Jornal Oficial
da União Europeia

PT
Série L

2025/2050

9.10.2025

REGULAMENTO DELEGADO (UE) 2025/2050 DA COMISSÃO

de 1 de julho de 2025

que completa o Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho estabelecendo as condições técnicas e os procedimentos de acordo com os quais os fornecedores de plataformas em linha de muito grande dimensão e de motores de pesquisa em linha de muito grande dimensão devem partilhar dados com os investigadores habilitados

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE ([1]), nomeadamente o artigo 40.º, n.º 13,

Considerando o seguinte:

(1) O artigo 40.º do Regulamento (UE) 2022/2065 estabelece as regras relativas à concessão de acesso aos dados pelos fornecedores de plataformas em linha de muito grande dimensão e de motores de pesquisa em linha de muito grande dimensão. Mais especificamente, permite a concessão desse acesso aos investigadores que concluam um processo no qual demonstrem o cumprimento das condições estabelecidas no n.º 8 do referido artigo (a seguir designados por «investigadores habilitados»).

(2) Nos termos do artigo 40.º, n.º 4, do Regulamento (UE) 2022/2065, os investigadores habilitados devem ter acesso aos dados, a fim de os ajudar a estudar os riscos sistémicos na União e a avaliar a eficácia das medidas de atenuação desses riscos. As suas conclusões podem constituir um contributo valioso para a execução do Regulamento (UE) 2022/2065 e promover a responsabilização dos fornecedores de plataformas em linha de muito grande dimensão e de motores de pesquisa em linha de muito grande dimensão. O presente regulamento tem por objetivo estabelecer as condições técnicas e os procedimentos necessários para permitir esse acesso de forma segura, eficiente e coerente entre todos os coordenadores dos serviços digitais, e de modo a garantir a igualdade de tratamento dos investigadores e dos fornecedores de dados.

(3) De modo a assegurar que o processo de acesso aos dados seja coerente entre todos os coordenadores dos serviços digitais e claro e transparente para todos, é necessário criar uma infraestrutura digital específica (a seguir designada por «portal de acesso aos dados do RSD»). O portal de acesso aos dados do RSD deve permitir que os investigadores, os fornecedores de dados e os coordenadores dos serviços digitais participem no processo de acesso aos dados, tenham acesso e divulguem informações pertinentes, como os dados dos pontos de contacto específicos, e comuniquem entre si. O portal de acesso aos dados do RSD não deve ser considerado uma das modalidades de acesso a utilizar para facultar acesso aos dados na sequência de um pedido fundamentado.

(4) Os fornecedores de dados e os investigadores que pretendam participar no processo de acesso aos dados devem criar uma conta no portal de acesso aos dados do RSD para esse efeito. Para assegurar que os coordenadores dos serviços digitais possam aceder às informações apresentadas através do portal de acesso aos dados do RSD sem terem de criar uma conta separada no portal, este deve ser interoperável com o sistema de partilha de informações AGORA, criado nos termos do Regulamento de Execução (UE) 2024/607 da Comissão ([2]).

(5) Para assegurar a transparência do processo de acesso aos dados para todas as partes envolvidas e acompanhar a eficiência e a eficácia do referido processo, bem como o cumprimento do disposto no artigo 40.º, n.º 4, do Regulamento (UE) 2022/2065 e no presente regulamento, o portal de acesso aos dados do RSD deve gerar notificações automáticas relativas às diferentes etapas e atualizações do processo.

([1]) JO L 277 de 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

([2]) Regulamento de Execução (UE) 2024/607 da Comissão, de 15 de fevereiro de 2024, relativo às disposições práticas e operacionais para o funcionamento do sistema de partilha de informações nos termos do Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho (Regulamento dos Serviços Digitais) (JO L, 2024/607, 16.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/607/oj).

(6) A fim de fornecer aos investigadores informações coerentes sobre o processo de acesso aos dados, os coordenadores dos serviços digitais devem disponibilizar e tornar facilmente acessíveis nas suas interfaces em linha informações sobre o referido processo, incluindo hiperligações para o portal de acesso aos dados do RSD. Para evitar a criação de encargos administrativos desnecessários, aumentar a eficiência e facilitar a comunicação entre todas as partes envolvidas no processo de acesso aos dados, os coordenadores dos serviços digitais são incentivados a facilitar a gestão das informações relativas ao referido processo, também do ponto de vista linguístico.

(7) De modo a permitir que os investigadores identifiquem os dados pertinentes para os fins previstos no artigo 40.º, n.º 4, do Regulamento (UE) 2022/2065, os fornecedores de dados devem disponibilizar catálogos de dados do RSD para os seus serviços. Esses catálogos devem ser facilmente localizáveis e acessíveis nas interfaces em linha dos fornecedores de dados e descrever os ativos de dados disponíveis, a sua estrutura de dados e os metadados, cujo acesso pode ser solicitado nos termos do artigo 40.º, n.º 4, do Regulamento (UE) 2022/2065. Ao disponibilizarem os catálogos de dados do RSD, os fornecedores de dados devem ter em conta os riscos para a confidencialidade, a segurança dos dados ou a proteção de dados pessoais que possam advir da divulgação pública dessas informações.

(8) De modo a contribuir para o desenvolvimento de projetos de investigação pertinentes para os fins previstos no artigo 40.º, n.º 4, do Regulamento (UE) 2022/2065, os catálogos de dados do RSD devem incluir, designadamente, dados relacionados com os riscos sistémicos na União identificados pelos fornecedores de dados nas suas avaliações anuais dos riscos efetuadas nos termos do artigo 34.º do referido regulamento, bem como dados relacionados com quaisquer medidas de atenuação dos riscos referidas no artigo 35.º do mesmo regulamento. Para assegurar a pertinência e a atualidade dos catálogos de dados do RSD, estes devem ser atualizados regularmente e tendo em devida conta os riscos sistémicos recém-identificados e a evolução dos riscos sistémicos. Por exemplo, devem refletir os riscos emergentes identificados na sequência de uma avaliação *ad hoc* dos riscos efetuada nos termos do artigo 34.º do Regulamento (UE) 2022/2065 ou de um relatório de auditoria apresentado nos termos do artigo 37.º do mesmo regulamento. Para minimizar a carga processual suportada pelos fornecedores de dados, se for caso disso, esses catálogos poderão basear-se nos recursos de documentação de dados existentes e utilizados para outros fins e públicos, como a publicidade, a criação de conteúdos ou o desenvolvimento de aplicações de terceiros. Os catálogos de dados do RSD não devem ter de ser exaustivos nem, por conseguinte, vincular ou limitar os investigadores requerentes nos seus pedidos de acesso aos dados.

(9) A fim de permitir que o coordenador dos serviços digitais de estabelecimento determine mais facilmente as modalidades de acesso e de reduzir os encargos globais do processo de acesso aos dados para todos os intervenientes envolvidos, os fornecedores de dados devem publicar as modalidades de acesso por eles propostas para os dados descritos nos catálogos de dados do RSD. Estas modalidades de acesso propostas devem ser proporcionais à sensibilidade dos dados e incluir informações sobre as eventuais condições técnicas, organizativas e jurídicas consideradas adequadas pelos fornecedores de dados para permitir o fornecimento dos dados. As modalidades de acesso propostas pelos fornecedores de dados não devem vincular os coordenadores dos serviços digitais de estabelecimento, que devem continuar a ter competência para determinar as modalidades de acesso adequadas.

(10) A fim de assegurar que os pedidos de acesso aos dados beneficiem de igualdade de tratamento, independentemente do coordenador dos serviços digitais ao qual o pedido de acesso aos dados seja apresentado ou de que provenha o pedido fundamentado, deve ser fixado um prazo para a formulação de pedidos fundamentados, de modo a garantir a coerência entre todos os coordenadores dos serviços digitais. Se a formulação do pedido fundamentado exigir mais tempo, o coordenador dos serviços digitais de estabelecimento deve notificar o investigador principal, indicando os motivos do atraso. Esses motivos podem incluir a necessidade de verificações adicionais por parte do coordenador dos serviços digitais do organismo de investigação ou de estabelecimento, por exemplo, se os pedidos de acesso aos dados implicarem transferências internacionais de dados ou o coordenador dos serviços digitais de estabelecimento identificar potenciais riscos para a segurança da União, caso os dados sejam partilhados. Com vista a alinhar também as etapas do processo de acesso aos dados que antecedem a formulação de pedidos fundamentados, nomeadamente a avaliação dos pedidos de acesso aos dados e a concessão do estatuto de investigador habilitado, os coordenadores dos serviços digitais são incentivados a desenvolver um método de trabalho coerente e coordenado, incluindo critérios operacionais comuns, no quadro do Comité Europeu dos Serviços Digitais.

(11) A fim de simplificar os procedimentos da formulação de pedidos fundamentados, todos os coordenadores dos serviços digitais de estabelecimento devem ser obrigados a verificar se determinados elementos comuns do processo de acesso aos dados foram devidamente cobertos pelos pedidos de acesso. Para o efeito, os coordenadores dos serviços digitais de estabelecimento devem verificar se todos os investigadores requerentes mencionados no pedido de acesso aos dados demonstraram a sua filiação num organismo de investigação, por exemplo, fornecendo provas documentais de contratos de trabalho ou de qualquer outra forma de associação jurídica com o organismo de investigação. Os coordenadores dos serviços digitais de estabelecimento devem igualmente verificar se os investigadores requerentes demonstraram a sua independência em relação a interesses comerciais, por exemplo, através de uma declaração nesse sentido.

(12) O coordenador dos serviços digitais de estabelecimento deve verificar se o financiamento do projeto de investigação para o qual os dados são solicitados é indicado no pedido de acesso aos dados. As informações fornecidas pelos investigadores requerentes devem incluir pormenores sobre as contribuições, tais como a entidade financiadora, o montante, a natureza e a duração da contribuição, e indicar, nomeadamente, se o financiamento já foi concedido ou se há ainda um pedido de financiamento em avaliação, bem como, se for caso disso, referências pertinentes a projetos financiados pela União. O pedido de acesso aos dados deve também incluir os resultados das avaliações realizadas pela entidade ou entidades financiadoras, caso estes estejam disponíveis.

(13) O coordenador dos serviços digitais de estabelecimento deve verificar se o pedido de acesso aos dados descreve a forma como os dados e o respetivo formato são selecionados, tendo em conta os requisitos em matéria de necessidade e proporcionalidade em relação à finalidade da investigação prevista. Se os dados solicitados estiverem também disponíveis através de outras fontes, o coordenador dos serviços digitais de estabelecimento deve avaliar, tendo em consideração as informações constantes do pedido de acesso aos dados, se a solicitação desses dados incluída no pedido de acesso está devidamente justificada. As justificações possíveis podem incluir provas de má qualidade ou falta de fiabilidade desses dados de outras fontes ou a inadequação do formato em que os mesmos podem ser extraídos de outras fontes para efeitos do projeto de investigação, o que prejudicaria a execução do referido projeto. Os dados que podem ser solicitados para estudar os riscos sistémicos ou a sua atenuação na União poderão evoluir no futuro. Atualmente, incluem, por exemplo, dados relativos aos utilizadores dos serviços, tais como informações sobre perfis, redes de relações, exposição individual a conteúdos e históricos de interações; dados de interação, tais como comentários ou outras formas de interação; dados relativos a recomendações de conteúdo, incluindo os dados utilizados para personalizar as recomendações; dados relativos ao direcionamento de anúncios publicitários e à definição de perfis, incluindo os relativos ao custo por clique e a outras métricas de preços publicitários; dados relativos ao ensaio de novas funcionalidades antes da sua implantação, incluindo os resultados de testes A/B; dados relativos à moderação e governação de conteúdos, tais como dados sobre sistemas e processos algorítmicos ou outros sistemas e processos de moderação de conteúdos, nomeadamente registos de alterações, arquivos ou repositórios que documentem os conteúdos moderados, incluindo contas, bem como dados relativos a preços, quantidades e características de bens ou serviços fornecidos ou intermediados pelo fornecedor de dados.

(14) O coordenador dos serviços digitais de estabelecimento deve verificar se o pedido de acesso aos dados fornece informações suficientes que demonstrem que o investigador é capaz de cumprir os requisitos específicos de confidencialidade, segurança e proteção de dados pessoais no que diz respeito aos dados solicitados, identifica os possíveis riscos decorrentes do acesso e tratamento desses dados para efeitos da investigação e documenta as modalidades de acesso propostas, nomeadamente as condições jurídicas, organizativas e técnicas que serão estabelecidas para minimizar os riscos identificados, por exemplo, através de uma carta de compromisso do organismo de investigação que confirme o acesso a meios passíveis de constituir garantias pertinentes, ou de outros documentos comprovativos.

(15) Sempre que sejam solicitados dados pessoais, o coordenador dos serviços digitais de estabelecimento deve verificar se o pedido de acesso aos dados inclui informações sobre o fundamento jurídico do tratamento de dados pessoais, incluindo de categorias especiais de dados pessoais, se for caso disso, e se esse fundamento jurídico está em conformidade com o artigo 6.º, n.º 1, alínea e) ou f), e, quando aplicável, com o artigo 9.º, n.º 2, alínea g) ou j), do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([3]). Além disso, o coordenador dos serviços digitais de estabelecimento deve verificar se o pedido de acesso aos dados contém indicações suficientes de que os investigadores avaliaram os riscos para a proteção de dados pessoais. Por exemplo, tal pode ser demonstrado por uma avaliação de impacto sobre a proteção de dados, na aceção do artigo 35.º do referido regulamento. A fim de assegurar a possibilidade de acesso a dados pessoais em conformidade com o Regulamento (UE) 2016/679, os coordenadores dos serviços digitais devem ser autorizados a consultar as autoridades de controlo pertinentes estabelecidas nos termos do artigo 51.º do mesmo regulamento, que continuam a ter competência para avaliar o cumprimento do Regulamento (UE) 2016/679.

([3]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(16) De modo a facilitar a formulação do pedido fundamentado e a preservar a integridade das informações constantes do pedido de acesso aos dados, o coordenador dos serviços digitais de estabelecimento deve verificar se este pedido de acesso inclui um resumo. Esse resumo deve apresentar uma síntese das informações que integrarão o pedido fundamentado, publicado no portal de acesso aos dados do RSD, nos casos em que a avaliação do pedido de acesso aos dados leve à formulação de um pedido fundamentado.

(17) A fim de assegurar que as modalidades de acesso determinadas pelo coordenador dos serviços digitais de estabelecimento são adequadas para dar resposta à sensibilidade dos dados específicos solicitados num pedido de acesso aos dados, o coordenador dos serviços digitais de estabelecimento deve efetuar uma avaliação caso a caso, com base nas informações fornecidas no pedido de acesso aos dados. As modalidades de acesso enunciadas no pedido fundamentado devem ser adequadas para cumprir os requisitos de segurança dos dados, confidencialidade dos dados e proteção dos dados pessoais e, ao mesmo tempo, permitir a realização dos objetivos de investigação do projeto. O acesso aos dados pode ocorrer, por exemplo, mediante a transmissão dos dados aos investigadores habilitados através de uma interface adequada e de um armazenamento de dados adequado; a transmissão dos dados e o seu armazenamento num ambiente de tratamento seguro operado pelo fornecedor de dados ou por um terceiro fornecedor a que os investigadores habilitados tenham acesso, mas sem haver lugar à transmissão de dados aos investigadores habilitados, ou outras modalidades de acesso a criar ou facilitar pelo fornecedor de dados. Ao especificar as modalidades de acesso, o coordenador dos serviços digitais de estabelecimento deve igualmente enumerar todas as condições jurídicas, técnicas ou organizativas a que o acesso deve estar sujeito. Nos casos em que o facultamento do acesso envolva uma transferência de dados pessoais para países terceiros ou organizações internacionais, na aceção do capítulo V do Regulamento (UE) 2016/679, as modalidades de acesso deverão também incluir informações sobre a necessidade de criar um mecanismo de transferência adequado, de modo a assegurar que o fornecedor de dados tome as medidas necessárias para dar cumprimento ao referido regulamento.

(18) A fim de assegurar que as modalidades de acesso aos dados sejam adequadas para responder a sensibilidades específicas em termos de proteção de dados, segurança dos dados ou confidencialidade, o coordenador dos serviços digitais de estabelecimento deve, com base nas informações recebidas no pedido de acesso aos dados, poder exigir que o acesso aos dados seja facultado através de ambientes de tratamento seguros. Nesses casos, o coordenador dos serviços digitais de estabelecimento deve assegurar que o ambiente escolhido funciona em conformidade com a tecnologia mais adequada e permite que os investigadores habilitados atinjam os objetivos da sua investigação.

(19) A fim de assegurar a coerência das informações transmitidas pelos coordenadores dos serviços digitais de estabelecimento aos fornecedores de dados, é necessário especificar o conteúdo dos pedidos fundamentados.

(20) A fim de salvaguardar os interesses dos fornecedores de dados, de reduzir a frequência dos pedidos de alteração ao longo do tempo e de facilitar a formulação de pedidos de acesso aos dados pertinentes por parte dos investigadores, o coordenador dos serviços digitais de estabelecimento que emitiu os respetivos pedidos fundamentados deve disponibilizar ao público, no portal de acesso aos dados do RSD, uma síntese de cada pedido fundamentado, incluindo as suas eventuais alterações e atualizações.

(21) A fim de assegurar que o coordenador dos serviços digitais de estabelecimento dispõe das informações pertinentes para avaliar um pedido de alteração e de facilitar uma abordagem uniforme na avaliação dos pedidos de alteração, o fornecedor de dados deve ser obrigado a especificar os motivos desse pedido, tal como referido no artigo 40.º, n.º 5, do Regulamento (UE) 2022/2065. Mais especificamente, ao avaliar um pedido de alteração apresentado com base na falta de acesso de um fornecedor de dados aos dados, o coordenador dos serviços digitais de estabelecimento deve estar em condições de analisar se a alegada impossibilidade é devidamente justificada, por exemplo, pela inexistência dos dados solicitados ou por restrições técnicas como a encriptação, e deve dispor das informações necessárias para apurar se a falta de acesso é permanente ou temporária. A este respeito, deve ficar claro que as considerações comerciais não devem ser tidas como motivo para recusar automaticamente o acesso aos dados solicitados, mas antes como motivo para alterar os meios de concessão do acesso aos dados, o que pode resultar na imposição de requisitos adicionais em matéria de confidencialidade e segurança dos dados.

(22) A fim de assegurar uma resolução eficiente de litígios e de incentivar a identificação de uma solução mutuamente aceitável, na sequência de um pedido de alteração, os fornecedores de dados devem poder solicitar aos coordenadores dos serviços digitais de estabelecimento que participem na mediação. Esta participação deve ser voluntária ao longo de todo o processo de mediação e não deve ter qualquer resultado vinculativo para o coordenador dos serviços digitais de estabelecimento, que continua a ter competência para decidir sobre os pedidos de alteração. Todas as partes envolvidas no processo de mediação devem agir de boa-fé e procurar alcançar um acordo justo e mutuamente aceitável.

(23) A fim de evitar que a mediação prolongue indefinidamente o processo de acesso aos dados, a transmissão do pedido escrito de mediação, a escolha do mediador e o próprio processo de mediação devem ter lugar dentro de prazos especificados. Os coordenadores dos serviços digitais de estabelecimento devem fixar um prazo para o processo de mediação relativo a um determinado pedido fundamentado e o mediador deve ter autoridade para encerrar o processo de mediação em circunstâncias específicas.

(24) A fim de manter a confiança mútua entre as partes envolvidas na mediação, o coordenador dos serviços digitais de estabelecimento deve assegurar que o mediador proposto cumpre os requisitos de imparcialidade e independência e possui conhecimentos especializados pertinentes sobre o objeto da mediação.

(25) Para facilitar a tomada de decisões informadas e eficazes em relação ao processo de acesso aos dados, os coordenadores dos serviços digitais devem ter a possibilidade de solicitar pareceres periciais sobre elementos específicos do processo de acesso aos dados, nomeadamente a determinação das modalidades de acesso, incluindo as interfaces adequadas, a formulação do pedido fundamentado e quaisquer pedidos de alteração apresentados pelo fornecedor de dados. Os peritos consultados devem possuir experiência comprovada na matéria sobre a qual é solicitado o seu parecer e ser independentes. Mais concretamente, não devem ter qualquer conflito de interesses decorrente, por exemplo, de ligações aos investigadores requerentes ou ao fornecedor de dados.

(26) A fim de aumentar a transparência e permitir que os coordenadores dos serviços digitais tirem partido dos conhecimentos especializados que adquiriram ao longo do tempo, cada pedido de consulta pericial e o seguimento por ele gerado devem ser registados no AGORA.

(27) A fim de facilitar a supervisão eficaz do cumprimento das condições enunciadas no pedido fundamentado, o fornecedor de dados deve notificar o coordenador dos serviços digitais de estabelecimento no prazo de três dias úteis a contar da data da concessão do acesso aos investigadores habilitados e da data da cessação do acesso.

(28) A fim de permitir que os investigadores habilitados utilizem os dados solicitados para efeitos da investigação e forneçam informações contextuais pertinentes, os fornecedores de dados devem facultar aos investigadores habilitados os metadados e a documentação pertinentes que descrevem os dados disponibilizados, tais como livros de códigos, registos de alterações e documentação arquitetural.

(29) A fim de facilitar uma investigação relevante por parte dos investigadores habilitados, inclusive permitindo a combinação dos dados solicitados com dados disponíveis de outras fontes, os fornecedores de dados não devem impor quaisquer restrições às ferramentas analíticas utilizadas pelos investigadores habilitados, incluindo bibliotecas de *software* pertinentes, nem impor requisitos de arquivo, armazenamento, atualização e supressão, a menos que estejam explicitamente mencionados nas modalidades de acesso identificadas no pedido fundamentado.

(30) Caso os dados fornecidos aos investigadores habilitados incluam dados pessoais, na aceção do artigo 4.º do Regulamento (UE) 2016/679, o fornecedor de dados deve observar as regras estabelecidas nesse regulamento. Mais especificamente, o artigo 40.º, n.º 4, do Regulamento (UE) 2022/2065 cria uma obrigação jurídica, na aceção do artigo 6.º, n.º 1, alínea c), do Regulamento (UE) 2016/679, relativa a qualquer tratamento de dados pessoais necessário para o fornecedor de dados facultar o acesso aos dados especificados no pedido fundamentado. Caso devam ser tratadas categorias especiais de dados pessoais, na aceção do artigo 9.º do Regulamento (UE) 2016/679, o presente regulamento cumpre o requisito previsto no artigo 9.º, n.º 2, alínea g), do Regulamento (UE) 2016/679.

(31) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([4]) e emitiu parecer em 4 de dezembro de 2024.

(32) Após consulta do Comité Europeu dos Serviços Digitais nos termos do artigo 40.º, n.º 13, do Regulamento (UE) 2022/2065 e após a sua aprovação,

ADOTOU O PRESENTE REGULAMENTO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto

O presente regulamento estabelece procedimentos e condições técnicas para facultar aos investigadores habilitados o acesso aos dados na posse de fornecedores de plataformas em linha de muito grande dimensão e de motores de pesquisa em linha de muito grande dimensão, nos termos do artigo 40.º, n.º 4, do Regulamento (UE) 2022/2065, nomeadamente:

a) As condições técnicas para o desenvolvimento e o funcionamento de um portal de acesso aos dados;

b) Os procedimentos e as condições técnicas para a gestão do processo de acesso aos dados por parte dos coordenadores dos serviços digitais e dos fornecedores de dados;

c) Os requisitos relativos à formulação de pedidos fundamentados e à avaliação de pedidos de alteração;

d) As condições técnicas para o facultamento de acesso aos dados pelos fornecedores de dados.

Artigo 2.º

Definições

Para efeitos do presente regulamento, são aplicáveis as definições constantes do artigo 4.º do Regulamento (UE) 2016/679 e do artigo 3.º do Regulamento (UE) 2018/1725. São igualmente aplicáveis as seguintes definições:

1) «Pedido de acesso aos dados», as informações e a documentação pertinente apresentadas pelos investigadores requerentes ao coordenador dos serviços digitais de estabelecimento ou ao coordenador dos serviços digitais do Estado-Membro do organismo de investigação em que o investigador principal está filiado, a fim de obter o estatuto de «investigador habilitado», tal como referido no artigo 40.º, n.º 8, primeiro parágrafo, do Regulamento (UE) 2022/2065, para um projeto de investigação específico que envolva o acesso aos dados de um fornecedor de dados;

2) «Processo de acesso aos dados», as etapas e os procedimentos que podem conduzir ao facultamento do acesso aos dados tal como referido no artigo 40.º, n.º 4, do Regulamento (UE) 2022/2065;

3) «Investigador requerente», qualquer pessoa singular que solicite o acesso aos dados tal como referido no artigo 40.º, n.º 4, do Regulamento (UE) 2022/2065, seja individualmente, em grupo ou como parte de uma entidade;

4) «Investigador principal», o investigador requerente que apresenta o pedido de acesso aos dados a título individual ou em nome de uma entidade ou de um grupo de investigadores requerentes;

5) «Fornecedor de dados», um fornecedor de uma plataforma em linha de muito grande dimensão ou de um motor de pesquisa em linha de muito grande dimensão designado como tal nos termos do artigo 33.º, n.º 4, do Regulamento (UE) 2022/2065 e ao qual pode ser dirigido um pedido fundamentado;

([4]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

6) «Pedido fundamentado», um pedido fundamentado de acesso aos dados nos termos do artigo 40.º, n.º 4, do Regulamento (UE) 2022/2065;

7) «Pedido de alteração», um pedido de alteração nos termos do artigo 40.º, n.º 5, do Regulamento (UE) 2022/2065, apresentado pelo fornecedor de dados ao coordenador dos serviços digitais de estabelecimento após a receção de um pedido fundamentado;

8) «Ambiente de tratamento seguro», um ambiente de tratamento seguro na aceção do artigo 2.º, ponto 20, do Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho ([5]).

CAPÍTULO II

OBRIGAÇÕES EM MATÉRIA DE INFORMAÇÃO E DE CONTACTO

Artigo 3.º

Portal de acesso aos dados do RSD

1. A Comissão cria e aloja um portal de acesso aos dados do RSD.

2. O portal de acesso aos dados do RSD tem as seguintes funções:

a) Apoiar e simplificar a gestão do processo de acesso aos dados para os investigadores, fornecedores de dados e coordenadores dos serviços digitais;

b) Servir de ponto digital central para informações sobre o processo de acesso aos dados e facilitar os intercâmbios de informações nos termos do presente regulamento entre investigadores requerentes, investigadores habilitados, fornecedores de dados e coordenadores dos serviços digitais.

3. O portal de acesso aos dados do RSD deve ser interoperável com o sistema de partilha de informações AGORA, criado pelo Regulamento de Execução (UE) 2024/607. No AGORA, os coordenadores dos serviços digitais têm acesso às informações apresentadas através do portal de acesso aos dados do RSD.

4. Os fornecedores de dados devem ter uma conta no portal de acesso aos dados do RSD.

5. Para participarem no processo de acesso aos dados, os investigadores requerentes devem ter uma conta no portal de acesso aos dados do RSD.

Artigo 4.º

Funções e responsabilidades no tratamento de dados pessoais no portal de acesso aos dados do RSD

1. Os coordenadores dos serviços digitais são responsáveis pelo tratamento distintos no que diz respeito ao tratamento de dados pessoais que efetuam para gerir o processo de acesso aos dados e publicar as informações pertinentes.

2. A Comissão é um subcontratante para os dados pessoais tratados no portal de acesso aos dados do RSD.

3. As responsabilidades da Comissão enquanto subcontratante relativamente às atividades de tratamento de dados realizadas no portal de acesso aos dados do RSD são as estabelecidas no anexo.

([5]) Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho, de 30 de maio de 2022, relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados) (JO L 152 de 3.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

Artigo 5.º

Tratamento de dados pessoais no portal de acesso aos dados do RSD

1. Caso sejam registados dados pessoais no portal de acesso aos dados do RSD, e trocados através do mesmo, o tratamento apenas deve ser efetuado na medida em que seja proporcionado e necessário para efeitos do processo de acesso aos dados e da publicação das informações pertinentes.

2. No portal de acesso aos dados do RSD, só é possível tratar dados pessoais das seguintes categorias de titulares de dados:

a) Pessoas singulares com uma conta no portal de acesso aos dados do RSD;

b) Pessoas singulares cujos dados pessoais constem do portal de acesso aos dados do RSD ou sejam incluídos em qualquer outro intercâmbio de dados relativo ao processo de acesso aos dados efetuado nos termos do presente regulamento.

3. No portal de acesso aos dados do RSD, só é possível tratar as seguintes categorias de dados pessoais:

a) Dados de identificação, tais como nome e a identificação do utilizador;

b) Informações de contacto, tais como o endereço postal, o endereço de correio eletrónico e os dados de contacto;

c) Dados pessoais constantes da documentação que demonstra a filiação num organismo de investigação, bem como outras informações pessoais consideradas necessárias para efeitos de participação no processo de acesso aos dados.

4. O tratamento de dados pessoais a que se refere o n.º 1 deve ser efetuado com recurso a uma infraestrutura informática localizada no Espaço Económico Europeu.

Artigo 6.º

Pontos de contacto e informações públicas sobre o processo de acesso aos dados

1. Cada coordenador dos serviços digitais e cada fornecedor de dados devem criar um ponto de contacto específico com a função de prestar informações e apoio sobre o processo de acesso aos dados.

2. Os coordenadores dos serviços digitais e os fornecedores de dados devem comunicar os seus pontos de contacto à Comissão tão rapidamente quanto possível. A Comissão publica os dados dos pontos de contacto a que se refere o n.º 1 na interface pública do portal de acesso aos dados do RSD.

3. Cada coordenador dos serviços digitais deve disponibilizar e tornar facilmente localizáveis, na sua interface em linha, os dados do ponto de contacto criado nos termos do n.º 1, juntamente com uma hiperligação para o portal de acesso aos dados do RSD.

4. Os fornecedores de dados devem disponibilizar e tornar facilmente localizáveis, nas suas interfaces em linha, as seguintes informações:

a) Os dados do ponto de contacto por eles criado nos termos do n.º 1;

b) Uma hiperligação para o portal de acesso aos dados do RSD;

c) Um catálogo de dados do RSD, que descreva os ativos de dados a que é possível aceder para os fins previstos no artigo 40.º, n.º 4, do Regulamento (UE) 2022/2065, bem como a sua estrutura de dados e os metadados;

d) As modalidades de acesso propostas para os dados constantes do catálogo nos termos da alínea c), adequadas ao nível de sensibilidade dos diferentes ativos de dados.

5. As informações referidas no n.º 4, alíneas c) e d), devem ser atualizadas de forma regular, nomeadamente para refletir os dados relativos às avaliações dos riscos efetuadas nos termos do artigo 34.º do Regulamento (UE) 2022/2065 e às auditorias realizadas nos termos do artigo 37.º do mesmo regulamento.

CAPÍTULO III

REQUISITOS RELATIVOS À FORMULAÇÃO E AO TRATAMENTO DE PEDIDOS FUNDAMENTADOS

Artigo 7.º

Formulação de um pedido fundamentado

1. No prazo de 80 dias úteis a contar da data da apresentação de um pedido de acesso aos dados, o coordenador dos serviços digitais de estabelecimento, tendo em devida conta os pré-requisitos estabelecidos no artigo 8.º e, se for caso disso, qualquer outra avaliação pertinente para o efeito, decide se é possível ou não formular um pedido fundamentado e toma uma das seguintes medidas:

a) Formula um pedido fundamentado, apresenta-o ao fornecedor de dados e notifica o investigador principal da apresentação do pedido fundamentado;

b) Informa o investigador principal dos motivos que não permitem a formulação do pedido fundamentado.

2. Se, em casos devidamente justificados, o coordenador dos serviços digitais de estabelecimento precisar de mais tempo para formular um pedido fundamentado, deve notificar o investigador principal tão rapidamente quanto possível e indicar os motivos do atraso, bem como uma nova data para a tomada das medidas previstas no n.º 1.

Artigo 8.º

Pré-requisitos para a formulação de um pedido fundamentado

O coordenador dos serviços digitais de estabelecimento decide se é possível ou não formular um pedido fundamentado tendo em conta os seguintes elementos:

a) Relativamente a cada investigador requerente:

   i) uma confirmação da filiação num organismo de investigação na aceção do artigo 2.º, ponto 1, da Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho ([6]),

   ii) uma declaração de independência em relação a interesses comerciais pertinente para o projeto específico para o qual os dados são solicitados,

   iii) o compromisso de disponibilizar gratuitamente ao público os resultados da investigação;

b) Informações sobre o financiamento de apoio ao projeto de investigação para o qual os dados são solicitados;

c) Uma descrição dos dados solicitados, incluindo o formato, o âmbito e, sempre que possível, os atributos específicos, os metadados e a documentação dos dados pertinentes, tendo igualmente em conta as informações disponibilizadas nos termos do artigo 6.º, n.º 4, do presente regulamento;

d) Informações sobre a necessidade e a proporcionalidade do acesso aos dados, bem como sobre os prazos da investigação para a qual os dados são solicitados;

e) Informações sobre os riscos identificados, em termos de confidencialidade, segurança dos dados e proteção de dados pessoais, relativos aos dados a que se acederia, uma descrição das medidas técnicas, jurídicas e organizativas que serão aplicadas, incluindo, sempre que possível, as modalidades de acesso propostas, para atenuar esses riscos aquando do tratamento dos dados solicitados;

f) Uma descrição das atividades de investigação a realizar com os dados solicitados;

g) Um resumo do pedido de acesso aos dados, com os seguintes elementos:

   i) o tema da investigação,

   ii) o fornecedor de dados ao qual os dados são solicitados,

   iii) uma descrição dos dados solicitados, tal como referido na alínea c).

([6]) Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE (JO L 130 de 17.5.2019, p. 92, ELI: http://data.europa.eu/eli/dir/2019/790/oj).

Artigo 9.º

Modalidades de acesso

1. O coordenador dos serviços digitais de estabelecimento determina as modalidades, incluindo as medidas técnicas, jurídicas e organizativas, que o fornecedor de dados deve aplicar para facultar o acesso aos dados aos investigadores habilitados.

2. Os coordenadores dos serviços digitais estão autorizados a consultar as autoridades de controlo pertinentes estabelecidas nos termos do artigo 51.º do Regulamento (UE) 2016/679.

3. Ao determinar as modalidades de acesso, o coordenador dos serviços digitais de estabelecimento deve ter em conta as informações fornecidas no pedido de acesso aos dados, em especial as informações referidas no artigo 8.º, alínea e), considerando também os direitos e interesses dos fornecedores de dados e dos destinatários do serviço em causa, nomeadamente a proteção de informações confidenciais e segredos comerciais, e mantendo a segurança do seu serviço e das informações disponibilizadas pelos fornecedores de dados nos termos do artigo 6.º, n.º 4, alínea d).

4. Além dos elementos referidos no n.º 3, o coordenador dos serviços digitais de estabelecimento deve, ao determinar as modalidades de acesso, ter em conta os seguintes elementos:

a) Caso o acesso envolva o tratamento de dados pessoais:

   i) a avaliação dos riscos relativos ao tratamento de dados pessoais descritos no artigo 8.º, alínea e), incluindo, se for caso disso, avaliações de impacto sobre a proteção de dados, na aceção do artigo 35.º do Regulamento (UE) 2016/679,

   ii) as medidas técnicas e organizativas previstas, apresentadas nos termos do artigo 8.º, alínea e);

b) As medidas pertinentes de segurança da rede, a encriptação, os mecanismos de controlo do acesso, as políticas de salvaguarda, os mecanismos de integridade dos dados e os planos de resposta a incidentes;

c) Se for caso disso, informações sobre o período de armazenamento previsto e os planos de destruição de dados pertinentes;

d) Medidas organizativas, nomeadamente processos de revisão interna, restrições dos direitos de acesso e partilha de informações;

e) Cláusulas contratuais propostas, nomeadamente acordos de não divulgação, acordos sobre dados e qualquer outro tipo de declarações escritas, que estabeleçam possíveis condições de acesso e tratamento entre o investigador principal e o fornecedor de dados;

f) A existência de formação sobre segurança dos dados e proteção de dados pessoais ministrada aos investigadores requerentes;

g) A necessidade ou não de ambientes de tratamento seguros para tratar os dados.

5. Se considerar que se deve recorrer a um ambiente de tratamento seguro para facultar o acesso aos dados solicitados, o coordenador dos serviços digitais de estabelecimento deve exigir documentação que comprove que o operador desse ambiente:

a) Especifica as condições de acesso ao ambiente de tratamento seguro, de modo a minimizar o risco de leitura, cópia, alteração ou remoção não autorizada dos dados alojados no ambiente de tratamento seguro;

b) Assegura que os investigadores habilitados acedem apenas aos dados abrangidos pelo pedido fundamentado, através de identidades de utilizador individuais e únicas e de modos de acesso confidenciais;

c) Conserva registos identificáveis de acesso ao ambiente de tratamento seguro durante o período necessário para verificar e auditar todas as operações de tratamento nesse ambiente;

d) Assegura que a capacidade computacional disponibilizada aos investigadores habilitados é adequada e suficiente para os fins do projeto de investigação;

e) Controla a eficácia das medidas enumeradas nas alíneas a) a d).

Artigo 10.º

Conteúdo de um pedido fundamentado

1. Um pedido fundamentado deve incluir, pelo menos, os seguintes elementos:

a) A data em que o fornecedor de dados faculta o acesso aos dados solicitados e a data da cessação desse acesso;

b) As modalidades de acesso determinadas nos termos do artigo 9.º;

c) O resumo do pedido de acesso aos dados a que se refere o artigo 8.º, alínea g).

2. Sempre que tal seja necessário para permitir o acesso aos dados solicitados, em conformidade com as modalidades de acesso especificadas no pedido fundamentado, o coordenador dos serviços digitais de estabelecimento pode incluir no pedido fundamentado os nomes e os dados de contacto de todos os investigadores habilitados mencionados no pedido de acesso aos dados.

3. Se o facultamento do acesso envolver uma transferência de dados pessoais para um país terceiro ou uma organização internacional, na aceção do capítulo V do Regulamento (UE) 2016/679, o pedido fundamentado deve incluir informações sobre a necessidade de criar ou remeter para um mecanismo de transferência adequado para assegurar o cumprimento do Regulamento (UE) 2016/679.

Artigo 11.º

Publicação de uma síntese do pedido fundamentado no portal de acesso aos dados do RSD

1. Após a formulação de um pedido fundamentado, o coordenador dos serviços digitais de estabelecimento deve publicar uma síntese do pedido fundamentado na interface pública do portal de acesso aos dados do RSD. A síntese deve incluir todos os elementos seguintes:

a) O resumo do pedido de acesso aos dados a que se refere o artigo 8.º, alínea g);

b) As modalidades de acesso determinadas nos termos do artigo 9.º.

2. A síntese a que se refere o n.º 1 deve ser atualizada de modo a refletir quaisquer alterações resultantes da modificação de um ou mais elementos na sequência da análise de um pedido de alteração ou do resultado de uma mediação nos termos do artigo 13.º.

Artigo 12.º

Procedimentos de análise dos pedidos de alteração

1. Após a receção de um pedido de alteração nos termos do artigo 40.º, n.º 5, do Regulamento (UE) 2022/2065, o coordenador dos serviços digitais de estabelecimento informa o investigador principal em causa.

2. Ao decidir sobre um pedido de alteração apresentado nos termos do artigo 40.º, n.º 5, alínea a), do Regulamento (UE) 2022/2065, o coordenador dos serviços digitais de estabelecimento deve ter em conta se:

a) Os motivos da alegada falta de acesso aos dados estão devidamente fundamentados;

b) Essa falta de acesso aos dados é permanente ou temporária.

3. Ao decidir sobre um pedido de alteração apresentado nos termos do artigo 40.º, n.º 5, alínea b), do Regulamento (UE) 2022/2065, o coordenador dos serviços digitais de estabelecimento deve ter em conta todos os seguintes aspetos:

a) Se as alegadas vulnerabilidades e a sua importância estão devidamente fundamentadas;

b) A probabilidade e a gravidade dos danos resultantes destas alegadas vulnerabilidades significativas;

c) Em que medida as modalidades de acesso enunciadas no pedido fundamentado atenuam efetivamente o risco de ocorrência de tais danos.

4. Em qualquer momento da avaliação de um pedido de alteração, o coordenador dos serviços digitais de estabelecimento pode solicitar ao fornecedor de dados ou ao investigador principal as informações adicionais que considere necessárias para concluir a sua avaliação.

5. Esse pedido de informações adicionais deve ser apresentado tão rapidamente quanto possível para dar ao fornecedor de dados ou ao investigador principal um tempo de resposta suficiente e, em todo o caso, não deve afetar o prazo fixado no artigo 40.º, n.º 6, segundo parágrafo, do Regulamento (UE) 2022/2065. Caso o fornecedor de dados ou o investigador principal não forneça as informações solicitadas em absoluto ou num prazo especificado pelo coordenador dos serviços digitais de estabelecimento, ou forneça apenas informações parciais, o coordenador dos serviços digitais de estabelecimento toma a sua decisão no prazo estabelecido no artigo 40.º, n.º 6, do Regulamento (UE) 2022/2065, com base nas informações que lhe tenham sido disponibilizadas num prazo razoável.

Artigo 13.º

Mediação

1. Se discordar da decisão do coordenador dos serviços digitais de estabelecimento sobre o pedido de alteração, o fornecedor de dados pode, no prazo de cinco dias úteis a contar da data da comunicação do coordenador dos serviços digitais de estabelecimento nos termos do artigo 40.º, n.º 6, segundo parágrafo, do Regulamento (UE) 2022/2065, solicitar por escrito ao coordenador dos serviços digitais de estabelecimento que participe na mediação.

2. O coordenador dos serviços digitais de estabelecimento não é obrigado a participar no processo de mediação.

3. O pedido escrito a que se refere o n.º 1 deve incluir uma descrição concisa dos elementos específicos da decisão, comunicada pelo coordenador dos serviços digitais de estabelecimento nos termos do artigo 40.º, n.º 6, segundo parágrafo, do Regulamento (UE) 2022/2065, aos quais o fornecedor de dados se opõe.

4. O coordenador dos serviços digitais de estabelecimento e o fornecedor de dados acordam na nomeação de um mediador e dão início à mediação no prazo de vinte dias úteis a contar da data da apresentação do pedido de mediação nos termos do n.º 3.

5. Antes de aceitar a nomeação de um mediador, o coordenador dos serviços digitais de estabelecimento deve verificar se este é imparcial e independente e possui conhecimentos especializados pertinentes sobre o objeto descrito no pedido escrito a que se refere o n.º 1.

6. O fornecedor de dados suporta todos os custos da mediação.

7. O coordenador dos serviços digitais de estabelecimento informa, sem demora injustificada, o investigador principal do pedido de mediação referido no n.º 1 e pode decidir convidar o investigador principal a ser parte na mediação. Se o pedido de acesso aos dados for apresentado ao coordenador dos serviços digitais do organismo de investigação, o coordenador dos serviços digitais de estabelecimento pode convidar o coordenador dos serviços digitais do organismo de investigação a participar no processo de mediação. Qualquer parte que o coordenador dos serviços digitais de estabelecimento convide a participar na mediação não é obrigada a participar no processo de mediação.

8. A participação na mediação não afeta o direito de as partes intentarem processos judiciais em qualquer altura, antes, durante ou depois da mediação.

9. O coordenador dos serviços digitais de estabelecimento fixa um prazo para a mediação, que não pode ir além de 40 dias úteis a contar da data do início da mediação nos termos do n.º 4.

10. O mediador pode antecipar o termo da mediação num dos seguintes casos:

a) Uma das partes solicita explicitamente que seja posto termo à mediação;

b) Fica claro que o comportamento das partes durante a mediação, incluindo a falta de participação de boa-fé, torna improvável a obtenção de um acordo.

11. Se a mediação resultar num acordo entre as partes, o coordenador dos serviços digitais de estabelecimento tem em conta esse acordo e, se for caso disso, altera o pedido fundamentado e informa o investigador principal da alteração.

12. Se as partes não chegarem a acordo, o coordenador dos serviços digitais de estabelecimento notifica o fornecedor de dados de que a decisão do coordenador dos serviços digitais de estabelecimento sobre o pedido de alteração, conforme comunicada pela última vez nos termos do artigo 40.º, n.º 6, segundo parágrafo, do Regulamento (UE) 2022/2065, é considerada válida e constitui a base aplicável às etapas posteriores do processo, e informa o investigador principal.

13. O coordenador dos serviços digitais de estabelecimento regista no AGORA um relatório sumário da mediação, elaborado pelo mediador e assinado por todas as partes. O relatório inclui as seguintes informações:

a) A data do pedido escrito de mediação do fornecedor de dados;

b) A identidade e os dados de contacto das partes;

c) As datas do início e do termo da mediação;

d) O resultado da mediação, incluindo qualquer acordo alcançado ou o motivo do termo da mediação.

Artigo 14.º

Consulta de peritos independentes

1. Antes de formular um pedido fundamentado ou de tomar uma decisão sobre um pedido de alteração, o coordenador dos serviços digitais pode decidir consultar peritos.

2. Os peritos devem ser independentes e imparciais, possuir conhecimentos especializados pertinentes e competências comprovadas e ter a capacidade e os recursos necessários para executar a tarefa identificada, sem demora injustificada.

3. Para atestarem a sua imparcialidade, os peritos devem assinar uma declaração a confirmar que:

a) Não têm ligações financeiras ou pessoais ao fornecedor de dados ou aos investigadores requerentes;

b) Não têm interesse no resultado do processo de acesso aos dados;

c) Estão isentos de quaisquer conflitos de interesses.

4. O coordenador dos serviços digitais deve codificar no AGORA, sem demora injustificada, qualquer consulta realizada nos termos do n.º 1, juntamente com o parecer pericial recebido em resposta à consulta.

CAPÍTULO IV

CONDIÇÕES PARA FACULTAR OS DADOS SOLICITADOS AOS INVESTIGADORES HABILITADOS

Artigo 15.º

Partilha de dados e documentação de dados

1. No prazo de três dias úteis, os fornecedores de dados devem notificar o coordenador dos serviços digitais de estabelecimento de que:

a) Foi facultado aos investigadores habilitados o acesso aos dados solicitados, em conformidade com o pedido fundamentado;

b) Cessou o acesso facultado aos investigadores habilitados.

2. Os fornecedores de dados devem fornecer aos investigadores habilitados todas as informações adicionais necessárias para aceder e compreender os dados solicitados, tais como livros de códigos, registos de alterações e documentação arquitetural. Nos casos em que o fornecimento dessas informações possa resultar na vulnerabilidade significativa dos serviços do fornecedor de dados, este deve notificar o coordenador dos serviços digitais de estabelecimento desse risco e, sempre que possível, propor informações alternativas.

3. Ao facultarem o acesso aos dados, os fornecedores de dados não devem impor aos investigadores habilitados requisitos de gestão de dados, como requisitos de arquivo, armazenamento, atualização e supressão, ou limitações à utilização de ferramentas analíticas normalizadas que possam prejudicar a realização da investigação em causa, a menos que tais requisitos ou limitações estejam explicitamente mencionados no pedido fundamentado.

4. Em caso de tratamento de dados pessoais, os fornecedores de dados não devem impor aos investigadores habilitados quaisquer condições relativas ao tratamento dos dados pessoais partilhados diferentes das especificadas no pedido fundamentado.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Artigo 16.º

Entrada em vigor

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

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

Feito em Bruxelas, em 1 de julho de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO

Responsabilidades da Comissão enquanto subcontratante relativamente às atividades de tratamento de dados realizadas no contexto do portal de acesso aos dados do RSD

1. A Comissão deve criar e garantir uma infraestrutura informática segura e fiável, o portal de acesso aos dados do RSD, em nome dos coordenadores dos serviços digitais, que apoie e simplifique a gestão do processo de acesso aos dados para investigadores, organismos de investigação, fornecedores de dados e coordenadores dos serviços digitais.

2. A fim de cumprir as obrigações que lhe incumbem enquanto subcontratante para os coordenadores dos serviços digitais, a Comissão pode recorrer a terceiros como subcontratantes ulteriores. Nesse caso, os responsáveis pelo tratamento autorizam a Comissão a recorrer a ou a substituir os subcontratantes ulteriores, se necessário. A Comissão deve informar os responsáveis pelo tratamento do referido recurso a subcontratantes ulteriores ou da sua substituição, dando assim aos responsáveis pelo tratamento a oportunidade de se oporem a tais alterações. A Comissão deve assegurar que esses subcontratantes ulteriores cumpram as mesmas obrigações em matéria de proteção de dados estabelecidas no presente regulamento.

3. A Comissão só pode tratar dados pessoais na medida do necessário para:

   a) A autenticação e o controlo de acesso, no que respeita a todos os utilizadores do portal de acesso aos dados do RSD;

   b) A implementação da autorização dos pedidos apresentados pelos utilizadores do portal de acesso aos dados do RSD para criar, atualizar e suprimir quaisquer informações constantes do pedido no portal de acesso aos dados do RSD;

   c) A receção dos dados pessoais a que se refere o artigo 5.º, n.º 3, do presente regulamento carregados pelos utilizadores do portal de acesso aos dados do RSD;

   d) O armazenamento dos dados pessoais no portal de acesso aos dados do RSD;

   e) A supressão dos dados pessoais na respetiva data de expiração ou mediante instrução do responsável pelo tratamento;

   f) Após o termo da prestação dos serviços do portal de acesso aos dados do RSD, a supressão de quaisquer dados pessoais remanescentes, exceto se o direito da União ou dos Estados-Membros exigir o armazenamento de tais dados pessoais.

4. A Comissão deve tomar todas as medidas de segurança mais avançadas a nível organizacional, físico e lógico para garantir o funcionamento do portal de acesso aos dados do RSD. Para esse efeito, a Comissão deve:

   a) Designar uma entidade responsável pela gestão da segurança do portal de acesso aos dados do RSD, comunicar aos responsáveis pelo tratamento os seus dados de contacto e garantir a disponibilidade da mesma para reagir a ameaças à segurança;

   b) Assumir a responsabilidade pela segurança do portal de acesso aos dados do RSD, incluindo mediante a realização regular de testes, avaliações e análises das medidas de segurança.

5. A Comissão deve tomar todas as medidas de segurança necessárias para evitar comprometer o bom funcionamento operacional do portal de acesso aos dados do RSD, incluindo:

   a) Procedimentos de avaliação dos riscos para identificar e estimar as potenciais ameaças ao portal de acesso aos dados do RSD;

   b) Um procedimento de auditoria e revisão para:

      i) Verificar a correspondência entre as medidas de segurança tomadas e a política de segurança aplicável;

      ii) Controlar regularmente a integridade do portal de acesso aos dados do RSD, os parâmetros de segurança e as autorizações concedidas;

      iii) Detetar violações de segurança e intrusões no portal de acesso aos dados do RSD;

iv) Introduzir alterações para corrigir as vulnerabilidades de segurança existentes no portal de acesso aos dados do RSD;

v) Definir as condições de autorização, incluindo a pedido de responsáveis pelo tratamento, e contribuição para a realização de auditorias independentes, incluindo inspeções e revisões de medidas de segurança, sob reserva de condições que respeitem o Protocolo (n.º 7) do Tratado sobre o Funcionamento da União Europeia relativo aos Privilégios e Imunidades da União Europeia;

c) A alteração do procedimento de controlo para documentar e medir o impacto de uma alteração antes da sua introdução e manter os responsáveis pelo tratamento informados de quaisquer alterações que possam afetar a comunicação com o portal de acesso aos dados do RSD e/ou a segurança do mesmo;

d) O estabelecimento de um procedimento de manutenção e reparação para especificar as regras e condições a seguir caso seja necessária a manutenção e/ou reparação do portal de acesso aos dados do RSD;

e) O estabelecimento de um procedimento para incidentes de segurança para definir o sistema de notificação e escalada de incidentes, informar sem demora os responsáveis pelo tratamento afetados, inclusive para que estes notifiquem as autoridades nacionais de controlo da proteção de dados sobre qualquer violação de dados pessoais, e definir um processo disciplinar para lidar com violações de segurança no portal de acesso aos dados do RSD.

6. A Comissão deve tomar as medidas mais avançadas de segurança física e lógica para as instalações que alojam o portal de acesso aos dados do RSD e os controlos de acesso aos dados e à segurança das mesmas. Para esse efeito, a Comissão deve:

a) Aplicar meios de segurança física para estabelecer perímetros de segurança demarcados e permitir a deteção de violações no portal de acesso aos dados do RSD;

b) Controlar o acesso às instalações do portal de acesso aos dados do RSD;

c) Impedir a adição, substituição ou remoção de equipamentos sem a autorização prévia dos organismos competentes designados;

d) Controlar os acessos ao portal de acesso aos dados do RSD e a partir do mesmo;

e) Assegurar a autenticação dos utilizadores do portal de acesso aos dados do RSD que acedem ao mesmo;

f) Em caso de violação de segurança que afete o portal de acesso aos dados do RSD, rever os direitos de autorização relativos ao acesso ao mesmo;

g) Manter a integridade das informações transmitidas por meio do portal de acesso aos dados do RSD;

h) Aplicar medidas de segurança técnicas e organizativas para impedir o acesso não autorizado a dados pessoais no portal de acesso aos dados do RSD;

i) Sempre que necessário, tomar medidas para bloquear o acesso não autorizado ao portal de acesso aos dados do RSD (ou seja, bloquear um local/endereço IP).

7. A Comissão deve:

a) Tomar medidas para proteger o seu domínio, incluindo o corte de ligações, em caso de desvio substancial em relação aos princípios e conceitos de qualidade e segurança;

b) Manter um plano de gestão dos riscos relacionado com a sua área de responsabilidade;

c) Acompanhar, em tempo real, o desempenho de todas as componentes de serviço do portal de acesso aos dados do RSD, elaborar estatísticas regulares e manter registos;

d) Prestar apoio sobre o portal de acesso aos dados do RSD, em inglês, aos utilizadores do mesmo;

e) Apoiar os responsáveis pelo tratamento por meio de medidas técnicas e organizativas adequadas para o cumprimento da obrigação do responsável pelo tratamento de dar resposta a pedidos relativos ao exercício dos direitos dos titulares de dados estabelecidos no capítulo III do Regulamento (UE) 2016/679;

f) Apoiar os responsáveis pelo tratamento fornecendo informações sobre o portal de acesso aos dados do RSD para cumprir as obrigações estabelecidas nos artigos 32.º a 36.º do Regulamento (UE) 2016/679;

g) Assegurar que os dados tratados no portal de acesso aos dados do RSD são ininteligíveis para qualquer pessoa não autorizada a aceder ao mesmo;

h) Tomar todas as medidas pertinentes para impedir o acesso não autorizado a dados pessoais transmitidos por meio do portal de acesso aos dados do RSD;

i) Tomar medidas para facilitar a comunicação entre os responsáveis pelo tratamento;

j) Manter um registo das atividades de tratamento realizadas em nome dos responsáveis pelo tratamento, em conformidade com o disposto no artigo 31.º, n.º 2, do Regulamento (UE) 2018/1725.