, que dão margem à iniciativa privada e, simultaneamente, acautelam as normas de proteção de dados através do envolvimento das autoridades de controlo.

*5.6.1. Códigos de conduta*

A autoridade de controlo pode aprovar códigos de conduta ou alterações ou aditamentos aos mesmos. Sempre que o projeto de código de conduta diga respeito a atividades de tratamento em diversos Estados-Membros, antes da aprovação, a autoridade de controlo competente tem que submeter o projeto de código, de alteração ou de aditamento ao mesmo, ao Comité Europeu para a Proteção de Dados, para parecer.

A Comissão pode adotar atos de execução a fim de decidir que os novos códigos de conduta, bem como as alterações ou aditamentos aos códigos de conduta existentes aprovados pela autoridade de controlo competente, são de aplicabilidade geral na União.

O Comité Europeu para a Proteção de Dados deverá encorajar a elaboração de códigos de conduta. Cabe-lhe também recolher todos os códigos de conduta aprovados e respetivas alterações num registo e disponibilizá-los ao público por todos os meios adequados.

*5.6.2. Procedimentos de certificação, e selos e marcas de proteção de dados*

A posição do Conselho em primeira leitura estabelece que cada Estado-Membro tem que definir se os organismos de certificação são acreditados pela autoridade de controlo ou pelo organismo nacional de acreditação. Os organismos de certificação acreditados podem certificar os responsáveis pelo tratamento e os subcontratantes com base nos critérios aprovados pela autoridade de controlo competente ou, em conformidade com o procedimento de controlo da coerência, pelo Comité Europeu para a Proteção de Dados. Neste último caso, os critérios aprovados pelo Comité Europeu para a Proteção de Dados podem ter como resultado uma certificação comum: o Selo Europeu de Proteção de Dados. A certificação é emitida aos responsáveis pelo tratamento ou subcontratantes por um período máximo de três anos, renovável. O organismo de certificação tem que fornecer à autoridade de controlo os motivos que levaram à concessão ou revogação da certificação solicitada. Subsequentemente, a autoridade de controlo pode rejeitar ou declarar inválida essa certificação.

A Comissão tem competência para adotar atos delegados a fim de especificar os requisitos a ter em conta relativamente aos procedimentos de certificação em matéria de proteção de dados. O Comité Europeu para a Proteção de Dados tem de dar parecer sobre esses requisitos. A Comissão pode também adotar atos de execução sobre as normas técnicas para os procedimentos de certificação e os selos e marcas de proteção de dados, e sobre os procedimentos para promover e reconhecer os procedimentos de certificação e os selos e marcas de proteção de dados.

Por último, o Comité Europeu para a Proteção de Dados deverá encorajar o estabelecimento de procedimentos de certificação em matéria de proteção de dados, e de selos e marcas de proteção de dados.

## 6. Transferência de dados pessoais para países terceiros ou organizações internacionais

### 6.1. Introdução

A circulação transfronteiras de dados pessoais, com origem quer em países não pertencentes à União quer em organizações internacionais ou a eles destinados, é crucial num contexto de comércio mundial e de uma economia digital transfronteiras. O nível de proteção garantido pela União não pode ser posto em causa se os dados pessoais de cidadãos da UE forem transferidos para fora da União.

Como princípio geral, só pode ser efetuada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se os responsáveis pelo tratamento e os subcontratantes cumprirem as regras estabelecidas no regulamento. A posição do Conselho em primeira leitura tem plenamente em conta a jurisprudência do Tribunal de Justiça da União Europeia, designadamente o seu acórdão de 6 de outubro de 2015 no processo C-362/14. A posição do Conselho mantém as diferentes formas possíveis de transferências transfronteiras de dados pessoais, reforçando simultaneamente as garantias de que são respeitados os direitos à proteção de dados. Essas diferentes formas de transferência de dados pessoais consistem em decisões de adequação, garantias adequadas e derrogações.

A posição do Conselho em primeira leitura clarifica que as decisões judiciais e as decisões de autoridades administrativas de um país terceiro que exijam que o responsável pelo tratamento dos dados ou o subcontratante transfira ou divulgue dados pessoais só são reconhecidas ou executadas se tiverem como base um acordo internacional em vigor entre o país terceiro em causa e a União ou um dos Estados-Membros. Além disso, a posição do Conselho em primeira leitura especifica expressamente que tais acordos internacionais são aplicáveis sem prejuízo de outros motivos de transferências transfronteiras previstos no regulamento.

6.2. Decisões de adequação

As transferências internacionais podem ser efetuadas com base numa decisão de adequação da Comissão determinando que o país terceiro, ou um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção essencialmente equivalente ao garantido na União. A segurança jurídica e a uniformidade são assim garantidas em toda a União.

A Comissão pode decidir revogar uma decisão de adequação, após notificação e apresentação de justificação exaustiva ao país terceiro ou à organização internacional. A Comissão adota decisões de adequação e decisões de revogação de tais decisões sob a forma de atos de execução. Os atos de execução têm de prever um procedimento de revisão periódica, no mínimo de quatro em quatro anos. A Comissão tem de controlar os desenvolvimentos nos países terceiros e nas organizações internacionais que possam afetar o funcionamento das decisões de adequação. Para efeitos de controlo e de realização das revisões periódicas, a Comissão deverá ter em consideração os pontos de vista e as conclusões a que tenham chegado o Parlamento Europeu e o Conselho, bem como outros organismos e fontes pertinentes. No contexto da avaliação e revisão do regulamento, a Comissão tem ainda de apresentar relatórios periódicos ao Parlamento Europeu e ao Conselho. Por último, o Comité Europeu para a Proteção de Dados tem de dar parecer à Comissão para avaliar a adequação do nível de proteção num país terceiro ou numa organização internacional, e também para avaliar se o nível de proteção adequado deixou de ser assegurado.

As decisões adotadas pela Comissão com base no artigo 25.º, n.º 6, da Diretiva 95/46/CE permanecem em vigor até que sejam alteradas, substituídas ou revogadas por uma decisão da Comissão. Do mesmo modo, as autorizações concedidas por um Estado-Membro ou uma autoridade de controlo com base no artigo 26.º, n.º 2, da Diretiva 95/46/CE e as decisões adotadas pela Comissão com base no artigo 26.º, n.º 4, da Diretiva 95/46/CE continuam válidas até que sejam alteradas, substituídas ou revogadas, caso seja necessário, respetivamente por essa autoridade de controlo ou por uma decisão da Comissão. Ao assegurar a continuidade, a posição do Conselho em primeira leitura garante a segurança jurídica.

6.3. Garantias adequadas

Além de decisões de adequação, podem também ser efetuadas transferências transfronteiras se o responsável pelo tratamento ou o subcontratante tiver dado garantias adequadas para colmatar a insuficiência da proteção de dados no país terceiro ou na organização internacional. Tais garantias podem consistir em instrumentos juridicamente vinculativos e com força executiva entre autoridades ou organismos públicos, regras vinculativas aplicáveis às empresas, cláusulas-tipo de proteção de dados adotadas pela Comissão, cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo, ou cláusulas contratuais autorizadas por esta autoridade. Os responsáveis pelo tratamento ou os subcontratantes num país terceiro também podem oferecer garantias adequadas para as transferências de dados pessoais para países terceiros ou organizações internacionais. Podem fazê-lo através do cumprimento de um código de conduta aprovado acompanhado de compromissos vinculativos e com força executiva no sentido de aplicarem as garantias adequadas, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, inclusivamente em relação aos direitos dos titulares dos dados. Podem igualmente fazê-lo através de um procedimento de certificação aprovado pela autoridade de controlo competente, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, inclusivamente em relação aos direitos dos titulares dos dados.

6.4. Derrogações

Na falta de uma decisão de adequação ou de garantias adequadas, podem ser efetuadas transferências ou conjuntos de transferências de dados pessoais para países terceiros ou organizações internacionais com base nas derrogações que estejam expressamente enumeradas no regulamento. Uma dessas derrogações diz respeito aos interesses legítimos visados pelo responsável pelo tratamento, desde que os interesses ou os direitos e liberdades do titular dos dados não prevaleçam sobre aqueles interesses. De modo a que possam ser previstas garantias suficientes para as transferências transfronteiras de dados pessoais, os interesses legítimos do responsável pelo tratamento são rigorosamente enquadrados e só podem ser invocados como *ultimum remedium*. A fim de assegurar uma aplicação coerente do regulamento, o Comité Europeu para a Proteção de Dados tem de elaborar e reexaminar, por sua própria iniciativa ou a pedido da Comissão, diretrizes, recomendações e melhores práticas para especificar mais em detalhe os critérios e requisitos aplicáveis às transferências de dados na falta de uma decisão de adequação ou de garantias adequadas.

## 7. Autoridades de controlo

### 7.1. Independência

A fim de proteger os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento dos seus dados pessoais e facilitar a livre circulação desses dados na União, os Estados-Membros têm de estabelecer que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do regulamento no seu território. Cada autoridade de controlo e respetivos membros têm de agir com total independência e integridade no desempenho das funções e no exercício dos poderes que são atribuídos a essa autoridade de controlo e respetivos membros.

As autoridades de controlo têm de contribuir para a aplicação coerente do regulamento em toda a União. Para esse efeito, as autoridades de controlo têm de cooperar entre si e com o Comité Europeu para a Proteção de Dados, e bem assim com a Comissão. A coerência na aplicação do regulamento é ainda assegurada pelo estabelecimento das competências das autoridades de controlo e a definição das funções e dos poderes de investigação, poderes de correção e de autorização, bem como dos poderes consultivos, que as autoridades de controlo devem, no mínimo, possuir.

### 7.2. Sigilo profissional

A posição do Conselho em primeira leitura estabelece regras em matéria de sigilo profissional aplicáveis às autoridades de controlo e aos seus membros. Em primeiro lugar, os membros e o pessoal de cada autoridade de controlo têm de ficar sujeitos, nos termos do direito da União ou dos Estados-Membros, à obrigação de sigilo profissional, tanto durante o seu mandato como após o termo deste, no que respeita a quaisquer informações confidenciais a que tenham tido acesso no desempenho das suas funções ou no exercício dos seus poderes. É ainda especificado que, durante o seu mandato, o dever de sigilo profissional é aplicável, em especial, à comunicação, por pessoas singulares, de violações ao regulamento. Cabe ainda ao Comité Europeu para a Proteção de Dados emitir diretrizes, recomendações e melhores práticas para definir procedimentos comuns para a comunicação, por pessoas singulares, de violações ao regulamento.

## 8. Cooperação e coerência

### 8.1. Comité Europeu para a Proteção de Dados

A posição do Conselho em primeira leitura institui o Comité Europeu para a Proteção de Dados como um organismo da União dotado de personalidade jurídica tendo em vista assegurar a aplicação correta e coerente do regulamento. As intervenções do comité consistem nomeadamente na emissão de pareceres, na adoção de decisões vinculativas no contexto da resolução de litígios entre autoridades de controlo ou na emissão de orientações sobre qualquer assunto relativo à aplicação do presente regulamento a fim de assegurar a aplicação coerente do regulamento.

O Comité Europeu para a Proteção de Dados é composto pelo diretor de uma autoridade de controlo de cada Estado-Membro e da Autoridade Europeia para a Proteção de Dados, ou pelos respetivos representantes. A Comissão tem o direito de participar nas atividades e reuniões do Comité Europeu para a Proteção de Dados, sem direito de voto. Os debates do Comité Europeu para a Proteção de Dados são confidenciais quando o referido comité o considerar necessário, nos termos do seu regulamento interno.

Caso o Comité Europeu para a Proteção de Dados adote uma decisão vinculativa no contexto da resolução de litígios, a Autoridade Europeia para a Proteção de Dados apenas tem direito de voto nas decisões que digam respeito a princípios e normas aplicáveis às instituições, órgãos, organismos e agências da União que correspondam, em substância, às do regulamento.

### 8.2. Procedimento de controlo da coerência

Nos casos de tratamento transfronteiras de dados pessoais em que participe mais do que uma autoridade de controlo, o procedimento de controlo da coerência assegura a tomada de uma única decisão que será aplicável em toda a União Europeia, sendo simultaneamente tido em conta o parecer de várias autoridades de controlo interessadas. O procedimento de controlo da coerência reforça por conseguinte a proximidade entre os titulares dos dados e a autoridade de controlo que toma as decisões, ao associar as autoridades de controlo locais ao processo de tomada de decisões. Além disso, em caso de litígios entre autoridades de controlo de diferentes Estados-Membros, o recém-criado Comité Europeu para a Proteção de Dados é competente para tomar decisões vinculativas.

As regras do procedimento de controlo da coerência não são aplicáveis caso o tratamento dos dados seja efetuado por autoridades públicas ou organismos privados que atuem no interesse público. Em tais casos, a única autoridade de controlo competente é a autoridade de controlo do Estado-Membro em que estiver estabelecida tal autoridade pública ou organismo privado.

A posição do Conselho em primeira leitura prevê que, no contexto da avaliação do regulamento a efetuar pela Comissão, seja examinada a aplicação do procedimento de cooperação e controlo da coerência.

## 9. Vias de recurso, responsabilidades e sanções

A posição do Conselho em primeira leitura estabelece um conjunto pormenorizado de regras que confere aos titulares dos dados várias possibilidades de recurso, incluindo a de pedir indemnização por danos resultantes da violação do regulamento.

### 9.1. Direito de apresentar reclamação e direito à ação judicial

A posição do Conselho em primeira leitura prevê que todos os titulares dos dados tenham direito a apresentar reclamação a uma autoridade de controlo, se considerarem que o tratamento dos seus dados pessoais não cumpre o presente regulamento. Além disso, os titulares dos dados têm ainda direito a uma ação judicial efetiva contra decisões juridicamente vinculativas das autoridades de controlo que lhes digam respeito. Têm também direito a uma ação judicial efetiva caso a autoridade de controlo não trate a reclamação ou não preste informações sobre o andamento ou o resultado da reclamação.

Os titulares dos dados têm ainda direito a uma ação judicial efetiva se considerarem ter havido violação dos direitos que lhes assistem nos termos do presente regulamento, na sequência do tratamento dos seus dados pessoais efetuado em violação do disposto no regulamento.

É assegurada a proximidade entre o titular dos dados e os tribunais nacionais porquanto o titular tem direito a que a decisão da respetiva autoridade de proteção de dados seja apreciada pelo seu tribunal nacional, independentemente do Estado-Membro no qual está estabelecido o responsável pelo tratamento ou o subcontratante. Os recursos contra os responsáveis pelo tratamento dos dados ou os subcontratantes têm de ser interpostos nos tribunais do Estado--Membro em que tenham um estabelecimento. Em alternativa, esses recursos podem ser interpostos nos tribunais do Estado-Membro em que o titular dos dados tenha a sua residência habitual, salvo se o responsável pelo tratamento dos dados ou o subcontratante for uma autoridade pública de um Estado-Membro no exercício dos seus poderes públicos.

Por último, todas as pessoas singulares ou coletivas têm o direito de interpor recurso de anulação das decisões do Comité Europeu para a Proteção de Dados para o Tribunal de Justiça da União Europeia nas condições previstas no artigo 263.º do TFUE.

9.2. Representação dos titulares dos dados

O titular dos dados tem o direito de mandatar os organismos, organizações ou associações que satisfaçam critérios específicos, como as que não têm fins lucrativos e cuja atividade abrange a proteção de dados, para, em seu nome, apresentar reclamação, exercer o direito de recurso judicial e exercer o direito a receber uma indemnização, se tal estiver previsto no direito do Estado-Membro. Estes critérios específicos visam evitar o desenvolvimento de uma cultura de reclamações de natureza comercial no domínio da proteção de dados. Além disso, os Estados--Membros podem prever que tal organismo, organização ou associação, independentemente de um mandato conferido pelo titular dos dados, tenha nesse Estado-Membro direito a apresentar uma reclamação à autoridade de controlo competente, e a exercer os direitos de intentar ação judicial caso considere que ocorreu uma violação dos direitos do titular dos dados em virtude do tratamento de dados pessoais efetuado em violação do disposto no regulamento.

9.3. Suspensão do processo

A fim de evitar que a mesma questão relativa ao tratamento de dados pelo mesmo responsável ou subcontratante seja apreciada em vários tribunais, os tribunais competentes que não o tribunal onde foi intentada a primeira ação podem suspender o processo ou, a pedido de uma das partes, declarar-se incompetentes.

9.4. Direito de indemnização e responsabilidade

A posição do Conselho em primeira leitura estabelece que qualquer titular de dados que tenha sofrido danos materiais ou imateriais devido a uma violação do regulamento tem direito a receber uma indemnização do responsável pelo tratamento dos dados ou do subcontratante. Com vista a dar aos titulares dos dados a possibilidade de pedir uma indemnização em caso de danos, proporcionando simultaneamente segurança jurídica aos responsáveis pelo tratamento e subcontratantes, o regulamento especifica as respetivas responsabilidades. Os responsáveis pelo tratamento implicados no tratamento são responsáveis pelos danos causados. O subcontratante é responsável apenas se não tiver cumprido as obrigações decorrentes do regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido ou tiver desrespeitado as instruções legítimas do responsável pelo tratamento. Todavia, o responsável pelo tratamento ou o subcontratante é exonerado da sua responsabilidade se provar que o facto que causou o dano não lhe é de modo algum imputável.

Caso mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, estejam envolvidos no mesmo tratamento e sejam responsáveis por eventuais danos causados pelo tratamento, cada responsável pelo tratamento ou subcontratante é responsável pela totalidade dos danos, a fim de assegurar a efetiva indemnização do titular dos dados. Todavia, quando tenha pago uma indemnização integral pelos danos sofridos, o responsável pelo tratamento ou o subcontratante tem o direito de reclamar aos outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento a parte da indemnização correspondente à respetiva parte de responsabilidade pelo dano.

9.5. Sanções

A fim de assegurar o cumprimento do regulamento, a posição do Conselho em primeira leitura prevê que as autoridades de controlo podem impor coimas. Essas coimas devem ser eficazes, proporcionadas e dissuasivas. Os Estados-Membros podem prever as regras que permitam determinar se e em que medida as coimas podem ser aplicadas às autoridades e organismos públicos estabelecidas no seu território. Para além de impor coimas, as autoridades de controlo podem exercer também outros poderes de correção como advertências ou repreensões. Com vista a uma maior harmonização, o Comité Europeu para a Proteção de Dados deve elaborar diretrizes dirigidas às autoridades de controlo relativas à aplicação dos seus poderes de correção e à fixação de coimas.

A posição do Conselho em primeira leitura contém uma lista de critérios a respeitar pela autoridade de controlo quando decidir sobre aplicar ou não uma coima e, em caso afirmativo, determinar o respetivo montante. Esses critérios prendem-se, nomeadamente, com a natureza, a gravidade e a duração ou o caráter intencional ou negligente da violação do regulamento. O regulamento estabelece a lista de infrações e as correspondentes coimas máximas. Dentro da moldura estabelecida para essas coimas máximas, a autoridade de controlo deve determinar o montante adequado em função das circunstâncias de cada infração. Com vista a garantir segurança jurídica aos responsáveis pelo tratamento e subcontratantes e a reforçar a harmonização das coimas dentro da União, deixando, simultaneamente, uma margem de apreciação às autoridades de controlo, essas infrações são subdivididas em três categorias. As infrações na primeira categoria relacionadas com as obrigações dos responsáveis pelo tratamento e dos subcontratantes podem ser sancionadas com coimas até 10 000 000 EUR ou, no caso de uma empresa, até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado. A segunda categoria de violações dos direitos dos titulares de dados e dos princípios gerais tem um limite máximo de 20 000 000 EUR ou 4 % do volume de negócios. A terceira categoria de infrações diz respeito ao não cumprimento de uma ordem da autoridade de controlo e é igualmente sancionada com uma coima máxima de 20 000 000 de EUR ou 4 % do volume de negócios.

## 10. Situações específicas de tratamento de dados

10.1. Tratamento de dados pessoais e liberdade de expressão e de informação

Os Estados-Membros têm de garantir por lei a conciliação do direito à proteção de dados pessoais com o direito à liberdade de expressão e de informação, incluindo o tratamento de dados pessoais para fins jornalísticos e para fins de expressão académica, artística ou literária. A fim de garantir a transparência no que respeita à conciliação destes direitos, os Estados--Membros são obrigados a notificar à Comissão as disposições pertinentes do seu direito e as alterações a essas disposições, bem como as novas disposições pertinentes.

10.2. Tratamento de dados no contexto laboral

Os Estados-Membros podem, através de disposições legislativas ou em convenções coletivas, prever normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos assalariados no contexto laboral.

Estas normas devem incluir medidas adequadas e específicas que garantam a dignidade humana, os interesses legítimos e os direitos fundamentais do titular dos dados. Os Estados--Membros devem notificar à Comissão as disposições pertinentes do seu direito e as alterações a estas disposições, bem como as novas disposições pertinentes.

10.3. Garantias e derrogações ao tratamento dos dados pessoais para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos

A posição do Conselho em primeira leitura especifica as regras aplicáveis ao tratamento dos dados pessoais para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos. Estas regras destinam-se a conciliar, por um lado, o interesse da disponibilidade dos dados pessoais para manter arquivos, fornecer estatísticas e fazer investigação e, por outro lado, os direitos em matéria de proteção de dados.

O tratamento dos dados pessoais para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, tem de estar sujeito a garantias adequadas para os direitos e liberdades do titular dos dados nos termos do regulamento. Os Estados-Membros são autorizados a estabelecer, sob condições específicas e mediante garantias adequadas para o titular dos dados, especificações e derrogações dos requisitos de informação e direitos à retificação, ao apagamento dos dados pessoais, a ser esquecido, à limitação do tratamento, à portabilidade dos dados e de oposição aquando do tratamento de dados pessoais para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos.

A posição do Conselho em primeira leitura prevê uma derrogação à proibição de tratar dados pessoais sensíveis em caso de tratamento de dados para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos. Estas derrogações são autorizadas se o tratamento em causa estiver baseado no direito da União ou no direito de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados.

**11. Acordos celebrados anteriormente**

A posição do Conselho em primeira leitura especifica que os acordos internacionais celebrados pelos Estados-Membros antes da entrada em vigor do presente regulamento, que impliquem a transferência de dados pessoais para países terceiros ou organizações internacionais e que sejam conformes com o direito da União aplicável antes de o presente regulamento entrar em vigor, permanecem em vigor até serem alterados, substituídos ou revogados. Desta forma fica garantida a segurança jurídica para os responsáveis pelo tratamento de dados e evitam-se encargos administrativos desnecessários para os Estados--Membros. Por outro lado, é tido em conta o facto de os Estados-Membros dependerem da cooperação do país terceiro ou da organização internacional para alterar os acordos em vigor.

## IV. CONCLUSÃO

A posição do Conselho em primeira leitura reflete o compromisso alcançado nas negociações informais realizadas entre o Conselho e o Parlamento Europeu e mediadas pela Comissão. O Conselho convida o Parlamento Europeu a aprovar formalmente a posição do Conselho em primeira leitura, sem alterações, para que se possa estabelecer o novo quadro legislativo da UE para a proteção de dados, que reforçará os direitos de proteção de dados, facilitando simultaneamente o fluxo de dados pessoais no mercado digital.