Re.Data

Rede para a Gestão de Dados de Investigação

TOOLKIT SOBRE QUESTÕES JURÍDICAS, PROTEÇÃO DE DADOS E LICENÇAS

novembro | 2025

Apoio

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia

Financiamento

PRR Plano de Recuperação e Resiliência | REPÚBLICA PORTUGUESA | Financiado pela União Europeia NextGenerationEU

Autoria:

Nuno David, Iscte – Instituto Universitário de Lisboa

Marta Cordeiro, Iscte – Instituto Universitário de Lisboa

Gabriel Cipriano, Iscte – Instituto Universitário de Lisboa

Clara Boavida, Iscte – Instituto Universitário de Lisboa

Jorge Figueiredo, Universidade do Minho

Cláudia Conceição, Instituto de Higiene e Medicina Tropical, Universidade Nova de Lisboa

Paula Ochôa, Faculdade de Ciências Sociais e Humanas, Universidade Nova de Lisboa

Kevin Gallagher, Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa

Carina Cunha, Iscte – Instituto Universitário de Lisboa

Agradecimentos:

Gostaríamos de expressar o nosso sincero agradecimento a todos os especialistas que participaram no workshop "Questões Jurídicas, Proteção de Dados e Licenças", realizado no dia 16 de outubro de 2025, no Iscte – Instituto Universitário de Lisboa, no âmbito do projeto ***Re.Data****, no qual foi apresentado este Toolkit. O Toolkit beneficiou significativamente das sugestões, revisões e recomendações recebidas no âmbito do workshop e nas semanas seguintes, com contributos de Cecília Aguiar, Cláudia Afonso, Diogo Morais, Elisabete Castela, Graça Canto Moniz, Inês Oliveira, Liliana Paula, Madalena Ramos, Oleksandr Horchak, Paulo Simões Lopes, Pedro Inácio, Pedro Penteado, Raquel Rocha, Rui Godinho e Saul Leite. As suas considerações e perspetivas foram determinantes para reforçar a qualidade, a relevância e a aplicabilidade prática do documento.*

Como citar este documento:

David, N., Cordeiro, M., Cipriano, G., Boavida, C. P., Figueiredo, J., Conceição, M. C., Ochôa, P., Gallagher, K., & Cunha, C. (2025). *Toolkit sobre Questões Jurídicas, Proteção de Dados e Licenças.* Zenodo. https://doi.org/10.5281/zenodo.17632500

PREÂMBULO

Este toolkit foi desenvolvido no âmbito do projeto **Re.Data**, com o objetivo de apoiar investigadores no planeamento dos seus projetos no que diz respeito às obrigações legais associadas à gestão de dados de investigação. Destina-se a projetos que envolvam dados pessoais e cujo tratamento esteja abrangido pelo Regulamento Geral sobre a Proteção de Dados (RGPD – Regulamento (UE) 2016/679) e pela respetiva Lei de Execução nacional (Lei n.º 58/2019, de 8 de agosto). A sua elaboração contou com a colaboração de profissionais de diferentes formações e experiências — incluindo Encarregados de Proteção de Dados (DPO), membros de comissões de ética, investigadores, *data stewards* e juristas —, o que permitiu refletir sobre as tensões recorrentes entre exigências legais, princípios éticos e práticas de investigação no terreno. Esta diversidade de perspetivas procurou contribuir para a criação de um toolkit não apenas juridicamente sólido, mas também útil e prático.

O toolkit foi elaborado a partir da análise da legislação europeia e portuguesa, de documentos institucionais de universidades nacionais e internacionais, bem como de outros recursos existentes na área da gestão de dados de investigação. Identificámos que muitas das abordagens disponíveis são excessivamente técnicas ou densas do ponto de vista jurídico, tornando-se pouco práticas e acessíveis à maioria dos investigadores. Essa constatação reforçou a necessidade de criar uma ferramenta de fácil utilização, orientada para a ação e adaptada ao contexto académico real.

Para essa concretização, o toolkit parte de um conjunto de perguntas sobre as características do projeto de investigação, promovendo uma abordagem contextualizada. Com base nas respostas são apresentadas orientações jurídicas e técnicas, exemplos práticos, modelos e recursos complementares. Ao adotar uma abordagem centrada na investigação, o toolkit pretende promover uma cultura de gestão de dados de investigação mais consciente, informada e alinhada com os princípios legais e da ciência aberta. O seu objetivo é assim apoiar práticas de investigação mais responsáveis, contribuindo para aproximar a complexidade normativa da legislação em vigor à realidade quotidiana dos investigadores nas suas Unidades de Investigação.

Na página seguinte, encontra-se a árvore de decisão que permite explorar os Nós do toolkit. A azul estão identificados os Nós principais e a cinzento, quando necessário, Nós complementares. O utilizador pode percorrer todos os Nós pela ordem ou, em alternativa, clicar diretamente em cada título para ser reencaminhado para o respetivo conteúdo. No final de cada Nó, um navegador permite ao utilizador voltar à árvore inicial, regressar ao Nó anterior ou avançar para o Nó seguinte. Esperamos que este recurso seja claro, acessível e eficaz, tal como foi idealizado desde a sua conceção.

Toolkit sobre questões jurídicas, proteção de dados e licenças

Planeamento da Investigação

Investigação e Pós-investigação

Direitos e Deveres

1. Considere elaborar um plano de gestão de dados

Clarificação de conceitos

Um **Plano de Gestão de Dados (PGD)** é um documento formal que apoia o planeamento e a execução das atividades de gestão de dados num projeto de investigação. Descreve as práticas e métodos aplicados ao longo do ciclo de vida dos dados — desde a recolha, tratamento, armazenamento e partilha, até à sua preservação ou eliminação.

O PGD é frequentemente exigido por entidades financiadoras, mas também se revela útil em projetos não financiados, funcionando como instrumento estruturante para o cumprimento de exigências legais e requisitos éticos.

Importa sublinhar que o PGD abrange dimensões para além da proteção de dados pessoais, como a propriedade intelectual, licenciamento, curadoria digital ou estratégias de reutilização de dados. Este toolkit não tem como objetivo a elaboração de um PGD. Destina-se a apoiar decisões e implementações relacionadas com o tratamento de dados pessoais, com foco nas recomendações éticas e obrigações legais decorrentes da legislação de proteção de dados pessoais, incluindo aspetos de reutilização de dados quando aplicável.

Neste sentido, as orientações práticas aqui apresentadas podem — e devem — alimentar um eventual PGD, sempre que este seja exigido ou adotado como boa prática. O utilizador é incentivado a registar no PGD as decisões tomadas no âmbito da proteção de dados pessoais.

Reconhecendo que o PGD é um documento dinâmico, sujeito a atualizações ao longo do ciclo de vida dos dados, o toolkit recomenda a sua criação e utilização desde o início do projeto, sublinhando o seu valor como prática estruturante. A partir daí, o foco incide exclusivamente na dimensão da proteção de dados pessoais.

Vantagens da criação de um PGD

- Ajuda a estruturar as etapas do ciclo de vida dos dados, desde a preparação da recolha de dados, ao tratamento, armazenamento, preservação e partilha.
- Facilita o planeamento e a documentação relativa ao cumprimento do RGPD e de normas éticas, inclusive aquelas relacionadas com dados sensíveis, nas suas várias dimensões.
- Ajuda a garantir a correta alocação de recursos financeiros, computacionais e humanos às diversas atividades de gestão de dados de investigação, criando potencial para a automação de atividades de gestão de dados.
- Permite monitorizar e validar a veracidade dos factos reportados.
- Define antecipadamente se, como, onde e quando os dados serão partilhados, promovendo a transparência e a ciência aberta.
- Aumenta a qualidade dos dados e dos metadados, criando condições para o cumprimento dos Princípios de Dados **FAIR**, isto é, a produção de dados que são Localizáveis *(**F**indable)*, Acessíveis *(**A**ccessible)*, Interoperáveis *(**I**nteroperable)* e Reutilizáveis *(**R**eusable)*.
- Ajuda a planear a disponibilidade futura dos dados, definindo que dados devem ser preservados, em que formatos, com que documentação e sob que condições de acesso ou restrição, incluindo a possibilidade de eliminação quando apropriado.

Pergunta de controlo

Está a registar as decisões relativas ao tratamento de dados pessoais da sua investigação?

O registo das decisões é essencial e pode — se aplicável — alimentar o seu Plano de Gestão de Dados (PGD).

Se sim, avance para o Nó **Dados Pessoais**, para verificar se o seu projeto envolve dados deste tipo e se o seu tratamento – quer de dados recolhidos junto de pessoas, quer de dados reutilizados (dados secundários) –, cumpre requisitos éticos, obrigações legais e orientações institucionais.

Se não, consulte os requisitos do financiador da sua investigação ou as políticas institucionais aplicáveis. Verifique se existem modelos de PGD disponíveis na sua instituição e avalie se será necessário criar um PGD para o seu projeto.

Ligações úteis:

- Digital Curation Centre. (n.d.). *DMPonline*. Disponível em: https://dmponline.dcc.ac.uk/

- FAIR Data Austria. (2021). Data Management Plan (DMP) in: *Research Data Management Open Educational Resources Collection*. Disponível em: https://fair-office.at/index.php/dmp/?lang=en

- Horizon Europe. (2021). *Data Management Plan Template*. Disponível em: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e502e83f42&appId=PPGMS

- la Caixa Foundation. (n.d.). *Model of the data management plan*. CaixaResearch. Disponível em: https://caixaresearch.org/en/caixaresearch-management-policy-open-access-research-data-management-model

- OpenAIRE. (n.d.). *Argos: Open and FAIR Data Management Planning*. Disponível em: https://argos.openaire.eu/splash/

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para avançar para o nó seguinte – Recolhe dados pessoais? (Nó 2)

2. Recolhe dados pessoais?

Clarificação de conceitos

Idealmente, um projeto de investigação deve procurar evitar a recolha de dados pessoais. Sempre que os objetivos da investigação possam ser atingidos com dados anónimos — isto é, informações que, desde logo no momento da recolha, não permitam a identificação, direta ou indireta, de qualquer pessoa — deve ser essa a abordagem preferencial. Nestes casos, o **Regulamento Geral sobre a Proteção de Dados** (RGPD) não se aplica.

Mas será que os dados que julgamos anónimos o são realmente?

É frequente recolhermos dados que, à primeira vista, parecem não permitir a identificação de ninguém, mas uma análise cuidada ou quando combinados com outros dados, tornam possível identificar participantes. Outras vezes, os dados são inicialmente pessoais e apenas anonimizados numa fase posterior do projeto — o que significa que houve, efetivamente, tratamento de dados pessoais e aplica-se o RGPD.

O que são, então, dados pessoais?

Por dados pessoais entende-se qualquer informação, de qualquer natureza, relativa a uma **pessoa singular identificada ou identificável** – designada o *titular dos dados*. Neste Toolkit, aplicado a projetos de investigação científica, o termo titular dos dados é frequentemente referido como *o participante*.

É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular (Artigo 4.º, n.º 1 do RGPD).

O regime de proteção de dados aplica-se independentemente do formato ou suporte da informação, seja ele digital ou físico (como gravações áudio, imagens, formulários em papel ou bases de dados eletrónicas).

Por *tratamento de dados pessoais* entende-se qualquer operação efetuada sobre esses dados pessoais, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, a disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição (Artigo 4.º, n.º 2 do RGPD).

É importante compreender que a identificação de uma pessoa pode resultar da combinação de diferentes dados — mesmo que nenhum deles, isoladamente, permita essa identificação. Sempre que uma informação, em conjunto com outras, possa singularizar uma pessoa e estabelecer uma ligação com a sua identidade, essa informação deve ser tratada como dado pessoal.

Se a informação disser respeito a pessoas singulares e não for possível excluir com segurança a possibilidade de identificação, ela deve ser considerada um dado pessoal, aplicando-se-lhe o RGPD.

Importa clarificar que o facto de um estudo não apresentar resultados individualizados dos participantes não significa necessariamente que não está a tratar dados pessoais. O tratamento existe sempre que o investigador tenha acesso, mesmo que temporário, a dados que permitam identificar direta ou indiretamente os participantes — por exemplo, durante a recolha, transcrição ou análise dos dados.

Assim, os dados pessoais devem ser tratados como tal até ao momento em que sejam eliminados, ou efetiva e irreversivelmente anonimizados. A *anonimização* consiste na transformação dos dados de forma irreversível, de modo que não exista qualquer possibilidade de reidentificação dos titulares, ou que essa possibilidade seja negligenciável.

Se essa transformação ocorrer numa fase posterior da recolha de dados no projeto — como, por exemplo, na limpeza de transcrições ou na transferência para uma base de dados a anonimizar — então tanto os dados originais como os dados transformados continuam a ser considerados pessoais, estando sujeitos a todas as obrigações previstas no RGPD até que a anonimização esteja concluída.

Quando se considera concluída a anonimização?

Considera-se a anonimização concluída apenas quando todos os requisitos definidos no Nó **Anonimização** forem cumpridos. Um desses requisitos estabelece que a anonimização só é efetiva após a desvinculação definitiva dos dados originais – o que, na maioria dos casos apenas se concretiza com a sua **eliminação**. Enquanto os dados originais existirem e puderem ser associados aos dados resultantes do processo de anonimização, o conjunto deve ser considerado, no máximo, pseudonimizado. Os critérios e salvaguardas aplicáveis à pseudonimização são detalhados no Nó **Pseudonimização**.

Exemplos

Exemplo 1: Num estudo longitudinal são pedidos dados de identificação e de contacto que permitem relacionar os vários questionários a realizar ao longo do tempo. Mesmo que as respostas aos questionários não contenham outros identificadores, todas as respostas do questionário são consideradas dados pessoais, pois dizem respeito a pessoas identificadas.

Exemplo 2: O nível de detalhe com que se recolhem dados sociodemográficos pode originar a criação inadvertida de identificadores indiretos. Um exemplo clássico é a combinação de código postal e data de nascimento: quando recolhidos com precisão elevada, têm elevada probabilidade de ser atribuíveis a uma pessoa. Nestes casos, os dados são considerados pessoais, mesmo na ausência de nomes ou contactos.

Exemplo 3: Numa entrevista semiestruturada, pode acontecer que os participantes não sejam diretamente identificados (por exemplo, não se recolhe o nome ou contacto). Ainda assim, as respostas podem conter informação identificável (referências a locais, cargos, eventos, etc.), o que caracteriza esses dados como pessoais. Além disso, mesmo que as respostas sejam genéricas, o simples facto de o suporte ser um registo de voz já torna os dados pessoais, pois a voz é um identificador biométrico capaz de identificar um titular.

Exemplo 4: O retrato físico de uma pessoa (fotografia, vídeo ou imagem) e o registo de voz são dados pessoais, por permitirem a identificação do titular. Como tal, estão sujeitos às regras de proteção de dados desde o momento da recolha.

Exemplo 5: Num estudo quantitativo conduzido por uma instituição, são recolhidos dados pessoais contendo identificadores indiretos — como idade, profissão e localização — cuja combinação pode tornar uma pessoa identificável. Enquanto os dados originais forem conservados pela instituição, mantém-se aplicável o regime de proteção de dados pessoais, mesmo que esteja prevista a sua anonimização posterior. Assim, todos os dados devem ser tratados como pessoais até à desvinculação completa dos dados originais, o que, em regra, implica a eliminação dos dados brutos originais.

Perguntas de controlo

A sua investigação envolve o tratamento de dados pessoais?

Questões para verificação:

1. **A informação não é relativa a pessoas?**
   Se não é, então não são dados pessoais.

2. **A informação inclui dados ou combinação de dados, suficientemente específicos para permitir identificar a pessoa a que respeitam, direta ou indiretamente?**
   Se sim, então são dados pessoais.

3. **A investigação baseia-se na análise de aspetos particulares da vida dos participantes, sendo provável que, no seu conjunto, essas circunstâncias sejam únicas para alguns deles?**

Se sim, então são dados pessoais.

4. **Os dados com que trabalha não permitem, por si só, identificar as pessoas a que dizem respeito, mas…**
   a. … existem dados adicionais na sua instituição que, em conjunto com os dados a que tem acesso, permitiriam identificar essas pessoas — mesmo que não tenha acesso direto a esses dados adicionais?
   b. … **ou** tem acesso a dados públicos ou a dados de outras fontes que, quando combinados com os dados com que trabalha, tornam possível identificar as pessoas em causa?

   Se sim, então são dados pessoais.

Se concluiu que trata dados pessoais, siga para o Nó **Responsáveis e Fontes de Dados**.

Se concluiu que não está a tratar dados pessoais, o RGPD não se aplica ao seu projeto.

No entanto, deve ter um grau elevado de confiança de que nenhuma pessoa é identificável, mesmo de forma indireta ou por combinação com outras fontes. Essa exigência torna-se particularmente relevante quando os dados são de natureza sensível (por exemplo, relativos à saúde, etnia, religião, orientação sexual, infrações ou condenações penais). Além disso, quando os dados não sejam considerados pessoais, deve:

- garantir que a obtenção dos dados respeitou princípios éticos (e.g., consentimento, legitimidade da fonte);
- avaliar potenciais riscos éticos para os participantes e informá-los dos mesmos;
- implementar medidas de mitigação, como controlo de acessos, exclusão de variáveis sensíveis ou revisão por comissões de ética, quando aplicável.

Ligações úteis:

- Artigo 4.º, n.º 1 do RGPD Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#art_4

- Article 29 Data Protection Working Party. (2007). *Opinion 4/2007 on the concept of personal data (WP 136)*. European Commission. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

- Regulamento Geral sobre a Proteção de Dados. (2016). *Considerando 26*. Disponível em: https://gdpr-text.com/pt/read/recital-26/

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Considere elaborar um plano de gestão de dados (Nó 1)

Carregue aqui para avançar para o nó seguinte – Identificação dos responsáveis pelo tratamento e as fontes dos dados (Nó 3)

3. Identifique os responsáveis e as fontes dos dados

Clarificação de conceitos

A forma como os dados pessoais são obtidos num projeto de investigação científica — diretamente junto dos participantes, através de terceiros, por fontes públicas ou provenientes de projetos anteriores — implica diferentes obrigações legais e éticas. Neste Nó, deve identificar os diversos conjuntos de dados que pretende utilizar ao longo da sua investigação e registar, para cada um, o respetivo responsável pelo tratamento e a fonte dos dados.

O **responsável pelo tratamento é a instituição** que determina a finalidade e os meios do tratamento desses dados, sendo, geralmente, a instituição onde o projeto está sediado. Contudo, se a definição da finalidade e dos meios for partilhada com outras instituições, há mais do que uma instituição responsável, configurando-se uma situação de **responsabilidade conjunta**.

As fontes de dados enquadram-se, frequentemente, nas seguintes categorias:

1. **Dados recolhidos diretamente junto dos participantes**

   Por exemplo, dados fornecidos pelos próprios participantes, através de entrevistas ou questionários realizados após a prestação do consentimento informado.

2. **Dados secundários, isto é, obtidos em projetos anteriores, em bases de dados institucionais ou de outras instituições, e posteriormente reutilizados para finalidades distintas daquelas que motivaram a sua recolha inicial.**

   Estes dados são geralmente designados, em investigação científica, como *dados secundários*.[1] **Qualquer reutilização de dados para uma finalidade diferente da original – mesmo no âmbito de um mesmo projeto – ou a sua utilização noutro projeto, constitui uma nova finalidade de tratamento**. Isto é verdade mesmo que os objetivos científicos dos dois projetos aparentem ser idênticos e inclui cenários como o envolvimento de uma nova equipa, critérios de inclusão/exclusão diferentes, novas questões de investigação, ou a combinação com outras fontes de dados. Por este motivo, tais dados devem ser sempre classificados como dados secundários.

   Existem duas situações distintas:

   2.1 Dados secundários cedidos por outra instituição:

   Quando a base legal do tratamento no projeto inicial não tiver sido o consentimento dos participantes, deve celebrar um protocolo de transferência entre a instituição de origem e a que irá proceder ao novo tratamento, assegurando a legitimidade da transferência e da nova finalidade. Esse protocolo pode limitar-se à transferência ou, quando aplicável, regular também a **responsabilidade conjunta** pelo tratamento, nos termos do artigo 26.º do RGPD. No caso de transferências entre entidades públicas, o protocolo é obrigatório.

[1] European Data Protection Supervisor (EDPS) (2020). Opinion 3/2020 on the European strategy for data and the European Research Area – scientific research and data protection. Brussels, 6 January 2020. Disponível em: https://www.edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf

Quando a base legal do tratamento no projeto inicial tiver sido o consentimento dos participantes, e o *formulário de consentimento* contemplar também o consentimento específico para a utilização dos dados noutro projeto, incluindo a transferência para outra instituição, a celebração de protocolo pode não ser juridicamente exigida. Ainda assim, é recomendável a sua adoção, a fim de clarificar responsabilidades e salvaguardas. Nos casos que envolvam **dados sensíveis** ou outros **fatores críticos de risco,** a celebração do protocolo poderá ser não apenas recomendável, mas obrigatória.

Finalmente, **se o formulário de consentimento inicial não tiver previsto a utilização dos dados noutro projeto**, deverá ser obtido novo consentimento dos participantes, específico para a nova finalidade, sendo obrigatório a celebração de um protocolo entre as instituições envolvidas.[2]

Em qualquer dos casos, deve ser consultado o serviço competente nos domínios jurídico e de investigação da instituição para apoiar a análise da situação específica, a elaboração e a celebração do protocolo.

2.2 Dados secundários com origem na mesma instituição:

Quando os dados são reutilizados por outro projeto dentro da mesma instituição, é necessário garantir a legitimidade dessa reutilização. A forma mais comum de a assegurar é ter previsto, no formulário do consentimento do projeto inicial, a possibilidade de os participantes consentirem em que os seus dados sejam utilizados também no outro projeto, indicando as condições aplicáveis. Na ausência desse consentimento específico, deve ser avaliada a possibilidade de obter novo consentimento dos participantes. Caso tal não seja exequível, recomenda-se consultar o serviço competente em matéria jurídica e de investigação da instituição, a fim de avaliar a possibilidade de invocar uma base legal alternativa.[3] Sem base legal válida ou novo consentimento, a reutilização dos dados não é permitida.

3. Informações pessoais obtidas a partir de fontes públicas

Alguns estudos poderão recorrer a dados pessoais disponíveis em fontes acessíveis ao público — como websites institucionais, portais web, bases de dados, registos públicos ou plataformas online públicas. O facto de uma informação pessoal estar disponível publicamente (por exemplo, o nome de um docente numa página universitária ou um comentário numa rede social) não lhe retira o estatuto de dado pessoal, e o RGPD continua a ser aplicável. A reutilização de dados publicamente acessíveis configura também uma forma de utilização secundária de dados. É permitida para fins de investigação científica, desde que sejam cumpridas as obrigações legais aplicáveis, a serem desenvolvidas no Nó **Dever de informação** ao participante

Exemplos

Exemplo 1: Dados recolhidos diretamente junto dos participantes

Um projeto de investigação sobre saúde mental em estudantes universitários é desenvolvido por uma equipa sediada numa universidade. Os dados são recolhidos diretamente junto dos participantes, os estudantes dessa universidade, por meio de entrevistas. A universidade onde o projeto está alojado é a responsável pelo tratamento dos dados, uma vez que define a finalidade e os meios de recolha e análise.

---

[2] Nota técnica – Uma solução alternativa, de carácter excecional, poderá considerar a adoção de uma base legal diferente do consentimento para o novo tratamento. Nesse caso, aplica-se o regime do tratamento posterior (art. 6.º, n.º 4 do RGPD), que exige uma avaliação de compatibilidade de finalidades e o cumprimento das garantias adequadas previstas no art. 89.º para investigação científica. Esta via deve ser entendida como último recurso, devidamente fundamentada e acompanhada de medidas reforçadas de mitigação de risco, dado o impacto potencial sobre os direitos dos participantes — nomeadamente, a perda do direito de retirada. Nessas situações, a celebração do protocolo de transferência é obrigatória, a consulta ao Encarregado de Proteção de Dados (EPD) é altamente recomendável, e, consoante o nível de risco (volume, sensibilidade ou contexto dos dados), a formalização da Avaliação de Impacto sobre a Proteção de Dados (AIPD) poderá ser recomendável ou mesmo obrigatória (art. 35.º).

[3] Nota técnica – Mas ver nota de rodapé anterior, relativa à adoção excecional de uma nova base legal e à avaliação de compatibilidade de finalidades (ponto 2.1).

Exemplo 2: Dados secundários obtidos de outra equipa de investigação

Uma investigadora pretende reutilizar uma base de dados existente sobre práticas desportivas em adolescentes, previamente recolhida por outro grupo da mesma instituição. Embora os dados tenham sido inicialmente tratados por uma equipa distinta e para uma finalidade diversa, a reutilização ocorre no âmbito da mesma universidade. Neste caso, a universidade mantém-se como responsável pelo tratamento dos dados, sendo necessário verificar se a nova utilização é legítima e devidamente autorizada. O ideal seria que o consentimento inicial tivesse previsto a possibilidade de utilização dos dados no novo projeto. Não sendo esse o caso, deve ser obtido novo consentimento específico dos participantes antes da reutilização, assegurando que são claramente informados sobre as novas finalidades e condições de tratamento.

Exemplo 3: Dados secundários obtidos de outra instituição

Uma equipa de investigação planeia utilizar dados sobre internamentos hospitalares cedidos por um hospital parceiro. Os dados foram recolhidos originalmente para fins clínicos e serão agora reutilizados para investigação. Neste caso, a responsabilidade pelo tratamento é partilhada entre a instituição de investigação e o hospital, desde que ambas determinem conjuntamente as finalidades e os meios essenciais do novo tratamento. A transferência dos dados e as condições da sua reutilização devem ser formalizadas através de acordo de responsabilidade conjunta, que estabeleça as respetivas obrigações e garantias de proteção dos dados pessoais.

Exemplo 4: Dados obtidos de fontes públicas

Um grupo de investigadores analisa comentários públicos de pessoas identificáveis, sobre políticas ambientais, publicados em fóruns online e páginas de redes sociais abertas. Os dados são recolhidos a partir de fontes públicas acessíveis sem necessidade de autenticação. A instituição à qual pertence a equipa investigadora é a responsável pelo tratamento, pois determina os objetivos e os meios de recolha e análise. Apesar de os dados serem publicamente acessíveis, a sua reutilização continua sujeita às obrigações do RGPD.

Perguntas de controlo

Responsável pelo tratamento

1. Qual é a instituição que define a finalidade e os meios de tratamento dos dados no âmbito deste projeto?

2. O projeto é desenvolvido em parceria com outras instituições? A mera presença de investigadores de diferentes instituições na equipa não determina, por si só, uma situação de responsabilidade conjunta, mas é um forte indício. Se essas instituições colaboram na definição da finalidade e dos meios de tratamento dos dados, configura-se uma situação de responsabilidade conjunta.

Fontes dos dados

1. **Os dados pessoais serão recolhidos diretamente junto dos participantes?**
2. **Ou trata-se de dados secundários, isto é, reutilizados de projetos anteriores e, portanto, para outras finalidades?**

- No projeto inicial, os dados foram recolhidos com base em consentimento?
  - Em caso afirmativo, verificou se o formulário de consentimento original incluía a previsão de consentimento específico para a utilização dos dados no âmbito desse outro projeto? Na ausência desse consentimento, os dados não podem ser reutilizados, a menos que seja obtido novo consentimento junto dos participantes.

- Se no projeto inicial os dados não foram recolhidos com base em consentimento:
  - Assegurou que existem documentos ou políticas institucionais, ou protocolos ou contratos com outras entidades, que documentem e assegurem a legitimidade jurídica da sua reutilização para a nova finalidade?

Por exemplo, a reutilização, por parte de uma universidade, de dados clínicos de pacientes de um hospital exige a celebração de protocolo prévio que regule a transferência desses dados para a universidade. Além disso, implica, nos termos do artigo 7.º da Lei n.º 26/2016 (Regime de Acesso à Informação Administrativa e Ambiental e de Reutilização dos Documentos Administrativos), a recolha do consentimento dos pacientes para essa nova finalidade.

- Quando os dados são obtidos de outra instituição, qualquer que seja a base legal para a reutilização, foi celebrado um protocolo de transferência ou partilha de dados?

3. Os dados serão obtidos a partir de fontes públicas (ex: websites, redes sociais, registos públicos)?

- Essas fontes são efetivamente acessíveis ao público, por qualquer pessoa, sem condições ou autorização necessária para reutilização?
- Está prevista a garantia do dever de informação, mesmo tratando-se de dados publicamente acessíveis?

Identifique e registe no PGD os responsáveis pelo tratamento e as fontes de dados associadas a cada conjunto de dados.

Se pretender reutilizar dados recolhidos no âmbito de um projeto inicial cuja base legal tenha sido o consentimento, é crucial assegurar que o formulário de consentimento desse projeto inicial incluía um consentimento específico para a utilização dos dados no outro projeto. Na ausência desse consentimento, a reutilização exige a obtenção de novo consentimento **antes** de iniciar o tratamento. Consulte o Nó Dever de Informação e Consentimento.

Se os dados pessoais forem fornecidos por outra instituição, deve ser celebrado um **protocolo** entre a instituição que detém os dados e aquela que irá proceder ao seu tratamento. Contacte o serviço competente no domínio jurídico e de investigação da sua instituição, tendo em vista a análise da situação específica, a formulação e a celebração do protocolo.

Caso exista mais do que uma instituição a determinar conjuntamente as finalidades e os meios do tratamento, é igualmente necessário celebrar um protocolo. Neste caso, siga para o Nó Responsabilidade Conjunta.

Em seguida, avance para o Nó Minimização de Dados.

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Recolhe dados pessoais? (Nó 2)

Carregue aqui para avançar para o nó seguinte – Avaliação da existência de responsabilidade conjunta (Nó 3a))

Carregue aqui para saltar diretamente para o nó da minimização de dados (Nó 4)

3a). Avalie a existência de responsabilidade conjunta

Clarificação de conceitos

Quando duas ou mais entidades — geralmente pessoas coletivas, como instituições de ensino superior, centros de investigação ou organismos públicos ou privados — determinam em conjunto as finalidades e os meios (materiais e humanos) de um tratamento de dados pessoais, verifica-se uma situação de responsabilidade conjunta. Este tipo de responsabilidade é comum, por exemplo, quando há transferência ou partilha de dados pessoais entre instituições no âmbito de projetos de investigação conjuntos.

Desde que as instituições envolvidas participem na definição dos objetivos (fins) e dos métodos (meios) usados para tratar os dados pessoais existe responsabilidade conjunta, não obstante não ser necessário que todas as instituições envolvidas tenham igual acesso ou controlo sobre os dados, podendo, inclusivamente, uma das instituições envolvidas não ter qualquer acesso aos dados.

Havendo responsabilidade conjunta, as instituições devem determinar, por acordo, as respetivas responsabilidades pelo cumprimento do RGPD. Deve ainda ser tido em conta que o grau de envolvimento e responsabilidade de cada entidade pode variar, pelo que o acordo deve refletir essa repartição concreta de funções e obrigações. Nesse acordo – cuja sua essência deve ser acessível para os titulares de dados – tem de ficar vertido quem tem a responsabilidade por assegurar o exercício dos direitos dos titulares dos dados e quem tem o dever de fornecer as informações referidas nos artigos 13.º e 14.º do RGPD.

Artigos do RGPD relevantes: 4º/alínea 7), 5º/n.º 2, 6º/n.º 3, 24º, 25º e 26º.

Exemplos

Exemplo 1: Numa parceria formalizada entre duas instituições para um projeto de investigação, um investigador de uma dessas instituições conduz entrevistas para a recolha de depoimentos, enquanto um investigador da outra instituição procede à transcrição e tradução dessas entrevistas. Ambos participam ativamente nas decisões relativas ao questionário das entrevistas e às ferramentas tecnológicas a utilizar na recolha e tradução dos dados. Neste cenário, verifica-se uma determinação conjunta dos meios ou dos fins do tratamento, configurando uma situação de responsabilidade conjunta entre as duas instituições.

Exemplo 2: Um hospital colabora com uma universidade num projeto para estudar a relação entre genética e determinadas doenças. O projeto inclui a recolha de amostras biológicas (sangue, ADN) e dados clínicos dos pacientes, efetuado por técnicos e médicos do hospital e inclui a análise genética e estatística realizada por investigadores da universidade, com vista à publicação de resultados científicos. Se ambas as instituições definem quais os dados que serão recolhidos, como serão armazenados, quem a eles terá acesso, para que projeto de investigação científica serão usados ou quais os meios a usar (laboratórios, software de análise de dados, consentimento informado), existe responsabilidade conjunta.

Exemplo 3: Uma universidade e uma empresa tecnológica desenvolvem em conjunto uma aplicação móvel destinada ao acompanhamento remoto de doentes crónicos. Ambas as entidades decidem em conjunto quais os dados a recolher, para que finalidades, como serão tratados e que funcionalidades a app deve ter. A recolha e o armazenamento dos dados são efetuados exclusivamente pela universidade. A empresa tecnológica, embora sem acesso aos dados pessoais, participa ativamente no desenho da arquitetura e desenvolvimento técnico do sistema com base em decisões conjuntas. Apesar de só a universidade ter acesso aos dados, ambas determinam conjuntamente as finalidades e os meios do tratamento, pelo que são corresponsáveis pelo tratamento.

Exemplo 4: Uma doutoranda está inscrita num curso de doutoramento da Universidade de Lisboa. Tem uma orientadora interna desta universidade e uma coorientadora externa da Universidade do Minho. O curso é exclusivamente gerido pela Universidade de Lisboa e o projeto de investigação aprovado exclusivamente por esta universidade. Ambos os investigadores atuam como orientadores científicos, mas, em última análise, a decisão sobre o tratamento é institucional, e única, em sede da Universidade de Lisboa. Neste caso, **não há** responsabilidade conjunta. A única responsável pelo tratamento é a universidade onde decorre o doutoramento.

Perguntas de controlo

1 – Quem aprova, institucionalmente, por que razão os dados pessoais vão ser tratados? Uma só instituição ou mais do que uma?

2 – Quem determina como (com que ferramentas, processos, recursos humanos) os dados são tratados? Uma só instituição em exclusividade ou também outras instituições?

3 – Existe colaboração ativa entre investigadores de instituições diferentes na conceção do tratamento dos dados (por exemplo: participantes, categorias de dados, formas e prazos de retenção, recursos utilizados) e essa colaboração traduz-se numa influência efetiva de ambas as instituições sobre essas decisões?

Se a resposta for sim a qualquer uma das três perguntas, **existe responsabilidade conjunta entre as instituições.**

4 – O tratamento de dados pessoais resulta em benefícios científicos ou institucionais para mais do que uma entidade, e essas entidades estão de alguma forma envolvidas no tratamento?

Se sim, é muito provável que exista responsabilidade conjunta, devendo a situação ser esclarecida à luz da influência efetiva das instituições nas finalidades e meios do tratamento dos dados.

5 – Duas instituições tratam dados pessoais e uma das instituições age apenas segundo instruções documentadas de outra, sem participar nas decisões sobre finalidades ou meios essenciais?

Se uma das instituições não participa nas decisões, **não há responsabilidade conjunta**, pois apenas uma das instituições define as finalidades e meios, tratando-se de uma relação de **subcontratação**, que deve igualmente ser formalizada em acordo. Nesse caso consulte o Nó **Subcontratação**.

Se há responsabilidade conjunta, as instituições envolvidas devem celebrar um acordo de responsabilidade conjunta, nos termos do artigo 26º do RGPD. Para tal, o investigador deve contactar o serviço competente no domínio jurídico e de investigação da sua instituição, a fim de promover a celebração do referido acordo entre as instituições. Consulte as **Orientações para minuta de acordo de responsabilidade conjunta.**

Ligações úteis:

- European Data Protection Board. (2021). *Orientações 07/2020 sobre os conceitos de responsável pelo tratamento e subcontratante no RGPD.* Disponível em: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_pt.pdf

- Court of Justice of the European Union. (2018). C-25/17 - Jehovan todistajat. GDPRhub. Disponível em: https://gdprhub.eu/index.php?title=CJEU_-_C-25/17_-_Jehovan_todistajat

Orientações para minuta de acordo de responsabilidade conjunta

NOTA: Esta minuta é um template orientador, de caráter indicativo. A sua utilização deve ser precedida de consulta ao departamento jurídico da instituição, para análise da situação concreta. Cada acordo de responsabilidade conjunta pode ter especificidades próprias, pelo que este documento não substitui a avaliação técnica e jurídica necessária.

Objeto	Este Acordo deve ser usado quando duas ou mais entidades, geralmente pessoas coletivas, determinam conjuntamente, as finalidades e os meios materiais e humanos de um tratamento de dados pessoais. Este Acordo deve estabelecer os fins para os quais essas entidades podem tratar os dados pessoais; deve indicar os procedimentos que devem seguir, bem como determinar as respetivas responsabilidades, de forma transparente.
Legislação	Artigo 26º do Regulamento Geral de Proteção de Dados Pessoais
Conteúdo típico	O conteúdo típico de um Acordo de Responsabilidade Conjunta é o seguinte: - Identificação das entidades que são partes no acordo, designadamente: nome, morada, número de identificação de pessoa coletiva; - Identificação das finalidades do tratamento, o que significa, a título de exemplo: a identificação do projeto de investigação e das tarefas nele compreendidas que implicam o tratamento de dados pessoais; - Identificação dos dados pessoais que irão ser objeto de tratamento; - Identificação da base de licitude determinada em conjunto pelas partes para o seu tratamento, por referência às bases de licitude constantes do n.º 1 do artigo 6º do RGPD e, quando aplicável, do artigo 9.º do RGPD.; - Identificação das medidas técnicas e organizativas que as partes determinaram em conjunto que fossem implementadas para proteger a confidencialidade dos dados pessoais que irão ser tratados; - Identificação das funções e obrigações que cada uma das entidades assume, conjunta e individualmente, com especial destaque para as obrigações devidas para com os titulares de dados visados constantes dos artigos 13º e 14º do RGPD; - Identificação de eventuais **subcontratantes**; - Identificação dos contatos das partes (e-mail ou morada) para poderem ser contactadas pelos titulares dos dados para o exercício dos seus direitos e para poderem ser contactadas pela Autoridade de Controlo (sendo que o acordo pode designar um ponto de contacto preferencial para os titulares dos dados). - Identificação do modo de resposta a um incidente de violação de dados pessoais, designadamente, como vão as partes colaborar na investigação da violação, na adoção das medidas corretivas, bem como na notificação à autoridade de controlo competente e aos titulares de dados; - Identificação do Encarregado de Proteção de Dados de cada uma das entidades; - Lei aplicável e foro competente.
Divulgação	A essência do acordo deve ser disponibilizada aos titulares dos dados. Esta informação poderá ser disponibilizada, por exemplo, na página do projeto na internet.
Modelo	A Comissão Europeia não impõe um modelo único de acordo de responsabilidade conjunta.
Âmbito de aplicação	Esta ficha de orientação é adequada para acordos a celebrar por entidades com domicílio no Espaço Económico Europeu (EEA).
Países Terceiros	Os acordos com entidades de países terceiros à União Europeia devem cumprir com o disposto no capítulo V do RGPD. Consulte o nó **Transferências Internacionais**.

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Identificação dos responsáveis pelo tratamento e as fontes dos dados (Nó 3)

Carregue aqui para avançar para o nó seguinte – Planeamento da minimização dos dados (Nó 4)

4. Planeie a minimização dos dados

Clarificação de conceitos

Certamente já participou em estudos ou preencheu formulários que pediam uma quantidade excessiva de informação pessoal — muitas vezes, sem perceber porquê. É natural que se pergunte a si mesmo: “Mas para que precisam de saber tudo isto?”

De facto, há situações em que se recolhem várias categorias de dados pessoais sem que exista uma necessidade real para tal. Estas práticas são inadequadas — e, por vezes, até abusivas — e contrariam um princípio fundamental do RGPD: o princípio da **minimização**. O tratamento de dados pessoais deve evitar, tanto quanto possível, o uso de dados identificáveis. Mesmo quando a anonimização completa não é viável, devem ser adotadas medidas para maximizar a anonimidade, reduzindo o número de identificadores diretos ou o nível de detalhe dos dados recolhidos (por exemplo, evitar datas de nascimento exatas ou moradas completas).

A minimização de dados implica que os dados a recolher e tratar sejam:

- **Adequados** – ou seja, suficientes para cumprir devidamente a finalidade declarada ou os objetivos do estudo;
- **Pertinentes** – com uma ligação lógica e direta à finalidade em causa;
- **Limitados ao que é necessário** – sem recolher ou conservar mais dados do que os necessários para essa finalidade.

Em termos práticos, isto significa que não se deve recolher mais dados do que os estritamente exigidos pelas finalidades científicas do projeto. Para tal, a aplicação do princípio da minimização pode assumir várias formas, tais como:

- Minimizar a quantidade de dados pessoais recolhidos (por exemplo, limitar o número de participantes ou o número de atributos recolhidos por participante);
- Minimizar a granularidade dos dados (como recolher faixas etárias em vez de idades exatas);
- Minimizar a replicação dos dados pessoais, evitando cópias desnecessárias ou redundantes;
- Minimizar a transmissão de dados pessoais, reduzindo envios repetidos ou evitáveis;
- Minimizar o acesso interno aos dados, restringindo-o apenas a quem deles necessita para fins científicos legítimos;
- Minimizar a recolha de dados sensíveis (por exemplo, *categorias especiais de dados* na aceção do RGPD), sempre que não sejam necessários ao objetivo da investigação.

Além destas, duas outras formas de minimização merecem especial atenção, por constituírem mecanismos técnicos fundamentais na proteção de dados em contexto científico — a anonimização e a pseudonimização:

- Limitar ou minimizar a duração da conservação dos dados pessoais, estabelecendo prazos claros para a sua eliminação ou, alternativamente, para a anonimização, quando a identificação dos participantes já não for necessária. A anonimização não é isenta de riscos e é tratada no Nó **Anonimização.**
- Minimizar o acesso a identificadores diretos, recorrendo à pseudonimização — isto é, separando os identificadores dos restantes dados e condicionando o seu acesso ao estritamente necessário. Esta medida é abordada no Nó **Pseudonimização.**

Exemplos

Exemplo 1: Redução de atributos desnecessários

Numa investigação sobre fatores de stress em trabalhadores da administração pública, a equipa considera inicialmente recolher o nome do serviço onde cada participante trabalha. Após revisão ética, opta por recolher apenas a área funcional (ex: financeira, jurídica, técnica), por ser suficiente para os objetivos do estudo. Esta decisão evita a recolha de um dado que poderia facilitar a identificação dos participantes.

Exemplo 2: Granularidade adequada

Num inquérito sobre comportamentos de saúde, em vez de recolher a idade exata dos participantes, os investigadores optam por faixas etárias de cinco anos (ex: 18–24, 25–29, etc.), pois essa informação é suficiente para análise estatística e reduz o risco de identificação indireta.

Exemplo 3: Limitação da transmissão de dados

Num projeto colaborativo entre duas universidades, os dados sensíveis recolhidos são analisados localmente por cada equipa, e apenas os resultados agregados (sem dados pessoais) são partilhados entre parceiros. Evita-se, assim, a transmissão desnecessária de dados pessoais.

Exemplo 4: Controlo de acessos na equipa de investigação

Num estudo qualitativo com entrevistas a sobreviventes de violência doméstica, apenas a investigadora responsável tem acesso aos dados brutos das entrevistas. As transcrições utilizadas para análise por outros membros da equipa são previamente revistas para remoção de detalhes identificadores. Esta medida promove que o acesso a dados sensíveis seja limitado ao estritamente necessário.

Exemplo 5: Exclusão de variáveis sensíveis não essenciais

Num estudo sobre hábitos alimentares, o questionário inicial previa perguntas sobre religião, com o argumento de que poderia influenciar certos padrões alimentares. Após revisão metodológica, essa variável foi removida por não ser essencial à análise prevista, respeitando o princípio da minimização.

Perguntas de controlo

Avalio periodicamente os dados pessoais conservados no projeto e elimino tudo o que não for mais necessário?

1. Vou recolher os dados pessoais suficientes para cumprir adequadamente os objetivos da investigação?
2. Vou recolher apenas os dados pessoais que são realmente necessários para os objetivos da investigação?

Se a resposta for “sim” para ambas as questões, verifique se é possível posteriormente, em algum momento do projeto, anonimizar os dados, seguindo para o Nó **Anonimização.**

Se a resposta for “não” para alguma das questões, reavalie os seus conjuntos de dados.

3. Estabeleci prazos de conservação, após os quais se prevê eliminar os dados desnecessários ou anonimizá-los?

Se sim, depois de averiguar a Anonimização e/ou Pseudonimização, deve passar pelo Nó **Fatores críticos de risco.**

A minimização de dados não é um exercício único a ser feito apenas no início do projeto. Ela deve ser realizada periodicamente durante toda a execução da investigação, de forma a garantir que apenas os dados necessários continuam a ser tratados.

4. Avalio periodicamente os dados pessoais conservados no projeto e elimino tudo o que não for mais necessário?

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Avaliação da existência de responsabilidade conjunta (Nó 3a))

Carregue aqui para avançar para o nó seguinte – Planeamento da anonimização (Nó 5)

5. Planeie a anonimização

Clarificação de conceitos

Uma forma de mitigar preocupações éticas e riscos jurídicos associados à recolha de dados pessoais é proceder, em momento posterior à recolha, à sua **Anonimização** — ou seja, à transformação dos dados de modo que deixem de poder ser associados a pessoas identificáveis. A anonimização concretiza-se mediante a aplicação de técnicas como a supressão de atributos, a codificação, a generalização ou a introdução de ruído.

Importa sublinhar que os dados anonimizados são, por definição, dados que deixaram de permitir a identificação de uma pessoa, de forma irreversível, ainda que tenham inicialmente correspondido a uma pessoa identificável. Quando os dados são adequadamente anonimizados, o RGPD deixa de ser aplicável a esse conjunto de dados — mas **apenas** a partir do momento em que a anonimização é efetivamente realizada.

O que anonimizar?

A decisão sobre o que deve ser anonimizado (ou **eliminado**) depende da natureza e finalidade do projeto de investigação, devendo atender simultaneamente a:

- Critérios de minimização de dados e redução de risco, evitando conservar ou divulgar dados pessoais além do necessário, em especial aqueles que possam representar riscos para os participantes;
- Conformidade com as condições do consentimento obtido junto dos participantes, quando aplicável, e/ou o regime jurídico aplicável;
- Políticas institucionais e orientações de preservação documental e arquivística na administração pública, designadamente as emanadas pela Direção Geral dos Livros, Arquivos e Bibliotecas (DGLAB).

No plano da minimização, redução de riscos e conformidade com o consentimento, o que se anonimiza são tipicamente os dados pessoais recolhidos junto dos participantes — por exemplo, respostas a questionários, entrevistas, imagens ou registos biométricos — que não sejam necessários à conservação administrativa. O momento da anonimização deve respeitar os prazos e políticas de conservação aplicáveis, incluindo a necessidade de demonstrar a integridade científica do processo de investigação.

Já as políticas de preservação documental e arquivística incidem sobretudo sobre os documentos administrativos e processuais que integram os processos de investigação – por exemplo, modelos formais, dados administrativos, artigos, constituição das equipas, tramitação de autorizações, contratos, relatórios, correspondência institucional, avaliação de projetos, prémios, entre outros. Estes processos constituem arquivos de interesse público, cujos dados e informações **não são elimináveis**, devendo ser mantidos integralmente. No contexto da conservação administrativa, admite-se a **pseudonimização** reversível para proteção de dados pessoais, mas não a anonimização irreversível, uma vez que os dados devem manter a possibilidade de reversão quando for necessário comunicá-los ao público enquanto em arquivo definitivo.

Este Nó centra-se, portanto, nas condições de anonimização dos dados recolhidos diretamente junto dos participantes ou resultantes da sua participação, normalmente obtidos mediante consentimento, e não na gestão arquivística dos processos administrativos de investigação.

Aspetos a considerar antes de concluir que os dados estão efetivamente anonimizados:

- **Risco de reidentificação:** Toda anonimização acarreta um **risco inerente de reidentificação**, ou seja, a possibilidade de que o detentor dos dados ou um terceiro consiga revertê-la, associando novamente os dados a pessoas identificadas ou identificáveis, através de técnicas de correspondência ou cruzamento com outros conjuntos de dados. A anonimização só pode ser considerada efetiva quando o risco de reidentificação for negligenciável, tendo em conta todos os meios que possam razoavelmente ser utilizados para identificar alguém, à luz do estado da arte, dos custos, do tempo e dos recursos necessários. Apenas dados **efetivamente anonimizados** podem ser considerados não pessoais.

- **A eliminação de identificadores diretos não é suficiente:** A remoção ou codificação de identificadores diretos, como o nome, o NIF, números de identificação ou outros atributos que identificam diretamente pessoas, **não garante por si só** a anonimização.

- **Identificadores indiretos exigem especial cautela:** Mesmo sem identificadores diretos, a eliminação, codificação ou generalização de identificadores indiretos, como idade, localização, código postal ou género, **pode não ser suficiente**, pois a reidentificação pode ser possível com técnicas de inferência ou combinando os dados com outras fontes, públicas ou acessíveis.

- **Ausência de prescrição legal quanto às técnicas utilizadas:** Não existem métodos legalmente obrigatórios. A escolha da técnica de anonimização deve atender à sua robustez, ao contexto dos dados, ao valor da informação e aos riscos envolvidos.

- **Avaliação contínua do risco de reidentificação:** A eficácia da anonimização deve ser periodicamente reavaliada, tendo em conta o uso futuro dos dados e a evolução das capacidades tecnológicas. **Em caso de dúvida, os dados devem ser tratados como pessoais.**

- **Descarte dos dados brutos**: A anonimização só se considera efetiva após a desvinculação definitiva dos dados originais, o que geralmente só se torna efetivo após a eliminação dos dados originais. Se o investigador – ou qualquer pessoa, dentro ou fora da instituição – mantiver acesso aos dados brutos a partir dos quais se realiza a anonimização, os dados resultantes desse processo continuam a ser considerados pessoais, uma vez que subsiste uma possibilidade razoável de reidentificação.

- **Inexistência de conjuntos de dados que permitam reverter a anonimização:** Enquanto existirem outros conjuntos de dados — públicos, na própria instituição ou acessíveis via terceiros — que permitam identificar indivíduos no conjunto de dados supostamente anonimizado, então a anonimização não pode ser considerada efetiva.

- **Necessidade de consentimento ou autorização para divulgação pública**: Mesmo que os dados sejam anonimizados de forma robusta, a sua divulgação pública (por exemplo, em repositórios abertos, publicações ou bases de dados acessíveis) deve ter sido prevista no consentimento inicial dos participantes, antes da anonimização. A anonimização é uma operação de tratamento de dados pessoais e, por conseguinte, não elimina, por si só, as obrigações éticas e legais associadas à divulgação posterior dos dados.

Exemplos

Exemplo 1: A criação de um conjunto de dados resultante de entrevistas a participantes, mesmo que já desprovido de identificadores diretos, pode não constituir uma verdadeira anonimização. Enquanto subsistirem dados brutos ou outros elementos que permitam reidentificar os participantes, o tratamento continua a ser considerado de dados pessoais e sujeito ao regime de proteção aplicável.

Exemplo 2: Um conjunto de dados que omite nomes e números de identificação, mas mantém variáveis como idade, freguesia de residência, ocupação e sexo, pode não estar anonimizado, se for possível cruzar essas variáveis com bases de dados públicas ou institucionais e, assim, reidentificar indivíduos.

Exemplo 3: A aplicação de uma técnica de desidentificação por codificação, onde identificadores são substituídos por pseudónimos, não constitui uma anonimização efetiva se for possível, direta ou indiretamente, reverter a correspondência com os dados originais — por exemplo, através da posse da tabela de conversão ou acesso aos dados brutos.

Exemplo 4: Um investigador recolhe dados de geolocalização ao minuto de um conjunto de participantes durante uma semana. Mesmo após remover nomes e contatos, a trajetória individual de movimentos pode ser suficiente para identificar pessoas, especialmente se cruzada com registos de horários de trabalho ou locais frequentados — o que impede de se considerar os dados efetivamente anonimizados.

Exemplo 5: Um conjunto de dados que remove o nome do utilizador, mas mantém o endereço IP associado a cada registo de atividade, não pode ser considerado anonimizado. Endereços IP, especialmente se estáticos ou com data e hora associadas, podem permitir a identificação do utilizador através de dados mantidos pela instituição ou por outros fornecedores, configurando um risco de reidentificação.

As perguntas abaixo devem ser analisadas tanto na fase de planeamento do projeto, antes da recolha dos dados, como ao longo da fase de tratamento. A sua finalidade é apoiar a tomada de decisões informadas quanto à necessidade, viabilidade e robustez da anonimização.

Perguntas de controlo

Em algum momento do projeto, os fins do tratamento podem ser atingidos recorrendo apenas a dados anonimizados? Isto é, os fins podem ser cumpridos apenas com conjuntos de dados que já não permitam a identificação de indivíduos?

- Ao anonimizar os dados, os fins do tratamento podem ser atingidos apagando os dados brutos originais? Apagou os dados brutos originais?
- Foram aplicadas técnicas apropriadas de anonimização que garantam risco de reidentificação negligenciável, tendo em conta os meios razoavelmente disponíveis e a evolução tecnológica? Em particular, foi avaliado se o conjunto de dados a anonimizar inclui informações sensíveis — como dados de saúde, infrações criminais ou outros elementos de natureza altamente pessoal — que, no caso de reidentificação, ainda que improvável, possam pôr em risco a privacidade ou causar constrangimentos ou prejuízos aos titulares? Sendo o caso, aplicou técnicas de anonimização adequadas e rigorosas?
- Foi verificado que não existem outros conjuntos de dados — na própria instituição, acessíveis via terceiros ou públicos – que, quando combinados, possam permitir a reidentificação de pessoas no conjunto de dados supostamente anonimizado?

Se respondeu sim a todas as perguntas anteriores, o RGPD não se aplicará aos dados resultantes do processo de anonimização. Se está na fase de tratamento, implemente a anonimização. No entanto, esses dados devem continuar a ser monitorizados, pois a evolução tecnológica pode alterar o risco de reidentificação. Importa ainda sublinhar que os dados anonimizados podem estar sujeitos a requisitos éticos adicionais. A robustez da anonimização não legitima, por si só, a divulgação pública dos dados (por exemplo, em repositórios abertos, publicações ou bases de dados acessíveis). Essa divulgação apenas é admissível se tiver sido prevista e autorizada através de consentimento informado obtido junto dos participantes antes da anonimização.

Embora em algum momento do projeto os dados possam ser anonimizados, tal não obsta a que, antes da anonimização, os dados possam ser também pseudonimizados. Averigue a necessidade de **Pseudonimização** dos dados.

Se respondeu não a uma ou mais do que uma das questões anteriores, os dados mantêm o estatuto de dados pessoais, e o RGPD continua a aplicar-se. Mesmo que, na fase de tratamento, tenham sido aplicadas medidas de anonimização, estas não foram suficientes. Sempre que possível, procure anonimizar os dados tanto quanto for viável, mas não assuma que estão fora do âmbito do RGPD: até nova verificação, devem ser tratados como dados pessoais.

Se está na fase de planeamento, antes de passar à identificação de fatores críticos de risco, deve prosseguir para o Nó **Pseudonimização**, para verificar a eventual necessidade de pseudonimizar os dados.

Ligações úteis:

- Agencia Española de Protección de Datos (AEPD) & European Data Protection Supervisor (EDPS). (2021). *AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation*. European Data Protection Supervisor. Disponível em: https://www.edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en

- Article 29 Data Protection Working Party. (2014). *Opinion 05/2014 on Anonymisation Techniques* (WP216). Comissão Europeia. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf

- Comissão Nacional de Proteção de Dados. (2023). *Diretriz/2023/1 sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais*. CNPD. Disponível em: https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/122048

- Data Protection Commission. (2019, junho). *Guidance on Anonymisation and Pseudonymisation*. Autoridade de Proteção de Dados da Irlanda. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf

- Direção-Geral do Livro, dos Arquivos e das Bibliotecas (DGLAB) (s.d.). Lista Consolidada de Conservação e Eliminação – Classe 800.20: Investigação Científica. Disponível em: https://clav.dglab.gov.pt/classes/consultar/c800.20

- European Archives Group (EAG) (2022). Draft Guidelines on the Identification and Appraisal of Public Interest Archives. Version 1.11, May 2022. Disponível em: https://www.voea.at/wp-content/uploads/2022/05/EAG-Draft-Guidelines_1_11.pdf

- Personal Data Protection Commission. (2018). *A guide to basic data anonymisation techniques* (Versão 1.0). Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf

- 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 (Regulamento Geral sobre a Proteção de Dados) — Considerando 26. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#rct_26

- Tribunal de Justiça da União Europeia. (2025). *Parecer do Advogado-Geral Spielmann no processo C-413/23 P: EDPS vs. Single Resolution Board*. ECLI:EU:C:2025:59. Disponível em: https://curia.europa.eu/juris/document/document.jsf?docid=295078&doclang=EN

Ferramentas de anonimização e pseudonimização:

- Anonimatron. (n.d.). *Anonimatron – Data anonymization tool*. GitHub Pages. Disponível em: https://realrolfje.github.io/anonimatron/

- Argus. (n.d.). *Argus anonymization*. QoSient. Disponível em: https://qosient.com/argus/anonymization.shtml

- ARX Data Anonymization Tool. (s.d.). *A comprehensive open source software for anonymizing sensitive personal data*. Disponível em: https://arx.deidentifier.org/

- Datprof. (n.d.). *DATPROF Privacy – Data masking software*. DATPROF. Disponível em: https://www.datprof.com/products/datprof-privacy/

- Harvard University Privacy Tools Project. (s.d.). *DataTags: A suite of tools to help researchers share and use sensitive data in a standardized and responsible way*. Disponível em: https://privacytools.seas.harvard.edu/datatags-dataverse

- OpenAIRE. (s.d.). *Amnesia: Data anonymization tool*. Disponível em: https://amnesia.openaire.eu/

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Planeamento da minimização dos dados (Nó 4)

Carregue aqui para avançar para o nó seguinte – Planeamento da pseudonimização (Nó 6)

6. Planeie a pseudonimização

Clarificação de conceitos

A anonimização dos dados pessoais é preferível à pseudonimização. No entanto, quando a anonimização não é possível ou conveniente para os objetivos do projeto de investigação, deve recorrer-se à *pseudonimização*. Trata-se de uma técnica de tratamento de dados pessoais que consiste em substituir ou modificar informações de forma a impedir a identificação do titular dos dados sem uso de informações adicionais.

Essas informações suplementares, que permitem a reidentificação dos titulares, devem ser armazenadas separadamente e protegidas por medidas técnicas e organizativas adequadas, de modo a garantir que os dados pseudonimizados não possam ser atribuídos a uma pessoa singular identificada ou identificável.

Os métodos utilizados para a pseudonimização podem incluir, substituição de texto (por exemplo, o uso de identificadores alternativos), a criptografia (convertendo os dados para um formato ilegível, mas reversível com uma chave) ou o *hashing* (um processo de codificação unidirecional que não pode ser revertido facilmente).

Dados pseudonimizados são dados pessoais?

A pseudonimização visa dificultar a ligação entre os dados e uma pessoa específica, diminuindo o risco de reidentificação, mas sem o eliminar por completo. Por norma, **os dados pseudonimizados continuam a ser dados pessoais**, pois quem detém a informação suplementar (as chaves de correspondência) pode recuperar os dados originais e reidentificar os titulares.

A jurisprudência europeia recente veio, porém, introduzir uma distinção crucial baseada na existência — ou ausência — de meios razoáveis de reidentificação.[4] Essa distinção permite compreender de forma prática diferentes cenários de transmissão de dados pseudonimizados:

- Transmissão interinstitucional — Quando uma instituição (por exemplo, a Universidade A) que controla os dados originais partilha dados pseudonimizados com outra instituição (por exemplo, a Universidade B), e esta não dispõe de meios razoáveis para reidentificar os titulares, esses dados podem deixar de ser considerados dados pessoais para a instituição destinatária (a Universidade B). Isto porque a capacidade de reidentificação reside na instituição transmissora (Universidade A), que reteve a chave de correspondência. Assim, o estatuto de dado pessoal depende de quem detém efetivamente os meios suplementares.

- Transmissão intrainstitucional (no âmbito do mesmo responsável pelo tratamento) — Se a transmissão ocorrer dentro da mesma instituição (ainda que entre pessoas ou serviços distintos, em que um tenha a chave e o outro não), os dados pseudonimizados são sempre considerados dados pessoais. Tal decorre do facto de, no contexto de um único responsável pelo tratamento, se considerarem existir, em princípio, meios razoáveis suscetíveis de permitir a reidentificação.

Considerações a ter em conta na pseudonimização:

- A pseudonimização é uma medida de proteção, mas não é uma solução definitiva para garantir a impossibilidade de identificação dos titulares de dados. Em regra, dados pseudonimizados continuam a ser considerados dados pessoais.
- As informações suplementares que permitem a identificação dos titulares devem ser conservadas separadamente dos dados pseudonimizados, com medidas de segurança que previnam o acesso não autorizado.

[4] Caso C-413/23 P (Tribunal de Justiça da União Europeia), acórdão de 4 de setembro de 2025, ECLI: EU:C:2025:645.

- Tal como na anonimização, não existem métodos legalmente obrigatórios. A escolha da técnica de pseudonimização deve considerar a sua praticabilidade, robustez, o valor da informação e os riscos envolvidos.
- No âmbito de uma dada instituição, mesmo que um investigador não tenha acesso às informações suplementares (por exemplo, estando acessíveis apenas por um grupo restrito dentro dessa instituição), os dados continuam a ser considerados pessoais e devem ser tratados como tal.
- Mesmo que se eliminem as informações suplementares, isso não transforma automaticamente os dados pseudonimizados em dados anonimizados. Para que os dados sejam considerados anonimizados, é necessário garantir que não é possível, por nenhum meio razoável, reidentificar os titulares.

Exemplos

Exemplo 1: Base de dados de alunos

Uma base de dados de alunos com os atributos nome, número, curso, idade e média final é pseudonimizada através de uma cópia dos dados, na qual os identificadores diretos (nome e número) são substituídos por códigos ou identificadores aleatórios, e alguns identificadores indiretos são generalizados — por exemplo, convertendo a idade em faixas etárias (18–20, 21–23, etc.). Se o atributo "curso" não for necessário, pode ser removido ou também codificado. O investigador deve manter a base de dados original separadamente, com medidas de segurança adequadas. Os dados pseudonimizados também devem ser protegidos.

Exemplo 2: Estudo clínico com pacientes

Numa investigação sobre a eficácia de um novo tratamento, a base de dados inclui nome, número do utente, idade, sexo, tipo de tratamento e resultados clínicos. Para pseudonimizar os dados, os identificadores diretos (nome e número do utente) são substituídos por códigos aleatórios. A idade é convertida em intervalos (ex.: 30–40 anos), e o tipo de tratamento é codificado com letras (ex.: A, B, C). As chaves que permitem associar os códigos aos pacientes são mantidas separadamente, com acesso restrito apenas à equipa clínica, e não aos investigadores responsáveis pela análise.

Exemplo 3: Plataforma de inquéritos online

Numa plataforma que recolhe respostas de inquéritos para fins académicos, os dados dos participantes incluem e-mail, profissão, idade, localização e respostas abertas. Para pseudonimização, os e-mails são substituídos por identificadores alfanuméricos, a idade é agrupada em faixas etárias, e a localização é reduzida ao nível de região (em vez de cidade ou código postal). As respostas abertas são revistas para remover menções diretas que possam identificar o participante (por exemplo, o nome de uma empresa pequena onde um participante trabalhe). Os dados originais são mantidos sob controlo da instituição promotora do inquérito, não acessíveis aos investigadores externos.

Exemplo 4: Entrevistas transcritas

Num estudo sobre a experiência de migrantes, entrevistas gravadas foram transcritas para análise qualitativa. As transcrições incluíam nomes próprios, locais, datas e referências pessoais. Após as entrevistas, os registos de voz foram apagados, mas mantidas as transcrições. Para pseudonimizar as transcrições os nomes foram substituídos por pseudónimos, os locais específicos por descrições genéricas (ex.: "bairro periférico"), as datas por expressões vagas (ex.: "há alguns anos") e as referências a instituições pequenas foram generalizadas. As transcrições originais foram armazenadas separadamente, com acesso restrito. As versões pseudonimizadas, usadas na análise, continuam a ser tratadas como dados pessoais.

As perguntas abaixo devem ser analisadas tanto na fase de planeamento do projeto, antes da recolha dos dados, como ao longo da fase de tratamento. A sua finalidade é apoiar a tomada de decisões informadas quanto à necessidade, viabilidade e robustez da pseudonimização.

Perguntas de controlo

A pseudonimização é viável sem comprometer os objetivos da investigação, a qualidade ou a validade dos resultados esperados?

- Foram aplicadas técnicas adequadas de pseudonimização?
- As informações suplementares são armazenadas separadamente e com medidas de segurança técnicas e organizativas apropriadas?
- Está assegurado que apenas pessoas autorizadas têm acesso às informações suplementares que permitem a reidentificação?
- Foi avaliado se a combinação dos dados pseudonimizados com outras fontes (internas ou externas) pode permitir a reidentificação de titulares?
- Mesmo sem acesso direto às chaves de reidentificação, foi ponderado o risco de que terceiros possam cruzar os dados com outras fontes e identificar pessoas?
- Há medidas definidas para destruição segura das informações suplementares quando deixarem de ser necessárias?
- Foi esclarecido que, em regra, os dados pseudonimizados continuam a ser considerados dados pessoais e sujeitos ao RGPD, salvo quando sejam transmitidos a uma entidade distinta que não detenha nem tenha acesso, por meios razoáveis, às informações suplementares?
- O tratamento de dados pseudonimizados envolve dados sensíveis, tais como categorias especiais de dados? Se sim, foram aplicadas medidas adicionais de mitigação de risco?

Se respondeu sim a todas as perguntas anteriores, os dados poderão ser considerados pseudonimizados. Se está na fase de tratamento, implemente a pseudonimização. Note que, mesmo pseudonimizados, os dados continuam a ser dados pessoais e devem respeitar todos os princípios e obrigações do RGPD.

Se respondeu não a uma ou mais do que uma das perguntas anteriores, os dados não podem ser suficientemente pseudonimizados, o que pode aumentar os riscos para os titulares. Procure otimizar as medidas de pseudonimização sempre que possível. Caso as exigências técnicas de pseudonimização comprometam os objetivos científicos, aplique as medidas viáveis e documente as razões pelas quais não foi inteiramente possível pseudonimizar os dados.

NOTA: Se está na fase de planeamento, prossiga para o Nó **Fatores críticos de risco**.

Ligações úteis:

- Comissão Nacional de Proteção de Dados. (2020). *Deliberação 2020/238 relativa ao tratamento estatístico de dados de compras e consumos de medicamentos no âmbito da atividade hospitalar do Hospital de Braga E.P.E.*. CNPD. Disponível em: https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121800

- Consultar também as ligações úteis disponibilizadas no Nó Anonimização

Ferramentas de anonimização e pseudonimização:

- OpenAIRE. (s.d.). *Amnesia: Data anonymization tool*. Disponível em: https://amnesia.openaire.eu/

- Harvard University Privacy Tools Project. (s.d.). *DataTags: A suite of tools to help researchers share and use sensitive data in a standardized and responsible way*. Disponível em: https://privacytools.seas.harvard.edu/datatags-dataverse

- ARX Data Anonymization Tool. (s.d.). *A comprehensive open source software for anonymizing sensitive personal data*. Disponível em: https://arx.deidentifier.org/

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Planeamento da anonimização (Nó 5)

Carregue aqui para avançar para o nó seguinte – Identificação de fatores críticos de risco (Nó 7)

7. Identifique os fatores críticos de risco

Clarificação de conceitos

Nem todos os tratamentos de dados pessoais envolvem o mesmo nível de risco. Alguns projetos podem tratar dados com impacto limitado na privacidade e nos direitos dos participantes, enquanto outros envolvem contextos de maior sensibilidade ou complexidade, implicando medidas mais rigorosas de proteção. A identificação de fatores críticos de risco visa adequar as medidas técnicas, organizativas e éticas ao grau de exposição dos participantes.

O risco não é uma categoria absoluta: resulta da combinação entre a natureza dos dados (sensibilidade e forma de tratamento), o âmbito do tratamento (extensão, escala e volume dos dados), o contexto (circunstâncias da relação entre o responsável e o participante, incluindo, por exemplo, tecnologias utilizadas e as características das populações envolvidas) e os objetivos da investigação (nível de intrusão na privacidade, se é legítima, consequências para o participante).

Quanto mais elevado for o risco — real ou potencial — de ocorrência de danos concretos para os participantes (como discriminação, perda de oportunidades, exclusão social ou perda de controlo sobre os seus dados), maior deve ser o nível de proteção implementado, dado que esses danos correspondem, em última análise, a uma afetação dos seus direitos e liberdades fundamentais. Isto inclui medidas de transparência, gestão adequada do consentimento, minimização e segurança dos dados, entre outras, e, quando aplicável, avaliação por comissões de ética ou outras estruturas de supervisão.

A análise de risco deve ser iniciada desde a fase de planeamento do projeto, antes da recolha de dados, e revista sempre que o tratamento evolua ou se alterem os pressupostos iniciais (por exemplo, nova recolha de dados, introdução de novas tecnologias, reutilização ou partilha de dados). A identificação, avaliação e mitigação de risco corresponde, na prática, ao que o RGPD e o Regulamento n.º 798/2018 da Comissão Nacional de Proteção de Dados (CNPD) designam como **Avaliação de Impacto sobre a Proteção de Dados** (AIPD).

A AIPD é obrigatória sempre que um tratamento de dados pessoais possa resultar num elevado risco para os direitos e liberdades dos titulares, nos termos do artigo 35.º do RGPD. Sempre que o tratamento revele esse nível de risco e seja realizada uma AIPD, o parecer do Encarregado de Proteção de Dados (EPD) constitui elemento obrigatório do processo de avaliação. Regra geral, considera-se existir risco elevado quando estão presentes múltiplos fatores de risco, como os aqui descritos, com impacto significativo nos participantes.

A lista de fatores críticos de risco apresentada neste Nó tem como objetivo apoiar a identificação desses fatores e a definição de medidas de mitigação e proteção — quer a avaliação venha a ser formalizada numa AIPD, quer permaneça integrada na análise de risco geral do projeto.

Exemplos

Exemplo 1: Projeto suscetível de risco não elevado

Um estudo em psicologia recolhe dados sobre estratégias de regulação emocional em adultos, através de entrevistas semi-estruturadas gravadas em áudio. As gravações são transcritas, pseudonimizadas, e os ficheiros de áudio são eliminados após a transcrição. Os participantes são adultos sem características que os tornem particularmente vulneráveis, e os dados recolhidos não incluem categorias especiais de dados (ou seja, informações sensíveis, como saúde mental, etnia, religião ou orientação sexual). Embora envolva dados pessoais (nomeadamente a voz e as respostas durante a entrevista), este projeto apresenta um perfil de risco que não se afigura elevado: não trata categorias especiais, não envolve decisões tomadas por algoritmos, nem tecnologias intrusivas ou bases de dados combinadas. As medidas de mitigação — como a pseudonimização precoce, a eliminação de suportes identificáveis e a restrição de acessos — poderão ser proporcionais e suficientes. Ainda assim, poderá ser exigida a submissão do projeto a uma comissão de ética, dependendo das políticas da instituição ou do financiador. A avaliação ética, mesmo quando não obrigatória na instituição, constitui uma boa prática de responsabilidade científica e de proteção dos participantes.

Exemplo 2: Projeto suscetível de risco elevado

Um consórcio internacional de investigação médica recolhe dados clínicos e genéticos de milhares de pacientes com doenças autoimunes, em colaboração com centros hospitalares de vários países. O estudo envolve categorias especiais de dados (saúde e genética), é conduzido em larga escala, aplica técnicas de perfilagem automatizada para prever respostas ao tratamento e inclui transferências internacionais para países fora do Espaço Económico Europeu. Os participantes incluem ainda populações vulneráveis, como doentes crónicos e menores. Neste caso, o tratamento de dados envolve múltiplos fatores críticos de risco, o que impõe a adoção de medidas robustas de proteção, incluindo, entre outras, pseudonimização forte, consentimento informado específico e reforçado, salvaguardas nas transferências internacionais, revisão por comissão de ética e parecer do Encarregado de Proteção de Dados.

Avalie o risco do seu projeto considerando cada fator crítico identificado na lista abaixo, analisando, para cada um, a probabilidade de ocorrência e a gravidade do impacto nos direitos e liberdades dos participantes (ex.: discriminação, impacto reputacional, exclusão ou perda de oportunidades, perda de controle sobre os seus dados, fraude).

Por exemplo, o risco de discriminação decorrente do tratamento de determinados dados sensíveis (como origem étnica, opiniões políticas ou estado de saúde) pode configurar um impacto direto num direito fundamental (igualdade e não discriminação) e, ao mesmo tempo, traduzir-se em danos concretos para os participantes (como exclusão social, perda de oportunidades ou impacto reputacional). Ou seja, o exercício consiste em avaliar a probabilidade de o fator de risco se materializar em danos concretos para os participantes, os quais correspondem, em última análise, a uma afetação dos seus direitos e liberdades fundamentais.

Considere que cada fator de risco deve ser incluído na contagem final apenas quando a combinação entre probabilidade e gravidade indicar que o impacto pode ser significativo para os participantes. Por exemplo, categorize os fatores de risco da seguinte forma: baixo, moderado ou elevado, e contabilize apenas os fatores que avaliou com risco moderado ou elevado:

- Um factor com impacto de baixa probabilidade e baixa gravidade, poderá não ser contabilizado.
- Um factor com baixa probabilidade mas impacto grave, ou com probabilidade elevada mesmo com impacto moderado, será considerado como risco moderado ou elevado e, portanto, deverá ser incluído.

Esta lógica de contagem aplica-se a todos os riscos, exceto no caso de transferências internacionais, onde o risco só deve ser apreciado se não existir uma decisão de adequação relativamente ao país de destino.

Pergunta de controlo

A sua investigação envolve alguns dos seguintes fatores críticos de risco?

a) **Dados sensíveis**, incluindo as designadas no RGPD *Categorias Especiais de Dados?* Por exemplo, dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar pessoas, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. Ou *dados altamente pessoais*, ligados a atividades privadas ou familiares (tais como comunicações eletrónicas cuja confidencialidade deve ser protegida) ou porque afetam o exercício de um direito fundamental (tais como dados de localização cuja recolha põe em causa a liberdade de circulação) ou porque a sua violação implica claramente que a vida quotidiana do titular dos dados será gravemente afetada (tais como dados financeiros passíveis de ser usados para a prática de um crime de fraude). Ou quaisquer dados pessoais relacionados com *condenações penais e infrações*. Prossiga para o Nó **Dados sensíveis**.

b) **Transferências de ou para países fora do Espaço Económico Europeu?** Sempre que dados pessoais sejam enviados para um país terceiro fora do Espaço Económico Europeu (EEE) — seja para simples armazenamento ou qualquer outro tipo de utilização — considera-se uma exportação de dados. Por exemplo, mesmo que os dados permaneçam fisicamente no EEE, o acesso remoto por parte de alguém localizado fora do EEE (como um parceiro internacional ou prestador de serviços) configura uma exportação. Inversamente, se dados são recebidos de um país terceiro para serem tratados por uma instituição localizada no EEE, estamos perante uma importação de dados pessoais. Prossiga para o Nó **Transferências Internacionais**.

c) **Participantes menores de idade ou populações vulneráveis**? Quando há acentuado desequilíbrio com o responsável pelo tratamento dos dados pessoais, significando isto que os indivíduos podem não ser capazes de consentir, ou opor-se, facilmente ao tratamento dos seus dados ou de exercer os seus direitos. A vulnerabilidade pode resultar da idade, de situações de doença ou deficiência, de dependência institucional (como em lares, prisões ou centros de acolhimento), de fragilidade socioeconómica ou de relações de poder assimétricas (como em contextos educativos — por exemplo, na relação professor e aluno — ou laborais – por exemplo, no caso dos trabalhadores dependentes). Estas pessoas podem ter maior dificuldade em compreender os riscos associados ao tratamento dos seus dados ou em exercer plenamente os seus direitos, pelo que devem beneficiar de garantias adicionais. Prossiga para o Nó **Menores e Populações Vulneráveis**.

d) **Tratamento em grande escala?** O tratamento de dados pessoais em grande escala refere-se, de forma genérica, a operações de tratamento que envolvem um volume significativo de dados, abrangendo um número relevante de titulares, e que possam ter impacto alargado no conjunto da população afetada. Prossiga para o Nó **Tratamento em Larga Escala**.

e) **Definição de perfis com impacto nos participantes?** Inclui a avaliação ou classificação de aspetos relacionados com o desempenho profissional, a situação económica, a saúde, as preferências ou interesses pessoais, a fiabilidade ou o comportamento, bem como a localização ou deslocações do titular dos dados. Prossiga para o Nó **Definição de Perfis**.

f) **Decisões automatizadas por algoritmos com impacto nos participantes?** Tratamento destinado à tomada de decisões automatizadas sobre os participantes e que produza «efeitos jurídicos relativamente à pessoa singular» ou que «a afetem significativamente de forma similar». Prossiga para o Nó **Decisões automatizadas por algoritmos**

g) **Controlo sistemático?** Tratamento utilizado para observar, monitorizar ou controlar os participantes, incluindo dados recolhidos através de redes, ou um «controlo sistemático de zonas acessíveis ao público». Prossiga para o Nó **Controlo Sistemático**.

h) **Combinam-se bases de dados?** Tratamento que resulta da integração de dados provenientes de duas ou mais fontes, realizadas com diferentes finalidades e/ou por diferentes responsáveis pelo tratamento. Prossiga para o Nó **Combinação de bases de dados**.

i) **Envolve Inteligência Artificial ou outras novas soluções tecnológicas?** A utilização de soluções tecnológicas ou organizacionais inovadoras que possam ter riscos acrescidos para os participantes devido à incerteza quanto às suas consequências pessoais, sociais e éticas. Prossiga para o Nó **Inteligência Artificial ou outras novas soluções tecnológicas.**

j) **Elevado risco ético?** Considera-se existir elevado risco ético quando as ações ou decisões no âmbito da investigação possam ter consequências significativas para os participantes, investigadores, instituições ou outros stakeholders, colocando em causa valores ou princípios éticos (como a dignidade, o bem-estar físico ou psicológico, a justiça, a integridade ou a autonomia), ou gerando ambiguidades, conflitos, questões legais ou reputacionais. Caso a sua investigação esteja sujeita a elevado risco ético, prossiga para o Nó **Exposição a elevado risco ético**.

Se sim, se a sua investigação envolve alguns fatores críticos de risco acima referidos, dependendo do número, da probabilidade da ocorrência e da gravidade, poderá ser necessário realizar uma avaliação de impacto mais profunda e formalizar a submissão do projeto à comissão de ética e/ou ao Encarregado de Proteção de Dados. Consulte sempre as políticas da sua instituição nesta matéria, que podem variar de instituição para instituição. Por exemplo, uma regra possível poderá ser a seguinte:

- Zero fatores com risco moderado ou elevado → apreciação ética simplificada pela comissão de ética;
- Um fator com risco moderado → apreciação ética aprofundada pela comissão de ética;
- Um fator com risco elevado ou dois ou mais fatores com risco moderado → apreciação ética aprofundada pela comissão de ética e parecer do Encarregado de Proteção de Dados.

Há casos, porém, em que a formalização de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) é obrigatória, independentemente das políticas da instituição, de acordo com o art. 35º do RGPD. Se a sua investigação envolve os seguintes critérios e fatores críticos conjugados, é obrigatória a formalização de uma AIPD e o parecer do Encarregado de Proteção de Dados:

- Avaliação sistemática e completa dos aspetos pessoais relacionados com participantes, baseada no tratamento automatizado (f), incluindo a definição de perfis (e), sendo com base nela adotadas decisões que produzem efeitos jurídicos ou que os afetem significativamente de forma similar;
- Grande escala (d) e categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações (a)
- Controlo sistemático (g) de zonas acessíveis ao público, e grande escala (d).
- Nas situações previstas no Regulamento n.º 1/2018 da CNPD.

Se não, se a sua investigação não envolve nenhum fator crítico de risco, poderá ainda assim ser exigida a submissão do seu projeto a uma comissão de ética, dependendo das políticas da sua instituição ou do financiador. A **avaliação ética**, mesmo quando não obrigatória na instituição, constitui uma boa prática de responsabilidade científica e de proteção dos participantes.

Siga agora para o Nó **Software adequado**.

Ligações úteis:

- Grupo do Artigo 29.º para a Proteção de Dados. (2017). *Orientações sobre os encarregados da proteção de dados (DPO)* (WP 243 rev.01). Disponível em: https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf

- União Europeia (2016). 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 (Regulamento Geral sobre a Proteção de Dados) — Artigo 35.º: Avaliação de impacto sobre a proteção de dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#art_35

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Planeamento da pseudonimização (Nó 6)

Carregue aqui para avançar para o nó seguinte – Identificação de dados sensíveis (Nó 7a)

Carregue aqui para saltar todos os fatores críticos de risco e avançar diretamente para o nó Software (Nó 8)

7a). Dados sensíveis?

Clarificação de conceitos

Neste toolkit designamos como dados sensíveis os dados pessoais cuja natureza pode implicar riscos significativos para os direitos e as liberdades dos indivíduos:

Categorias especiais de dados

Incluem-se nesta categoria os previstos no art. 9.º do RGPD, designados como **categorias especiais de dados, que abrangem** informações relativas à origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos usados para identificar de forma inequívoca uma pessoa, dados de saúde e dados sobre a vida sexual ou orientação sexual.

Dados relativos a condenações penais e infrações.

São igualmente considerados dados sensíveis os dados pessoais relativos a condenações penais e infrações, previstos no art. 10.º do RGPD.

Dados de índole altamente pessoal

Para além das categorias previstos no RGPD, existem outros dados que, pela sua natureza, são considerados sensíveis. É o caso de informações associadas à vida privada ou familiar, como comunicações eletrónicas, dados que condicionam o exercício de direitos fundamentais, como os dados de localização, ou dados cuja violação teria um impacto direto e grave na vida do titular, como os dados financeiros. Além disso, podem ser considerados dados sensíveis outras informações de carácter muito pessoal, como documentos de identificação, diários ou notas em dispositivos eletrónicos, bem como registos inseridos em aplicações que acompanham acontecimentos da vida privada de uma pessoa.

O tratamento de categorias especiais de dados, quando baseado no consentimento do participante, exige um consentimento reforçado, designado consentimento explícito (art. 9.º, n.º 2, al. a) do RGPD).

Nos restantes casos, em que não estejam em causa categorias especiais de dados, o consentimento simples deve ser inequívoco.

A diferença entre consentimento inequívoco e consentimento explícito é a seguinte:

- Consentimento inequívoco (art. 6.º, n.º 1, al. a) do RGPD): corresponde a uma manifestação clara de vontade, e não pode ser deduzido do silêncio, da inação ou da utilização de caixas pré-selecionadas.
- Consentimento explícito (art. 9.º, n.º 2, al. a) do RGPD): além dos requisitos do consentimento inequívoco, requer uma confirmação expressa, como uma assinatura manuscrita, uma assinatura digital autenticada ou uma declaração escrita equivalente.

O artigo 9.º do RGPD prevê ainda outras condições legais alternativas ao consentimento que podem legitimar o tratamento de categorias especiais de dados. Entre estas situações encontra-se, por exemplo, o caso em que os dados tenham sido tornados públicos pelo próprio titular, o que pode moderar os riscos associados ao seu tratamento.

O RGPD, no seu artigo 10.º, estabelece um regime específico para os dados pessoais relacionados com condenações penais, infrações ou com medidas de segurança conexas.

Embora não integrem formalmente as "categorias especiais de dados" do art. 9.º, estão sujeitos a restrições reforçadas, dada a sua natureza particularmente sensível.

O seu tratamento só é permitido:

- Sob controlo da autoridade pública competente, como o Ministério Público, os tribunais ou entidades policiais no âmbito das suas funções legais.

  Na prática, isto significa que uma instituição de investigação, como uma universidade, não pode assumir a posição de responsável pelo tratamento destes dados. Nestes casos, deve ser realizado um acordo de subcontratação entre a autoridade competente e a universidade, garantindo que esta apenas atua segundo instruções da autoridade.

  Consulte também o Nó **Subcontratação**.

- Quando o tratamento esteja previsto em lei ou regulamento, nacional ou da União Europeia, desde que sejam estabelecidas garantias adequadas para os direitos e liberdades dos titulares, tais como limites claros de finalidade, prazos definidos de conservação e medidas de segurança técnicas e organizativas robustas.

Exemplos

Exemplo 1: Num estudo desenvolvido por uma faculdade de medicina sobre os fatores de risco associados a doenças cardiovasculares, os investigadores recolhem informações clínicas de voluntários, como historial médico, resultados de análises laboratoriais e medições de pressão arterial. Estes são dados de saúde, classificados como categorias especiais de dados, que exigem medidas rigorosas de confidencialidade, pois a sua divulgação poderia expor aspetos íntimos da vida e da saúde dos participantes.

Exemplo 2: Num projeto de engenharia informática que estuda métodos de autenticação seguros, os investigadores recolhem impressões digitais e dados de reconhecimento facial de estudantes, usando também funcionários para testar algoritmos de identificação. Estes são dados biométricos que identificam pessoas de forma inequívoca e que se enquadram nas categorias especiais de dados. Uma falha na sua proteção pode comprometer a privacidade e a segurança dos titulares.

Exemplo 3: Numa investigação em ciências sociais que analisa padrões de mobilidade urbana, os investigadores utilizam dados recolhidos através da georreferenciação de aplicações móveis instaladas nos telemóveis dos participantes. Embora úteis para compreender fluxos de transporte e apoiar o planeamento urbano, estes dados são considerados sensíveis, pois podem revelar hábitos diários, locais frequentados e até categorias especiais de dados, como práticas religiosas ou preferências políticas. O seu tratamento inadequado pode afetar a liberdade de circulação e a vida privada dos participantes.

Exemplo 4: Num estudo em psicologia que analisa o impacto das redes sociais na autoestima dos jovens, os investigadores recolhem mensagens privadas partilhadas por estudantes universitários com amigos próximos. Apesar de recolhidas com consentimento, estas mensagens podem conter informações íntimas sobre relações pessoais, estados emocionais ou crenças individuais, sendo, por isso, dados altamente pessoais que exigem salvaguardas de confidencialidade reforçadas.

Exemplo 5: Num projeto em ciências jurídicas que investiga padrões de reincidência criminal, os investigadores trabalham com registos de condenações penais e processos judiciais. Estes dados são especialmente sensíveis, pois podem afetar diretamente a reputação, os direitos e as oportunidades futuras das pessoas envolvidas. A sua utilização exige não só medidas técnicas de proteção, mas também uma avaliação legal e ética rigorosa quanto à legitimidade do tratamento. De acordo com o artigo 10.º do RGPD, estes dados devem permanecer sempre sob a responsabilidade da autoridade pública competente (por exemplo, tribunais ou Ministério Público). A universidade não pode assumir a posição de responsável pelo tratamento, podendo apenas aceder e tratar a informação sob instruções dessa entidade, ao abrigo de um acordo de subcontratação.

Pergunta de controlo

A sua investigação envolve dados sensíveis?

Se sim, existe um risco pelo menos moderado, podendo mesmo ser elevado, associado à sua investigação. Nestes casos, recomenda-se pelo menos a apreciação ética do seu projeto pela comissão de ética da sua instituição e, eventualmente, o parecer do Encarregado de Proteção de Dados. Consulte as políticas da sua instituição nesta matéria, uma vez que os procedimentos podem variar de instituição para instituição.

Se não, a natureza dos dados é de menor sensibilidade, associados a riscos mais limitados para os direitos e liberdades dos participantes. Ainda assim, devem ser observadas boas práticas de proteção de dados e as orientações da sua instituição.

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Identificação dos fatores críticos de risco (Nó 7)

Carregue aqui para avançar para o nó seguinte – Transferências internacionais (Nó 7b)

7b). Transferências internacionais de dados pessoais

Clarificação de conceitos

Este Nó é apenas relevante quando a transferência internacional de dados pessoais envolve a exportação, ou a importação, de dados pessoais para países terceiros, isto é, países que não façam parte do Espaço Económico Europeu (EEE) e que, como tal, não estão sujeitos ao RGPD. As transferências realizadas dentro do EEE não necessitam de medidas adicionais especificas.

Quando o investigador tenha necessidade de proceder a uma transferência internacional de dados pessoais de/para um país que não faz parte do EEE, tem de se assegurar que as pessoas a quem os dados respeitam beneficiam de um nível de proteção substancialmente equivalente ao garantido pelo regime de proteção de dados da União Europeia. Para facilitar este processo, o RGPD prevê o mecanismo da **decisão de adequação**. Trata-se de uma decisão emitida pela Comissão Europeia que reconhece que um determinado país, território ou setor específico garante um nível de proteção de dados pessoais essencialmente equivalente ao da UE. Nestes casos, a transferência de dados pode ocorrer sem necessidade de autorizações adicionais ou medidas suplementares, funcionando de forma semelhante à circulação de dados dentro do próprio EEE.

A **lista de países com decisão de adequação** é revista e atualizada periodicamente pela Comissão Europeia. Atualmente, incluem-se, por exemplo, países como Japão, Suíça, Canadá (para determinadas entidades), Reino Unido, Argentina e outros reconhecidos como oferecendo garantias adequadas de proteção.

Em contexto de investigação científica, quando a transferência internacional de dados se destina ou tem origem num país que não integra o EEE e não dispõe de uma decisão de adequação, existem duas vias para a legitimar.

A primeira, e mais desejável (embora mais burocrática), é com base em garantias adequadas, nos termos do Artigo 46.º do RGPD, por exemplo, através de Cláusulas Contratuais-Tipo (CCTs). Por exemplo, uma colaboração que inclua uma universidade portuguesa e uma instituição de investigação nos Estados Unidos implica a transferência de dados pessoais. Para permitir essa transferência, as instituições devem celebrar um acordo com base em CCTs, assegurando as garantias adequadas de proteção dos dados.

Caso não estejam previstas garantias adequadas nos termos do art. 46º, é ainda possível realizar transferências, com base no consentimento do participante, desde que este seja não apenas **inequívoco**, mas também **explícito**, e que o participante seja devidamente informado sobre os riscos e a natureza da transferência. A diferença entre consentimento inequívoco e explícito reside no grau de manifestação exigido:

- Consentimento inequívoco, nos termos da alínea a), do nº.1 do art. 6º: pressupõe uma manifestação clara de vontade, mas não pode ser inferido do silêncio, da inação ou da utilização de caixas pré-selecionadas.
- Consentimento explícito, nos termos da alínea a), do nº1 do art.º 49º: vai além do inequívoco, exigindo-se um ato afirmativo explícito associado a uma declaração específica, como uma assinatura manuscrita, uma assinatura digital autenticada ou uma manifestação expressa equivalente.

O **consentimento explícito** deve ainda ser específico para a finalidade da transferência em causa e precedido de informação suficiente para que o titular compreenda plenamente as implicações e riscos para si próprio da sua decisão.

Exemplos

Exemplo 1: Consentimento explícito (origem na UE)
Um investigador português pretende partilhar dados de um estudo clínico efetuado com participantes que se encontrem no território português com uma organização parceira na Índia, país sem decisão de adequação. Obtém o consentimento explícito dos participantes,

informando-os de forma clara sobre os riscos para si próprio que essa transferência acarreta, bem como a natureza da transferência internacional, em conformidade com o RGPD.

Exemplo 2: Consentimento explícito (origem fora da UE)

Um investigador português, no âmbito de um projeto conduzido por uma universidade portuguesa, realiza entrevistas a participantes na Tailândia, país que não beneficia de uma decisão de adequação da Comissão Europeia. Os dados pessoais são recolhidos com base no consentimento explícito dos participantes tailandeses, os quais foram previamente informados sobre os riscos associados ao tratamento de dados, nomeadamente pelo facto de a Tailândia aplicar regras e garantias diferentes das previstas no RGPD e não oferecerem um nível de proteção equivalente.

Exemplo 3: Decisão de adequação

Uma equipa de investigação portuguesa colabora com uma instituição de investigação no Japão para um estudo sobre envelhecimento. Os dados pessoais dos participantes portugueses são tratados com base no consentimento informado e inequívoco. Como o Japão beneficia de uma decisão de adequação da Comissão Europeia, a transferência dos dados pode ocorrer sem necessidade de salvaguardas adicionais, como cláusulas contratuais-tipo ou consentimento explícito.

Exemplo 4: Cláusulas contratuais-tipo

Um consórcio de investigação inclui uma universidade portuguesa e uma instituição de investigação nos Estados Unidos. Para permitir a transferência de dados pessoais dos membros da equipa de investigação entre as instituições, realizam um acordo com base em cláusulas contratuais-tipo aprovadas pela Comissão Europeia, assegurando garantias adequadas de proteção dos dados.

Exemplo 5: Acesso remoto com base em consentimento explícito

Um projeto de investigação envolve uma universidade portuguesa e uma universidade em Moçambique, país que não beneficia de uma decisão de adequação da Comissão Europeia. No âmbito do projeto, investigadores moçambicanos necessitam de aceder remotamente, a partir de Moçambique, a dados pessoais de participantes armazenados em servidores localizados em Portugal. Este acesso remoto constitui uma transferência internacional de dados pessoais e, na ausência de garantias adequadas, é realizado com base no consentimento explícito dos participantes. Estes foram previamente informados sobre os riscos associados à transferência para um país terceiro sem um nível de proteção de dados equivalente ao da União Europeia.

Exemplo 6: Subcontratação com cláusulas contratuais-tipo

Uma universidade portuguesa desenvolve um projeto de investigação em que os dados pessoais recolhidos são tratados por uma empresa de apoio à análise estatística sediada nas Filipinas, país que não beneficia de uma decisão de adequação da Comissão Europeia. Para assegurar a legalidade da transferência internacional de dados pessoais no âmbito da subcontratação, a universidade celebra com a empresa subcontratada um acordo com base em cláusulas contratuais-tipo aprovadas pela Comissão Europeia, garantindo assim um nível adequado de proteção dos dados, conforme exigido pelo artigo 46.º do RGPD.

Perguntas de controlo

O país para o qual vai exportar ou importar dados pessoais pertence ao Espaço Económico Europeu?

Se sim, a transferência de dados pessoais não requer medidas adicionais específicas, uma vez que estes países estão sujeitos ao RGPD, pelo que a circulação de dados pode ocorrer de forma direta, sem necessidade de autorizações suplementares.

Se não, o investigador deverá averiguar se existe uma decisão de adequação da Comissão Europeia (artigo 45º do RGPD) ou se existem garantias adequadas (artigo 46º do RGPD).

1. A base legal prevista para a recolha dos dados é o consentimento?

a) Se não existir decisão de adequação, deve ser verificada a existência ou a possibilidade de assegurar garantias adequadas, designadamente: cláusulas contratuais-tipo de proteção de dados ou outros mecanismos previstos no art. 46.º RGPD. Para esse efeito, o investigador deve procurar o apoio do serviço competente no domínio jurídico e de investigação da sua instituição. Caso existam garantias adequadas, o consentimento deve fazer referência às garantias adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.

Na ausência de garantias adequadas, a transferência de/para um país terceiro poderá ser efetuada desde que o consentimento seja, além de informado e específico, também explícito (expresso), nos termos do artigo 49.º, n.º 1, alínea a) do RGPD e possua as menções especiais:

- O consentimento deve mencionar a inexistência de decisão de adequação e a inexistência de garantias adequadas;

- O consentimento deve informar o titular de dados dos possíveis riscos para si próprio de tais transferências, devido à falta de uma decisão de adequação e das garantias adequadas.

b) Se existir decisão de adequação o consentimento informado, específico e inequívoco do titular de dados em causa não requer a explicitação das menções especiais já referidas.

2. A base legal prevista para a recolha dos dados é outra que não o consentimento?

a) O investigador deve verificar se o país terceiro tem decisão de adequação da Comissão Europeia. Se houver decisão de adequação, a transferência é permitida, de acordo com o art. 45º, sem necessidade das medidas adicionais específicas previstas nos art.ºs 46º-49º do RGPD.

b) Se o país terceiro não tem decisão de adequação, recomenda-se a consulta do serviço competente no domínio jurídico e de investigação da sua instituição. O investigador deve garantir, com o apoio do serviço competente no domínio jurídico e de investigação da sua instituição, que foi adotada uma das garantias adequadas previstas no RGPD (artigo 46º RGPD). Consideram-se garantias adequadas as seguintes:

- Cláusulas contratuais-tipo (CCT) aprovadas pela Comissão Europeia**;**

- Regras vinculativas aplicáveis às empresas (*Binding Corporate Rules*);

- Códigos de conduta ou mecanismos de certificação.

c) Na falta de uma decisão de adequação e de garantias adequadas, ainda é possível realizar transferências de dados pessoais, em situações excecionais, desde que se assegurem uma das condições adicionais previstas pelo RGPD (artigo 49º RGPD):

- Através de consentimento explícito, com as menções especiais descritas acima no ponto 1a).

- Celebração ou execução de um contrato no interesse, ou a pedido, do titular dos dados;

- Para proteger interesses vitais do titular de dados;

- Para defesa de um direito num processo judicial;

- Importantes razões de interesse público.

Na avaliação deste fator crítico de risco, quando a transferência de dados pessoais ocorre dentro do EEE ou para países com decisão de adequação, o risco é geralmente considerado reduzido, uma vez que as normas de proteção de dados aplicáveis são equivalentes às da União Europeia.

Por outro lado, quando a transferência internacional de dados pessoais envolve países fora do EEE sem decisão de adequação, pode constituir um fator de risco moderado ou elevado, exigindo salvaguardas adicionais e uma avaliação cuidadosa dos impactos sobre os direitos e liberdades dos titulares. Entre os fatores que podem aumentar o risco de países sem decisão de adequação, exemplificam-se:

- Ausência de legislação específica de proteção de dados, deixando os titulares sem garantias adequadas de privacidade.
- Acesso desproporcional por autoridades públicas, incluindo vigilância governamental sem mecanismos eficazes de recurso.
- Fragilidade de mecanismos de supervisão e de reparação, abrangendo autoridades independentes insuficientes e meios limitados de recurso em caso de violações.
- Diferenças culturais, políticas ou jurídicas que possam afetar a proteção de direitos fundamentais.
- Infraestrutura tecnológica e segurança cibernética vulneráveis, aumentando a probabilidade de vazamento ou uso indevido de dados.

Ligações úteis:

- European Data Protection Board. (n.d.). *Transferências internacionais de dados.* Disponível em: https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_pt

- European Data Protection Board. (2021). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.* Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

- European Data Protection Board. (2020). *Perguntas frequentes sobre o acórdão do Tribunal de Justiça da União Europeia no Processo C-311/18 – Data Protection Commissioner contra Facebook Ireland Limited e Maximillian Schrems*. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_faqs_schrems_ii_202007_adopted_pt.pdf

- European Commission. (2021). *Standard contractual clauses (SCCs).* Disponível em: https://commission.europa.eu/publications/publications-standard-contractual-clauses-sccs_en

- European Data Protection Board. (2018). *Diretrizes 2/2018 relativas às derrogações do artigo 49.º do Regulamento (UE) 2016/679.* Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_pt.pdf

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para volta ao nó anterior – Dados sensíveis (Nó 7a))

Carregue aqui para avançar para o nó seguinte – Menores de idade ou populações vulneráveis (Nó 7c))

7c). Menores de idade ou populações vulneráveis?

Clarificação de conceitos

Crianças

O RGPD determina que "as crianças merecem especial proteção quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais." [RGPD, considerando 38].

No entanto, o RGPD não define o conceito de criança. A referência consensual é aquela do artigo 1.º da Convenção sobre os Direitos da Criança (CDC) das Nações Unidas, que considera criança todo o ser humano menor de 18 anos, salvo se, nos termos da lei que lhe for aplicável, atingir a maioridade mais cedo.

A condição de especial vulnerabilidade das crianças deve ser considerada em todas as fases do tratamento:

- Na conceção e avaliação do impacto do tratamento, sobrevalorizando esses impactos se respeitarem a crianças.
- Na prestação de informações sobre o tratamento, adequando a linguagem, a clareza e a extensão dessas informações.
- Na obtenção de consentimento, se essa for a base legal para o tratamento. O consentimento de crianças terá de ser dado pelo seu representante legal. O artigo 8.º do RGPD prevê exceções para o consentimento no acesso a serviços da sociedade da informação (como redes sociais ou email), mas não tem aplicação em atividades de investigação.

Pessoas vulneráveis

O RGPD também não define o conceito de pessoa vulnerável, mas o Comité Europeu de Proteção de Dados (CEPD) aborda essa noção em várias orientações.[5] O CEPD entende que os titulares de dados vulneráveis podem incluir crianças, trabalhadores, pessoas com doenças mentais, requerentes de asilo, idosos, doentes e outros grupos em situação de fragilidade, bem como todos os casos em que exista um desequilíbrio na relação entre o participante e o responsável pelo tratamento. Tal desequilíbrio pode dificultar que o indivíduo consinta ou se oponha livremente ao tratamento dos seus dados, ou que exerça plenamente os seus direitos. A definição é aberta e deve ser apreciada à luz das circunstâncias concretas do tratamento e da capacidade dos participantes para compreenderem os seus impactos e protegerem os seus direitos.

Exemplos

Exemplo 1: Um estudo sobre padrões de alimentação e atividade física em crianças do 1º ciclo, que recolha dados como peso e outras medições físicas, evidencia a vulnerabilidade dos menores no tratamento de dados pessoais. O consentimento deve ser obtido junto dos encarregados de educação, mas as crianças podem sentir-se pressionadas por professores ou colegas e experienciar desconforto com a medição desses atributos. A desigualdade de poder e a menor maturidade das crianças limitam a sua liberdade para consentir, pelo que o investigador deve adotar medidas que reforcem a sua proteção. Por exemplo, assegurar que as medições sejam realizadas de forma privada, por profissionais qualificados, com possibilidade de recusa sem consequências, e garantindo que os resultados não são divulgados nem comparados entre colegas.

Exemplo 2: Para a realização de um estudo num serviço da administração pública ou numa empresa, não é normalmente adequado usar o consentimento informado como base legal para o tratamento de dados pessoais, uma vez que os empregados dificilmente têm liberdade para decidir no seu melhor interesse. Mesmo que formalmente possam recusar a participação no estudo, podem sentir que essa recusa afetaria a sua posição ou oportunidades na organização, ficando condicionados e sem plena autonomia para tomar uma decisão verdadeiramente livre e voluntária.

[5] Orientações do grupo do Artigo 29 relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD), 4 de abril de 2017.

Exemplo 3: Uma investigação conduzida por um professor universitário que utilize dados dos seus próprios alunos configura um potencial desequilíbrio de poder, dado que o tratamento de dados serve predominantemente os interesses do docente enquanto investigador. Nestas circunstâncias, o consentimento dificilmente pode ser considerado plenamente livre, pois o aluno poderá sentir-se pressionado a participar para não comprometer a sua relação com o professor ou o seu desempenho académico, interpretando a recusa como uma desvantagem face aos colegas. Assim, o investigador deve adotar medidas que assegurem uma participação genuinamente voluntária e isenta de consequências negativas para quem optar por não participar — por exemplo, recolhendo dados de alunos de outras turmas em que não exerça funções de docência.

Exemplo 4: Numa investigação com idosos em situação de doença, especialmente aqueles dependentes de cuidados médicos ou institucionais, o consentimento pode não refletir uma escolha livre e esclarecida. Um idoso internado numa instituição de saúde ou lar pode sentir-se pressionado a participar por receio de comprometer a qualidade dos cuidados ou por acreditar que a recusa seria mal interpretada pelos profissionais. Além disso, limitações cognitivas ou físicas podem dificultar a compreensão plena da informação sobre o tratamento dos dados, aumentando o risco de vulnerabilidade.

Pergunta de controlo

A sua investigação envolve o tratamento de dados pessoais de menores ou pessoas vulneráveis?

Se sim, existe um risco pelo menos moderado, podendo ser elevado na sua investigação. Procure verificar que:

- Solicita o consentimento do representante legal caso os participantes tenham menos de 18 anos; e obtém o assentimento do menor, sempre que possível, de forma adequada à sua idade e compreensão, garantindo que a criança entenda o que implica a participação.
- Adequa a linguagem, a complexidade e a extensão da informação prestada aos participantes à sua capacidade de entender o tratamento e as suas circunstâncias.
- Garante que os participantes têm condições de escolher em liberdade aceitar ou não aceitar o tratamento dos seus dados pessoais para o estudo que lhes é proposto.
- Garante que os participantes não estão condicionados no acesso aos direitos que lhes são devidos pelo tratamento dos seus dados pessoais.
- Garante que os participantes têm forma eficaz e conveniente para requerer o exercício dos seus direitos.
- Ao avaliar o impacto do tratamento nos direitos e interesses dos participantes atribui o devido valor às circunstâncias que os tornam vulneráveis.

A vulnerabilidade dos participantes deve ser compensada procurando melhorar a eficácia da prestação de informação sobre o tratamento e facilitando o exercício dos seus direitos. O desequilíbrio de poderes na relação entre os participantes e o responsável é crítica para a eficácia da proteção de dados porque o exercício dos direitos pelos participantes pressupõe a liberdade para o fazer. Assim sendo, os riscos associados ao condicionamento da liberdade de escolha dos participantes devem ser tratados e, quando isso não seja possível, a viabilidade do tratamento deve ser questionada.

Se não, não é necessário adotar medidas adicionais específicas para proteger participantes vulneráveis. O perfil dos participantes da sua investigação não indica riscos acrescidos relevantes para o exercício de direitos e liberdades, pelo que a investigação pode ser considerada de baixo risco nesse plano. Contudo, deve continuar a cumprir todas as normas gerais de proteção de dados, garantindo que o tratamento é legal, transparente e seguro.

Ligações úteis:

- Considerandos 38, 58, 71 e 75, e os artigos 6.º, 8.º e 12.º do RGPD. Disponíveis em https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

- Grupo de Trabalho do Artigo 29.º. (2017). *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é suscetível de resultar num elevado risco para efeitos do Regulamento (UE) 2016/679*. WP248 rev.01. Disponível em: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_pt.pdf

- *Lei n.º 58/2019, de 8 de agosto: Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679*. Diário da República, 1.ª série, n.º 151. Disponível em: https://files.dre.pt/1s/2019/08/15100/0000300040.pdf

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Transferências internacionais de dados pessoais (Nó 7b))

Carregue aqui para avançar para o nó seguinte – Tratamento em larga escala (Nó 7d))

7d). Tratamento em larga escala

Clarificação de conceitos

O tratamento de dados pessoais em grande escala refere-se, de forma genérica, a tratamentos que envolvem um volume significativo de dados, abrangendo um número relevante de titulares, e que possam ter impacto alargado no conjunto da população afetada. O Regulamento Geral sobre a Proteção de Dados (RGPD) não fornece, contudo, uma definição exata do que constitui "grande escala".

Para a sua apreciação, podem ser considerados os seguintes fatores:

- O número de titulares de dados afetados, seja como valor absoluto ou como percentagem da população relevante — por exemplo, uma percentagem significativa dos alunos de uma determinada instituição;
- O volume de dados tratados e/ou a variedade dos diferentes elementos de dados pessoais envolvidos;
- A duração ou carácter contínuo da atividade de tratamento;
- A abrangência geográfica da atividade de tratamento.

Exemplos

Constituem exemplos de tratamentos em grande escala:

a) O tratamento de dados por uma tecnologia utilizada por indivíduos de uma população para rastreio de contactos, como a aplicação Stayaway Covid.

b) Estudos de coorte envolvendo dezenas de milhares de participantes seguidos ao longo de vários anos para investigar fatores de risco para doenças crónicas.

c) Investigação genómica que analisa dados de sequenciação genética de uma população nacional ou de um biobanco de larga dimensão.

d) Projetos internacionais de epidemiologia que cruzam dados de diferentes países e sistemas de saúde.

e) Investigação baseada em imagens médicas (ressonâncias, TACs) recolhidas de múltiplos hospitais e armazenadas em repositórios centrais.

f) O tratamento de dados de doentes no âmbito das atividades regulares de um hospital.

g) O tratamento de dados de viagens das pessoas que utilizam o sistema de transportes públicos de uma cidade.

h) O tratamento de dados de clientes no contexto normal das atividades de uma companhia de seguros ou de um banco.

Exemplos que não constituem tratamentos em grande escala:

a) Um estudo piloto com um grupo restrito (ex.: 30 voluntários) para testar um novo questionário.

b) Um projeto de investigação local que recolhe dados de um número limitado de pacientes de uma única clínica.

c) A análise de dados com pequena amostra para validar um algoritmo antes de aplicá-lo a uma base maior.

d) O tratamento de dados de pacientes efetuado por um médico individual no exercício da sua atividade,

e) O tratamento de dados pessoais relativos a condenações penais e infrações por parte de um advogado, no âmbito de casos específicos.

Pergunta de controlo

A sua investigação envolve tratamento em larga escala?

Se sim, existe um risco pelo menos moderado, podendo ser elevado, na sua investigação, o que exige a implementação de medidas de mitigação de risco adequadas, bem como a monitorização contínua dos riscos para os participantes.

Nos casos em que o tratamento em grande escala incida sobre **categorias especiais de dados** ou de dados pessoais relacionados com condenações penais e infrações, é obrigatório, nos termos do artigo 35.º, n.º 3 do RGPD, a formalização de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) e o parecer do Encarregado de Proteção de Dados (EPD). De igual forma, estudos em larga escala que envolvam o **controlo sistemático** de zonas acessíveis ao público implicam a realização de uma AIPD e o parecer do EPD. Nestes casos, o investigador deve contactar o serviço competente no domínio de investigação da sua instituição e o Encarregado de Proteção de Dados.

Se não, a sua investigação é considerada de menor risco no contexto deste critério e não exige medidas adicionais específicas. No entanto, deve continuar a cumprir todas as normas gerais de proteção de dados, garantindo que o tratamento é legal, transparente e seguro.

Ligações úteis:

- Grupo do Artigo 29.º para a Proteção de Dados. (2017). *Secção 3. Funções do encarregado da proteção de dados*. In *Orientações sobre os encarregados da proteção de dados (DPO) (WP 243 rev.01)* (pp. 15–19). Disponível em: https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Menores de idade ou populações vulneráveis (Nó 7c))

Carregue aqui para avançar para o nó seguinte – Definição de perfis (Nó 7e))

7e). Definição de perfis

Clarificação de conceitos

A definição de perfis refere-se a qualquer forma de tratamento automatizado de dados pessoais que vise avaliar, analisar ou prever aspetos relacionados com a vida de uma pessoa, incluindo desempenho profissional, situação económica, saúde, preferências ou interesses pessoais, fiabilidade, comportamento, localização ou deslocações (art. 4.º, n.º 4, RGPD). O RGPD chama a atenção para o risco acrescido deste tipo de operações quando delas resultam efeitos jurídicos que digam respeito ao participante ou que o afetem significativamente de forma similar. Frequentemente, a perfilagem é realizada tendo em vista **decisões automatizadas**, o que potencia mais o risco para os participantes.

Em contexto de investigação, a criação de perfis nem sempre implica impacto direto ou significativo nos participantes. Frequentemente, os dados são tratados de forma agregada ou para fins analíticos, sem efeitos individuais. Contudo, se a perfilagem puder condicionar decisões, influenciar a experiência do participante ou expô-lo a riscos adicionais (por exemplo, em estudos sobre saúde, comportamento ou vulnerabilidades sociais), então podem surgir riscos acrescidos para os participantes, exigindo medidas de mitigação adequadas.

Mesmo quando a avaliação ou classificação dos participantes não é realizada de forma automatizada ou sistemática, mas manual ou pontual, continua a constituir tratamento de dados pessoais. Nestas situações, ainda que não se verifique "perfilagem" nos termos do RGPD, o investigador deve assegurar que qualquer forma de avaliação ou categorização de participantes respeita os princípios de proteção de dados, garantindo a salvaguarda dos direitos dos titulares e a mitigação dos riscos identificados.

Exemplos:

Exemplo 1: Uma instituição financeira pode recorrer a bases de dados de referências de crédito bancário para avaliar a fiabilidade e a capacidade de pagamento dos seus clientes. Com base nesses perfis, decide se concede ou não crédito, os limites aplicáveis, ou até as condições contratuais oferecidas. De igual modo, pode usar bases de dados destinadas ao combate ao Branqueamento de capitais, ao financiamento do terrorismo ou à prevenção de fraude, avaliando o grau de risco de cada cliente. Nestes casos, o perfil construído tem um impacto direto e significativo na vida das pessoas, podendo limitar o acesso a serviços financeiros essenciais.

Exemplo 2: Uma empresa de biotecnologia que fornece testes genéticos diretamente ao consumidor pode utilizar os resultados para criar perfis individuais de saúde. Esses perfis servem para prever riscos de desenvolvimento de determinadas doenças ou condições clínicas, bem como para recomendar medidas preventivas ou planos de estilo de vida. Embora possam trazer benefícios para os participantes, também envolvem riscos acrescidos de discriminação ou estigmatização caso essa informação seja mal utilizada, nomeadamente por seguradoras, empregadores ou outras entidades.

Exemplo 3: Um estudo em Psicologia recolhe dados pessoais identificáveis (nome, idade, género) e resultados de questionários sobre hábitos de estudo dos alunos universitários. Esses dados são usados para construir perfis de estilos de aprendizagem, mas apenas para análise estatística e publicação de resultados agregados. Nenhum perfil individual é comunicado aos próprios alunos ou a terceiros, nem utilizado para decisões que afetem diretamente a sua vida académica. Apesar de envolver dados pessoais, o impacto sobre os participantes é reduzido, porque os perfis não são aplicados de forma a condicionar direitos, oportunidades ou avaliações individuais.

Exemplo 4: Num estudo clínico, investigadores recolhem dados pessoais e clínicos de pacientes diabéticos, incluindo exames laboratoriais e históricos médicos, para desenvolver perfis de resposta a um novo tratamento. Com base nesses perfis, alguns participantes podem ser excluídos de fases posteriores do estudo ou receber regimes terapêuticos diferenciados. Além disso, esses perfis individuais podem influenciar perceções sobre o seu prognóstico de saúde e, se usados de forma indevida, expô-los a discriminação (por exemplo, junto de seguradoras). Aqui, a perfilagem tem impacto direto e significativo na vida dos participantes, criando riscos acrescidos para os participantes.

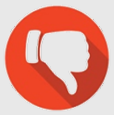
Exemplo 5: Numa plataforma de ensino à distância, podem ser recolhidos e analisados dados relativos às atividades dos alunos, como o tempo de acesso, número de tentativas em testes, participação em fóruns ou até padrões de navegação no ambiente virtual. Estes dados são usados para construir perfis de desempenho e comportamento, permitindo ao docente identificar dificuldades, adaptar metodologias e aplicar pedagogias diferenciadas para melhorar os objetivos de aprendizagem. Apesar do potencial benefício para a personalização do ensino e para o sucesso académico dos alunos, este tipo de perfis pode levantar riscos relacionados com a estigmatização de estudantes, a criação de expectativas limitadoras e a exposição desnecessária de informação sensível sobre o seu percurso educativo.

Pergunta de controlo

A sua investigação envolve a definição de perfis?

Se sim, deve avaliar-se se a definição de perfis tem impacto significativo sobre os participantes. Este tipo de tratamento pode incidir em aspetos como a saúde, o comportamento, os interesses pessoais ou o desempenho académico/profissional e, consoante o contexto, pode gerar riscos acrescidos para os seus direitos, liberdades e garantias.

Quando exista impacto significativo, a investigação apresenta pelo menos um risco moderado, podendo mesmo ser elevado. Nestes casos, torna-se indispensável implementar medidas de mitigação para proteger os participantes, bem como assegurar a monitorização contínua dos riscos a que estão expostos.



Se não, a sua investigação é considerada de menor risco no âmbito deste critério e não exige medidas adicionais específicas. No entanto, deve continuar a cumprir todas as normas gerais de proteção de dados, garantindo que o tratamento é legal, transparente e seguro.

Ligações úteis:

- Artigo 4.º, n.º 4 do RGPD, e Considerandos 72 e 91. Disponíveis em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679#art_4

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Tratamento em Larga Escala (Nó 7d))

Carregue aqui para avançar para o nó seguinte – Decisões automatizadas por algoritmos (Nó 7f))

7f). Decisões automatizadas por algoritmos?

Clarificação de conceitos

Decisões automatizadas por algoritmos, designadas no RGPD por *decisões individuais automatizadas*, correspondem a formas de tratamento de dados em que uma decisão relativa a um participante na investigação é tomada de forma exclusivamente automática, sem intervenção humana significativa, com a possibilidade de produzir efeitos jurídicos ou impactos relevantes na vida do indivíduo. Um exemplo pode ser a utilização de algoritmos que, com **base em perfis**, determinem o acesso a crédito, a elegibilidade para determinados apoios sociais, o acesso a um programa universitário, ou a exclusão de outras oportunidades, implicando potenciais situações de discriminação. Na prática, estas decisões são frequentemente geradas por **sistemas de inteligência artificial**, que processam grandes volumes de dados e podem produzir resultados em que questões como a transparência e a explicabilidade devem ser cuidadosamente consideradas e asseguradas.

O participante tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar, salvo se o tratamento for baseado em **consentimento explícito**.

Em contexto de investigação, as decisões automatizadas nem sempre implicam impacto direto ou significativo nos participantes, na medida em que são utilizadas para fins de investigação, em contexto experimental ou de simulação. No entanto, quando existem decisões exclusivamente automatizadas e as decisões daí resultantes afetam significativamente o participante, estamos pelo menos perante um cenário de risco moderado, podendo mesmo ser elevado, exigindo medidas de mitigação adequadas.

Exemplos:

Exemplo 1: Investigação em Saúde Pública

Durante a pandemia de COVID-19, investigadores em epidemiologia de um laboratório multinacional desenvolveram e testaram computacionalmente um sistema automatizado para definir prioridades de vacinação, com base em dados reais de pacientes, como idade, historial médico e fatores de risco. Na fase de investigação, este processo não produzia impacto direto nos participantes, pois os dados estariam anonimizados e tratava-se apenas de simular cenários e avaliar a eficácia e a equidade do algoritmo na priorização de grupos de risco. No entanto, caso o sistema viesse a ser adotado por uma autoridade de saúde, as decisões automatizadas passariam a determinar efetivamente quem receberia a vacina primeiro, com consequências imediatas e significativas para a saúde e a segurança das pessoas.

Exemplo 2: Investigação em Ciências Sociais e Criminalidade

Uma equipa utiliza um modelo de scoring automatizado para avaliar o risco de reincidência criminal entre participantes de um estudo. O algoritmo classifica indivíduos em diferentes níveis de risco, podendo influenciar recomendações sobre medidas de reintegração ou supervisão. O modelo foi desenvolvido exclusivamente para fins de investigação científica e não produziu efeitos jurídicos nem consequências práticas imediatas para os participantes, uma vez que não foi adotado em nenhuma decisão judicial ou administrativa. Para além disso, foram implementadas **medidas técnicas e organizativas** rigorosas, como a confidencialidade dos dados, controlos de acesso restritos e a anonimização dos resultados, de forma a proteger os participantes e reduzir os riscos éticos e legais. Ainda assim, o estudo foi publicado numa revista científica com elevado impacto, o que sugere que os resultados e métodos poderão, a médio ou longo prazo, influenciar políticas públicas ou decisões reais relacionadas com a justiça criminal, aumentando o potencial de impacto indireto sobre pessoas em situações semelhantes.

Exemplo 3: Investigação em Educação no Ensino Superior

Uma equipa de investigação de uma universidade desenvolve e testa um algoritmo para prever o risco de abandono escolar dos alunos dessa mesma universidade, com base em dados académicos, socioeconómicos e de assiduidade dos estudantes. O algoritmo é utilizado para identificar e recomendar acompanhamento adicional aos alunos, sem intervenção humana nas recomendações. As decisões automatizadas geradas pelo modelo podem influenciar diretamente quais os estudantes que recebem ou não apoio e programas de acompanhamento, produzindo efeitos significativos sobre a vida académica e as oportunidades educativas dos alunos dessa instituição.

Pergunta de controlo

A sua investigação envolve decisões automatizadas por algoritmos?

Se sim, este é um fator crítico de risco, importando avaliar se as decisões automatizadas por algoritmos têm impacto significativo sobre os participantes, caso em que a investigação apresenta pelo menos um risco moderado, podendo mesmo ser elevado. Nestes casos, torna-se indispensável implementar medidas de mitigação para proteger os participantes, bem como assegurar a monitorização contínua dos riscos a que estão expostos.

Se não, a sua investigação é considerada de menor risco no âmbito deste critério e não exige medidas adicionais específicas. No entanto, deve continuar a cumprir todas as normas gerais de proteção de dados, garantindo que o tratamento é legal, transparente e seguro.

Ligações úteis

- Artigo 35.º, n.º 3 alínea a) do RGPD. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679#art_35

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Definição de perfis (Nó 7e))

Carregue aqui para avançar para o nó seguinte – Monitorização sistemática (Nó 7g))

7g). Controlo sistemático?

Clarificação de conceitos

Controlo sistemático é uma forma de tratamento de dados que consiste em observar, monitorizar ou controlar pessoas, incluindo a recolha de dados através de redes ou o «controlo sistemático de zonas acessíveis ao público». A captação de vídeo para analisar os trajetos utilizados por pessoas em circulação num edifício acessível ao público, como uma universidade, configura uma situação de controlo sistemático.

O controlo sistemático não se limita a videovigilância — abrange qualquer forma contínua, organizada e potencialmente intrusiva de recolher e analisar dados pessoais.

De acordo com o art. 35.º, n.º 3, alínea c), do RGPD, a realização de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) é obrigatória no caso de "controlo sistemático de zonas acessíveis ao público em grande escala". Nestes casos, a equipe de investigação deve formalizar a AIPD, contactar o serviço competente no domínio de investigação da sua instituição e solicitar o parecer do Encarregado de Proteção de Dados.

Exemplos:

Exemplo 1: Controlo sistemático com recolha e tratamento de dados pessoais

Uma equipa de investigadores em Serviço Social pretende analisar as imagens de videovigilância de um terminal multimodal de transportes públicos, com o objetivo de identificar o número de pessoas em situação de sem-abrigo que pernoitam regularmente na estação. Esta análise das imagens configura uma situação de controlo sistemático, uma vez que envolve a observação e monitorização contínua de indivíduos em espaços públicos. Acresce ainda que estas pessoas pertencem a uma população vulnerável e não foram informadas de que as imagens de videovigilância seriam utilizadas para aquele fim específico, o que levanta questões de natureza ética e legal.

Exemplo 2: Controlo sistemático de atividade online com recolha e tratamento de dados pessoais

Uma equipa de investigação em ciências sociais pretende estudar padrões de participação em fóruns e redes sociais públicas, analisando tópicos, frequência de publicações e interações entre utilizadores. Para tal, recorre a ferramentas automatizadas que recolhem de forma contínua conteúdos publicados e metadados associados aos perfis, como endereços IP, horários e frequência de acessos. Esta recolha contínua, estruturada e direcionada para o acompanhamento de comportamentos individuais configura controlo sistemático, uma vez que permite observar, monitorizar e acompanhar a atividade online de pessoas potencialmente identificáveis.

Exemplo 3: Controlo sistemático com possibilidade de identificação indireta dos participantes

Uma equipa de investigação em mobilidade urbana acedeu a dados de georreferenciação das antenas de telemóvel para analisar padrões de deslocação da população na cidade. Os dados permitiram identificar trajetos mais frequentes, horários de maior circulação e fluxos entre diferentes zonas urbanas. Apesar de não incluírem diretamente informações pessoais como nomes ou contactos, a recolha contínua e sistemática de localização de milhares de telemóveis constitui um tratamento em grande escala e de monitorização sistemática, capaz de possibilitar a identificação indireta dos indivíduos associados. Nestas circunstâncias, a Avaliação de Impacto era obrigatória, tendo sido devidamente aprofundada e formalizada, com parecer solicitado ao Encarregado de Proteção de Dados.

Exemplo 4: Monitorização sistemática de fluxos de passageiros sem recolha nem tratamento de dados pessoais

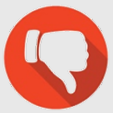
No mesmo terminal multimodal de transportes públicos do Exemplo 1, a equipa de investigação do Exemplo 3 pretende analisar os fluxos de passageiros entre comboio, metro e autocarro, de modo a propor alterações ao desenho da rede e dos serviços. Em vez de recorrer a imagens de videovigilância da estação, a equipa optou por instalar sensores que não recolhem dados pessoais, limitando-se a realizar contagens e medições de fluxos em determinados pontos da estação. Como não há recolha nem tratamento de dados pessoais, o RGPD não se aplica, garantindo-se ao mesmo tempo a proteção da privacidade dos utilizadores e a obtenção da informação necessária para os objetivos do estudo.

Pergunta de controlo

A sua investigação envolve controlo sistemático?

Se sim, este é um fator crítico de risco, fazendo com que a investigação apresente, no mínimo, um risco moderado, podendo mesmo configurar um risco elevado.

Se o controlo é realizado em zonas acessíveis ao público e em grande escala, deve ser formalizada uma Avaliação de Impacto sobre a Proteção de Dados (AIPD), conforme previsto no Artigo 35.º do RGPD, e a obtenção do parecer do Encarregado de Proteção de Dados (EPD). Este aprofundamento da avaliação de impacto permitirá identificar, antecipar e mitigar possíveis impactos sobre os direitos e liberdades dos participantes. Para tal, deverá contactar o serviço competente no domínio de investigação da sua instituição e o Encarregado de Proteção de Dados.



Se não, a sua investigação é considerada de menor risco no âmbito deste critério e não exige medidas adicionais específicas. No entanto, deve continuar a cumprir todas as normas gerais de proteção de dados, garantindo que o tratamento é legal, transparente e seguro.

Ligações úteis

- Artigo 35.º, n.º 3 alínea c) do RGPD. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679#art_35

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Decisões automatizadas por algoritmos (Nó 7f))

Carregue aqui para avançar para o nó seguinte – Combinação de base de dados (Nó 7h))

7h). Combinam-se bases de dados?

Clarificação de conceitos

Em contexto de investigação, a combinação de bases de dados pode ser entendida como o tratamento que resulta da integração de dados provenientes de **duas ou mais fontes**, realizadas com diferentes finalidades e/ou por diferentes **responsáveis pelo tratamento**. Quando essa combinação é realizada, pode exceder-se as expectativas razoáveis dos participantes, na medida em que informações recolhidas para um determinado fim passam a ser utilizadas para outro, podendo revelar perfis mais detalhados ou sensíveis do que inicialmente previsto. Por isso mesmo, este tipo de tratamento é suscetível de aumentar o risco para os participantes.

Exemplos

Exemplo 1: Uma equipa de investigação em educação pretende analisar fatores que influenciam o sucesso académico dos alunos de uma universidade. Para tal, pretende combinar os dados internos sobre percurso curricular e desempenho académico dos estudantes com informações públicas recolhidas nas redes sociais dos mesmos alunos, como interesses, atividades extracurriculares e postagens relevantes. Esta combinação de bases de dados permitirá **definir perfis** mais detalhados e abrangentes do comportamento e características dos alunos, mas pode exceder as expectativas razoáveis de uso dos seus dados pessoais e, por isso, pode constituir-se como um tratamento com maior risco para os participantes.

Exemplo 2: Uma equipa de investigação em saúde pública pretende analisar a relação entre a utilização de serviços de troca de seringas e a incidência de infeção por VIH na população toxicodependente. Para tal, pretende combinar registos internos dos serviços de troca de seringas com dados de pessoas em tratamento ao VIH. A integração de bases de dados permitirá identificar padrões de risco e avaliar a eficácia das intervenções. Porém, importa notar que os serviços de troca de seringas atendem também outras condições de saúde, como diabetes, e que a maioria dos infetados com VIH não são consumidores de drogas injetáveis. A integração destas duas bases de dados pode exceder as expectativas razoáveis dos participantes que cederam os seus dados, aumentando o risco de identificação, estigmatização ou discriminação. Acresce que está em causa o tratamento de dados de saúde, ou seja, **categorias especiais de dados**. A conjugação destes dois fatores de risco configura um projeto com elevado risco para os participantes, impondo a formalização de uma AIPD e o parecer do Encarregado de Proteção de Dados

Pergunta de controlo

A sua investigação estabelece correspondências ou combina conjuntos de dados?

Se sim, essa situação pode constituir um fator crítico de risco, fazendo com que a investigação apresente, no mínimo, um risco moderado, podendo mesmo configurar um risco elevado.

Se não, a sua investigação é considerada de menor risco no âmbito deste critério e não exige medidas adicionais específicas. No entanto, deve continuar a cumprir todas as normas gerais de proteção de dados, garantindo que o tratamento é legal, transparente e seguro.

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Monitorização sistemática (Nó 7g))

Carregue aqui para avançar para o nó seguinte – Inteligência Artificial e outras soluções tecnológicas (Nó 7i))

7i). Envolve Inteligência Artificial ou outras novas soluções tecnológicas?

Clarificação de conceitos

A utilização de soluções tecnológicas ou organizacionais inovadoras pode introduzir riscos acrescidos para os participantes, devido à incerteza quanto às suas consequências pessoais, sociais e éticas. Entende-se por nova tecnologia aquela que representa avanços face ao "nível de conhecimentos tecnológicos alcançado" (artigo 35.º, n.º1 e considerandos 89 e 91 do RGPD). A introdução de tecnologias inovadoras, mesmo em contexto de investigação científica, além de implicar o cumprimento dos requisitos nos nós **Software** ou **Subcontratação**, pode envolver novas formas de recolha, análise ou utilização de dados pessoais – frequentemente automatizadas, complexas ou de difícil explicação ao participante –, com potencial para gerar impactos desconhecidos na privacidade, autonomia e dignidade das pessoas, pelo que requer uma avaliação prévia e adoção de medidas de mitigação adequadas.

A IA generativa e os modelos de linguagem em grande escala

Entre as tecnologias emergentes dos últimos anos, destacam-se as baseadas em Inteligência Artificial (IA), em particular os modelos de linguagem de grande escala (Large Language Models – LLMs), como o ChatGPT e sistemas análogos. Estas ferramentas, frequentemente disponibilizadas por entidades externas, não controladas pelas instituições de investigação, levantam desafios quanto à origem e à natureza dos dados dos conjuntos de treino, com potencial para incluir dados pessoais (ou outros dados sensíveis ou **protegidos por direitos de autor**). A sua utilização — seja para criar chatbots de recomendação, gerar conteúdos automatizados, apoiar análises qualitativas ou resumir dados de investigação — exige avaliar se ocorre tratamento de dados pessoais e, em caso afirmativo, assegurar o dever de informação ao participante, bem como a legitimidade, minimização e segurança do tratamento.

Estes modelos colocam também desafios significativos ao exercício do direito ao apagamento. Os dados pessoais utilizados no treino destes sistemas passam a estar incorporados nos parâmetros do modelo, o que dificulta a identificação ou a remoção seletiva dessa informação sem comprometer a integridade global do sistema. O cumprimento do direito ao apagamento (artigo 17.º do RGPD) pode, por isso, tornar-se tecnicamente inviável ou extremamente complexo. Tal não dispensa, por conseguinte, o investigador de garantir, antes do início do tratamento, que evita a introdução de dados pessoais em sistemas externos. Sempre que tal seja inevitável ou justificado, deve ainda informar claramente os participantes sobre a forma como os seus dados serão utilizados, os eventuais riscos associados e as limitações técnicas existentes ao exercício dos seus direitos.

Mesmo quando empregues apenas como apoio indireto à atividade científica, estas ferramentas comportam riscos, incluindo a exposição de dados confidenciais, produção de resultados enviesados ou incorretos ("alucinações") e a dependência excessiva de sistemas não auditáveis. O recurso à IA generativa requer, portanto, cautela acrescida, apreciação do risco e, quando aplicável, documentação das medidas de mitigação adotadas, incluindo a garantia de supervisão humana sobre todos os resultados produzidos.

Outras IAs e sistemas automatizados

Para além da abordagem generativa, existem outros paradigmas e técnicas de IA, Ciência de Dados e Estatística que não produzem novo conteúdo, mas analisam, classificam ou predizem com base em dados existentes. Incluem-se abordagens simbólicas (e.g. baseadas em regras e ontologias), estatísticas e de aprendizagem automática, incluindo a profunda, utilizadas em modelos de análise preditiva, reconhecimento de padrões, classificação automática ou apoio à decisão. Estes sistemas são frequentemente aplicados em contextos de análise de dados comportamentais, sociais ou biomédicos, na identificação de tendências ou modelação de fenómenos complexos.

Em investigação científica, o impacto sobre os participantes pode ser menos direto, uma vez que estes sistemas são, tipicamente, utilizados para fins exploratórios ou de validação experimental, sem efeitos imediatos sobre pessoas identificáveis. Mas não se pode assumir a ausência de risco: o uso destas tecnologias está normalmente associado a outros fatores críticos de risco já mencionados —

a definição de perfis e as decisões automatizadas por algoritmos, ou mesmo o controle sistemático. Sempre que forem usados algoritmos para criar perfis individuais ou suportar decisões automatizadas com impacto sobre pessoas, o risco do tratamento deve ser considerado igualmente no âmbito desses nós, assegurando transparência, possibilidade de contestação e intervenção humana significativa nos processos de análise e decisão.

Acresce que outros riscos podem emergir, por exemplo, a reidentificação de dados anonimizados ou pseudonimizados, a propagação de enviesamentos ocultos nos conjuntos de dados ou a interpretação incorreta de resultados automatizados que possam vir a fundamentar decisões futuras. Mesmo em ambiente experimental, deve avaliar-se o potencial de impacto a médio prazo, sobretudo quando os resultados possam ser reutilizados ou transferidos para aplicações práticas.

Os riscos da IA no plano da privacidade

1. Viés algorítmico e discriminação: Os sistemas de IA aprendem a partir de dados históricos, podendo refletir padrões sociais, culturais ou institucionais de desigualdade. Quando esses enviesamentos não são detetados nem corrigidos, podem reproduzir ou amplificar discriminações indiretas com base em género, origem, idade, saúde ou outros fatores. Circunstâncias que podem afetar a qualidade e imparcialidade dos resultados, comprometendo a validade científica e ética do estudo.

2. Opacidade e dificuldade no exercício do direito à explicação: Muitos algoritmos de IA — sobretudo baseados em aprendizagem profunda — funcionam como "caixas negras", dificultando a compreensão dos critérios que sustentam as suas conclusões. Essa opacidade compromete a transparência do tratamento e pode limitar o direito dos participantes a compreenderem como os seus dados são utilizados ou como determinados resultados foram obtidos. Sempre que as limitações na explicabilidade possam influenciar decisões automatizadas com impacto sobre as pessoas, o risco deve ser avaliado em articulação com o Nó Decisões automatizadas por algoritmos.

3. Reutilização indevida de dados pessoais: Os sistemas de IA são frequentemente reutilizados em contextos distintos daqueles para os quais os dados foram recolhidos. Tal prática pode gerar tratamentos secundários não autorizados, violando o dever de informação ou o consentimento do participante, especialmente quando os dados passam a ser processados por terceiros ou integrados em conjuntos de treino.

4. Dificuldades no exercício de direitos, em especial o apagamento: O exercício dos direitos de acesso, oposição ou apagamento torna-se tecnicamente difícil quando os dados são incorporados em modelos de IA, cujos parâmetros não permitem identificar ou remover informação específica sem afetar o desempenho global. Esta limitação não dispensa o investigador de assegurar, na origem, medidas de minimização de dados e de informar os participantes sobre tais restrições.

5. Dependência tecnológica e transferência de controlo: A utilização de plataformas ou modelos de IA fornecidos por entidades externas, tal qual abordado no Nó Software, pode criar situações de dependência tecnológica e perda de controlo institucional sobre os dados pessoais tratados. Esta dependência aumenta o risco de acesso indevido, transferências internacionais não previstas e dificuldade na definição de responsabilidades entre a instituição e os seus subcontratantes.

Outras tecnologias inovadoras suscetíveis de risco

1. Tecnologias biométricas e de reconhecimento automático: A utilização de dados biométricos, como impressões digitais, reconhecimento facial, de voz ou íris, para fins de autenticação ou identificação, envolve tratamentos de dados particularmente sensíveis. Em investigação, a recolha e armazenamento destas informações exigem justificação científica robusta, consentimento explícito, medidas reforçadas de segurança e anonimização ou pseudonimização, evitando reutilização fora do contexto do estudo, salvo com medidas de mitigação de risco apropriadas.

2. Internet das Coisas (IoT) e dispositivos conectados: Sensores, wearables e aplicações móveis podem recolher grandes volumes de dados pessoais — muitas vezes de forma contínua e em tempo real. Em contexto de investigação, o risco reside na dificuldade de controlo do ciclo completo dos dados, especialmente quando dependem de plataformas comerciais ou quando a recolha é passiva, isto é, sem ação consciente do participante. Entre outras medidas, devem ser privilegiados métodos de **minimização**, **recolha local** e **transmissão cifrada**.

3. Tecnologias de registo distribuído (Blockchain e afins): A imutabilidade das transações em sistemas blockchain pode dificultar ou inviabilizar o **exercício do direito ao apagamento e a retificação de dados**. Uma solução em investigação científica passa por garantir que os dados pessoais não são registados diretamente na cadeia, mas apenas referências ou hashes anonimizados.

4. Tecnologias de monitorização e vigilância: Soluções que envolvem a gravação de vídeo, áudio, geolocalização ou monitorização comportamental contínua podem ter impacto grave na privacidade dos participantes. Mesmo quando utilizadas apenas para fins experimentais, devem ser objeto de avaliação de risco prévia, assegurando proporcionalidade, limitação temporal e informação clara aos participantes sobre o âmbito e as condições do tratamento. Sempre que estas tecnologias impliquem observação sistemática de pessoas em espaços físicos ou digitais, o risco deve ser analisado em articulação com o nó **Controlo Sistemático**.

Síntese e avaliação do risco

A utilização das tecnologias mencionadas, bem como de outras tecnologias ou contextos organizacionais inovadores, deve ser tratada como um fator crítico de risco, dadas as incertezas que podem envolver a recolha, análise e reutilização de dados pessoais. Na apreciação do risco, importa considerar o grau de novidade tecnológica, a escala e complexidade do tratamento e o potencial impacto nos direitos fundamentais dos participantes – incluindo a privacidade, a justiça e a não discriminação –, bem como nos valores éticos da investigação científica, como a transparência, a responsabilidade, a proporcionalidade (enquanto ponderação na minimização de riscos e danos), a autonomia dos participantes e a confiança na relação entre investigadores, participantes e sociedade.

Em grande medida, o risco deve ser avaliado caso a caso, em função do contexto da investigação e do nível de incerteza tecnológica, com consulta prévia à comissão de ética ou ao Encarregado de Proteção de Dados, sempre que se prevejam impactos significativos nos direitos ou liberdades dos participantes.

Exemplos:

Exemplo 1: Aplicação de algoritmos preditivos em projetos biomédicos

Num estudo sobre progressão de doenças, investigadores utilizam um modelo de aprendizagem profunda para prever respostas ao tratamento com base em dados clínicos e genéticos. O sistema aprende a partir de dados históricos e pode reproduzir enviesamentos existentes nos registos (viés algorítmico). Ainda que o estudo não envolva decisões clínicas diretas, o risco é elevado devido à sensibilidade dos dados e ao impacto potencial nas conclusões científicas.

Exemplo 2: Utilização de modelos de linguagem de grande escala (LLMs)

Um grupo de investigação em ciências sociais utiliza um modelo de linguagem como o ChatGPT para apoiar a análise e síntese automática de entrevistas com participantes. Embora os dados sejam pseudonimizados, o conteúdo textual contém descrições pessoais sensíveis. O envio dessas transcrições para uma plataforma externa configura tratamento de dados pessoais fora do controlo institucional, com riscos de violação de confidencialidade, impossibilidade de apagamento e reutilização indevida dos dados. Como medidas de mitigação, a equipa privilegiou o uso de versões anonimizadas ou sintetizadas das transcrições, soluções locais ou **contratualmente protegidas**, com cláusulas que assegurem a não reutilização e a eliminação dos dados. No consentimento informado foi explicitado que parte da análise pode recorrer a sistemas de IA externos, indicando os riscos potenciais e as salvaguardas adotadas, bem como a possibilidade de o participante optar por não autorizar esse tipo de tratamento.

Exemplo 3: Uso de sensores IoT em estudos de comportamento

Um projeto de investigação em psicologia instala sensores de movimento e câmaras em espaços de trabalho para observar padrões de colaboração. A recolha contínua e passiva de dados (incluindo áudio e imagem) configura monitorização sistemática de pessoas e exige avaliação de risco prévio, devendo ser analisado em articulação com o Nó Controlo Sistemático.

Perguntas de controlo

1. A investigação envolve o uso, aplicação ou desenvolvimento de tecnologias de IA, reconhecimento biométrico, Internet das Coisas (IoT), blockchain ou tecnologias de monitorização e vigilância que envolvem, ou são suscetíveis de envolver, o tratamento de dados pessoais?

2. A investigação recorre a tecnologias que representam um avanço face ao nível de conhecimento tecnológico atual, implicando novas formas de recolha, análise ou reutilização de dados pessoais, cujas consequências são ainda pouco conhecidas?

3. São utilizadas tecnologias que tratam dados pessoais e que podem gerar impactos desconhecidos na privacidade, autonomia ou noutros direitos fundamentais dos participantes?

Se respondeu não a todas as questões anteriores, a sua investigação é considerada de menor risco no âmbito deste critério e não exige medidas adicionais específicas. No entanto, deve continuar a cumprir todas as normas gerais de proteção de dados, garantindo que o tratamento é legal, transparente e seguro.

Se respondeu sim a qualquer uma das questões anteriores existe um risco pelo menos moderado, podendo mesmo ser elevado no plano deste critério. O projeto utiliza tecnologias suscetíveis de introduzir riscos acrescidos para os participantes, a serem identificados, ponderados e mitigados.

Verifique:

Dependência tecnológica e transferência de dados

• Foram assegurados os requisitos do Nó Software?

• A tecnologia utilizada envolve a transferência internacional de dados?

• Foram avaliadas as garantias contratuais e de segurança oferecidas pelos fornecedores externos ou prestadores de serviços em cloud?

Transparência e dever de informação

- Assegurou o dever de informação ao participante, mencionando na Ficha de Informação do formulário de consentimento o uso da tecnologia inovadora e os impactos ou riscos previsíveis para o participante?
- Indicou expressamente se a investigação envolve a geração de conteúdos sintéticos, como texto, imagem, voz, vídeo ou outros dados produzidos por sistemas de IA (por exemplo, *deepfakes*), esclarecendo a natureza artificial desses conteúdos?
- Foram definidos procedimentos para explicar de forma compreensível o funcionamento básico da tecnologia e os riscos potenciais?
- Existe um plano para responder a **pedidos de informação ou exercício de direitos** (acesso, apagamento, oposição)?

IA generativa e redes de aprendizagem profunda

- Caso sejam tratados dados pessoais através de redes de aprendizagem profunda, incluindo componentes generativas, **informou os participantes** sobre os limites técnicos do direito de acesso e apagamento dos seus dados pessoais?
- Se forem usadas ferramentas de aprendizagem generativa fora do controlo institucional (por exemplo, ChatGPT):
  - Assegurou a **anonimização** ou a **pseudonimização** prévia dos dados antes de os submeter à ferramenta?
  - Sempre que possível, **privilegiou soluções locais em detrimento de soluções SaaS**?
  - Caso não tenha sido possível anonimizar integralmente os dados, avaliou a legitimidade do tratamento e ponderou os riscos associados à sua utilização?
  - Configurou a ferramenta de forma a impedir a reutilização ou retenção dos dados submetidos para fins de treino, melhoria do sistema ou personalização da experiência do utilizador?

Qualidade, viés e auditabilidade dos sistemas

- Foram avaliadas a origem, qualidade e representatividade dos dados usados para treinar, validar ou testar algoritmos, de modo a reduzir enviesamentos e prevenir discriminação?
- Existem mecanismos de auditoria ou supervisão humana definidos (quem, quando e como intervém) sobre as **decisões ou análises geradas por sistemas automatizados**?
- Foram avaliadas as limitações técnicas e a auditabilidade das tecnologias utilizadas, incluindo a possibilidade de verificação independente dos resultados?

Segurança

- A tecnologia utilizada encontra-se em fase experimental, protótipo ou sem certificação, e, se sim, foram avaliadas as **implicações éticas** e de **segurança** do seu uso em ambiente de investigação?
- Foram previstos procedimentos para interromper ou rever o uso da tecnologia caso se detetem falhas graves de segurança, resultados incorretos ou riscos imprevistos para os participantes?

Articulação com outros fatores críticos de risco

• Existem processos de **definição de perfis** ou **decisões automatizadas por algoritmos sem supervisão ou intervenção humana**?

• Existe **controlo sistemático** de pessoas ou comportamentos através de sensores, vídeo, áudio, geolocalização ou outros?

Ligações úteis:

- Artigos 17.º e 35.º e considerandos 89 e 91 do RGPD. Disponíveis em: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Combinação de bases de dados (Nó 7h))

Carregue aqui para avançar para o nó seguinte – Exposição a elevado risco ético? (Nó 7j))

7j). Exposição a elevado risco ético?

Clarificação de conceitos

O conceito de riscos éticos refere-se aos potenciais impactos negativos que as decisões ou práticas de um projeto de investigação podem ter sobre os participantes, investigadores, instituições ou outros *stakeholders*, colocando em causa valores ou princípios éticos — como a dignidade, o bem-estar físico ou psicológico, a justiça, a integridade ou a autonomia —, ou gerando ambiguidades, conflitos, bem como questões legais ou reputacionais. A gestão ética dos riscos consiste no processo de identificar, avaliar e mitigar esses riscos, assegurando que as decisões de investigação são tomadas de forma responsável e proporcional, tendo em consideração:

- Fatores internos como a cultura, os valores, políticas, procedimentos que podem influenciar comportamentos e tomada de decisões da equipa de investigação e criar dilemas éticos, conflitos de interesses ou violações da lei.
- Fatores externos, tais como as condições de gestão de dados, normas e expectativas sociais e legais que podem funcionar como elementos de pressão ou causar dúvidas e incertezas.
- Fatores emergentes resultantes de inovações tecnologias ou mudanças sociais que possam introduzir novas questões éticas para as quais são necessárias adaptações e reflexão ética, de que são exemplos os progressos da inteligência artificial, big data ou biotecnologia com impacto na privacidade, segurança ou dignidade humana.

A gestão ética dos riscos implica a sistematização contínua do processo de investigação, podendo envolver várias etapas:
1 - Identificação dos riscos éticos e os seus potenciais impactos, antecipando eventuais consequências, desafios e oportunidades.
2 - Avaliação das suas causas e envolvidos, considerando que os riscos éticos podem ter diferentes impactos em grupos de pessoas diferenciados, podendo causar danos ou benefícios.
3 - Mitigar e implementar medidas apropriadas para a sua prevenção, redução e resolução no curto e longo prazo, se tal for necessário.
4 - Monitorizar e rever a eficácia das medidas adotadas, comunicando publicamente esse processo e obtendo feedback junto de outros grupos de investigação, aprendendo com as suas perspetivas e experiências de gestão de riscos éticos.

A prática de gestão de riscos éticos encontra-se estabelecida em vários tipos de atividade, existindo múltiplos exemplos de aplicação. No contexto da investigação, é comum — e recomendável — o recurso à apreciação pela Comissão de Ética da instituição onde o projeto está sediado, para validação dos impactos previstos e das respetivas medidas de mitigação. Para a emissão do parecer, recomenda-se a utilização de uma matriz de gestão de riscos éticos que integre os potenciais fatores de risco, a sua probabilidade de ocorrência e impacto, os mecanismos de controlo e a respetiva categorização. O investigador deve seguir o parecer e as orientações emitidas pela Comissão de Ética.

Exemplos:

Exemplo 1: Uma equipa de investigação interdisciplinar trabalha com dados pessoais sensíveis de saúde mental. Antes de iniciar o projeto, surgem dilemas éticos relacionados com conflitos de interesse entre investigadores que também exercem funções clínicas na instituição. O risco ético identificado resulta da possibilidade de decisões enviesadas no tratamento e interpretação dos dados, em função da cultura e valores internos da equipa. Para mitigar esse risco ético, foi solicitado parecer à Comissão de Ética, que recomendou a separação clara de funções entre clínicos e investigadores e a definição de procedimentos internos transparentes de tomada de decisão.

Exemplo 2: Uma universidade é contactada por um sindicato de trabalhadores para realizar um estudo sobre burnout numa determinada organização. Está prevista a recolha de dados pessoais de funcionários sindicalizados e, eventualmente, de outros colaboradores. O risco ético identificado surge da ausência de consulta prévia à entidade empregadora, o que pode gerar tensões institucionais, riscos reputacionais para a universidade e questionamentos sobre a legitimidade do estudo. Surge também um dilema ético adicional: a eventual negociação com a própria organização pode ser interpretada como pressão institucional, limitando a liberdade académica. A Comissão de Ética, neste caso, poderá recomendar a clarificação dos papéis de cada parte (universidade, sindicato, organização), a definição de garantias robustas de proteção dos dados pessoais e a explicitação das salvaguardas de independência científica, assegurando que a investigação não compromete a confiança dos participantes nem a reputação institucional.

Exemplo 3: Uma aluna de mestrado em sociologia pretende entrevistar adolescentes sobre o consumo de álcool entre menores de idade. Para além da **vulnerabilidade destes participantes** no sentido do RGPD — isto é, a dificuldade acrescida de consentir ou de exercer os seus direitos —, este caso levanta questões éticas adicionais: trata-se de menores de idade, envolvidos num tema potencialmente sensível e estigmatizante. Perante esta dupla dimensão, a investigadora submeteu o projeto à Comissão de Ética da universidade, que recomendou, entre outras medidas, não apenas o pedido de consentimento parental, mas também o assentimento dos próprios participantes e a formulação cuidadosa das perguntas, de modo a reduzir riscos de exposição ou desconforto.

Exemplo 4: Na conclusão de um projeto de investigação em Serviço Social, dois coautores discordam sobre a partilha de dados de entrevistas a uma população de risco, devidamente pseudonimizados, no repositório institucional. Apesar de a Ficha de Informação ao Participante prever a partilha de dados pseudonimizados e de ter sido obtido consentimento para tal, um dos autores considera que os dados não devem ser partilhados em acesso aberto, preocupado com uma possível reidentificação dos dados, possíveis pressões externas relacionadas com a publicação desses dados, bem como com riscos para a reputação dos participantes e da instituição. O dilema ético surge na necessidade de equilibrar o interesse na partilha científica com a proteção dos participantes e da imagem institucional. A equipa recorreu à Comissão de Ética da universidade, que emitiu um parecer relativamente aos procedimentos a adotar.

Perguntas de controlo

A sua investigação tem uma elevada exposição a riscos éticos? A sua instituição tem uma política onde estabelece formas de gestão dos riscos éticos?

Se respondeu sim a ambas as questões, e se a política da sua instituição incluir mecanismos de antecipação de riscos, deve adotar procedimentos sistemáticos para identificar os riscos éticos e os seus potenciais impactos, recorrendo a métodos quantitativos ou qualitativos, como análise de dados, inquéritos, entrevistas ou construção de cenários. Todo o processo de investigação deve ser acompanhado por registo e sistematização dos riscos, utilizando uma matriz criada especificamente para esse efeito.

Os riscos éticos identificados devem ser alvo de verificação e parecer da Comissão de ética da universidade. Ao longo de processo de investigação devem ser implementadas medidas apropriadas para a sua prevenção, redução e resolução no curto e longo prazo, se tal for necessário. Esta monitorização deve ser devidamente registada e acompanhada pela Comissão de Ética, podendo ser comunicada publicamente, em formato agregador, enquanto demonstração do compromisso institucional com a ética e a integridade da investigação.

Se respondeu sim à primeira questão e não à segunda, deve considerar a aplicação de um código de conduta ética que evidencie os princípios, valores e normas de conduta, tomada de decisão e responsabilidades ao longo da investigação. Este código deve especificar o que fazer para lidar com conflitos de interesse, confidencialidade, privacidade, diversidade e vulnerabilidade, direitos humanos e eventuais impactos sociais.

A utilização de planos de contingência de riscos éticos deve ser considerada para a sua mitigação. Pode ainda ser considerada a realização de formação ética em formatos como workshops, seminários, webinars, cursos online, estudos de caso, simulações, jogos ou mentoria para habilitar os participantes a lidar com a exposição a riscos éticos.

Se respondeu não à primeira questão, a sua investigação pode ser considerada de menor risco ético e pode não exigir medidas adicionais específicas. Ainda assim, deve considerar a aplicação do código de conduta da sua instituição ou de um outro código de conduta ética que evidencie os princípios, valores e normas de conduta, tomada de decisão e responsabilidades ao longo da investigação, cumprindo ainda todas as normas gerais de proteção de dados, garantindo que o tratamento é legal, transparente e seguro.

Ligações úteis:

- Oates, J., Carpenter, D., Iphofen, R., Rawnsley, A., & Whitman, B. (2020). *Research ethics support and review in research organisations*. UK Research Integrity Office & Association of Research Managers and Administrators. https://doi.org/10.37672/UKRIO-2020.01-ARMA
- UK Research Integrity Office. (n.d.). *Appendix 2: Risk assessment matrix*. UKRIO. Disponível em: https://ukrio.org/wp-content/uploads/Appendix-2-Risk-assessment-matrix.pdf

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Inteligência artificial e outras soluções tecnológicas (Nó 7i))

Carregue aqui para avançar para o nó seguinte – Escolheu software adequado? (Nó 8)

8. Escolheu software adequado?

Clarificação de conceitos

Em contexto de investigação científica, é frequente usar-se ou desenvolver-se software para armazenar, analisar, transformar ou processar dados pessoais de diversas formas. No entanto, qualquer software utilizado deve estar em conformidade com a legislação de proteção de dados e assegurar a proteção dos direitos dos participantes e/ou pessoas cujos dados sejam tratados no âmbito do projeto. Os investigadores devem, por isso, conhecer as características e limitações do software e ferramentas que utilizam, tendo em mente a proteção de dados ao adquirirem ou desenvolverem software para fins de investigação. Neste Nó, apresentam-se as considerações a ter em conta no uso, aquisição, criação ou extensão de software em projetos de investigação.

Importa clarificar os seguintes conceitos relativamente ao software usado pelo investigador:

Licença institucional: contrato formal celebrado entre uma instituição (por exemplo, universidade, centro de investigação ou hospital) e o fornecedor de software. Este contrato garante direitos de utilização, estabelece responsabilidades e define condições de segurança e conformidade legal, nomeadamente em matéria de proteção de dados. O uso de software com licença institucional oferece, em regra, maior previsibilidade e segurança jurídica do que a utilização de software gratuito, *open source* ou adquirido individualmente pelos investigadores, que pode não assegurar salvaguardas equivalentes.

Execução local vs. Software as a Service (SaaS):
Local – O software é instalado em computadores ou servidores da própria instituição. Os dados permanecem na infraestrutura institucional, que controla diretamente aspetos como armazenamento, encriptação, backups e gestão de acessos.
SaaS – O software é fornecido como serviço na nuvem, sendo executado em servidores do prestador deste serviço. Neste caso, os dados são transferidos para fora da instituição e processados em infraestruturas externas, o que exige contratos formais (por exemplo, um Acordo de Subcontratação – *Data Processing Agreement*), que definam a localização dos dados, as medidas de segurança e as políticas de retenção.

Exemplos:

Exemplo 1: Enquadramento geral
Suponha que realiza uma análise de dados qualitativos em entrevistas recolhidas de participantes sobre o uso recreativo de drogas. É preciso garantir que todo o software adquirido, usado e/ou desenvolvido protege os direitos das pessoas representadas no conjunto de dados.

Exemplo 2: Software com licença institucional
A instituição tem uma licença para utilizar um software de análise estatística (por exemplo, NVivo, SPSS). Neste caso, existe um contrato formal que assegura determinados padrões de segurança e conformidade legal com a proteção de dados. O investigador deve, ainda assim, verificar se as configurações de armazenamento, encriptação e gestão de acessos são adequadas, sobretudo quando estão em causa dados sensíveis (como dados de saúde).

Exemplo 3: Software sem licença institucional (uso público ou gratuito)
Um investigador opta por usar serviços de armazenamento gratuitos como Dropbox ou Google Drive/Sheets, ou ferramentas em código aberto (*open source*) descarregadas sem contrato de utilização com a instituição. Aqui, não existem garantias formais de conformidade legal com o RGPD, podendo os dados ser transferidos para fora da UE sem salvaguardas ou expostos a acessos não controlados. A responsabilidade recai sobre o investigador, que deve avaliar cuidadosamente a compatibilidade do uso com as obrigações legais e éticas.

Exemplo 4: Software instalado localmente

Um software de estatística, como SPSS ou MATLAB, é instalado e executado em servidores ou computadores da própria instituição. O processamento e o armazenamento decorrem dentro da infraestrutura institucional, sujeita às políticas internas de segurança. A instituição controla backups, encriptação e acessos, oferecendo maior previsibilidade e confiança no cumprimento das normas de proteção de dados.

Exemplo 5: Software remoto (cloud-based / SaaS)

Um grupo de investigação recorre a uma aplicação baseada na nuvem, como REDCap Cloud, ou outro serviço em modelo Software as a Service. Os dados são armazenados e tratados nos servidores do fornecedor. É imprescindível que exista um contrato formal entre a instituição e o prestador (ex.: Acordo de Subcontratação – *Data Processing Agreement*), especificando localização dos dados, medidas de segurança e políticas de retenção, de forma a assegurar conformidade legal com o RGPD e proteção adequada dos participantes.

Perguntas de controlo

O software irá processar dados de investigação que envolvem dados pessoais?

Se não, qualquer software servirá para esse propósito, mas opte, sempre que possível, ou sempre que exigido pelas políticas da instituição, por software com licença institucional de utilização. Além disso, poderá ser necessário atender a outros requisitos legais (para além da proteção de dados), bem como precauções no plano ético. Avance para o Nó seguinte, Subcontratação.

Existe na instituição software licenciado que possa cumprir a finalidade?

Se sim, prefira sempre esse software.

Se não, consulte as políticas da instituição. Algumas instituições podem não autorizar o uso de software sem licença de utilização pela instituição. Em última análise, se recorrer a software não licenciado, a responsabilidade pela conformidade legal com a proteção de dados recai inteiramente sobre o investigador.

Os dados já foram anonimizados, pseudonimizados ou minimizados?

Para ajuda nesta questão, consulte os Nós Minimização, Anonimização e Pseudonimização.

O princípio é:

- Sempre que possível, anonimizar os dados antes de os carregar no software.

- Se não for possível anonimizar, recorrer à pseudonimização antes do carregamento.

- Se não for possível pseudonimizar, só nesse caso os dados podem permanecer identificáveis — mas esta situação deve ser justificada, documentada e evitada, sobretudo quando se trata de dados sensíveis.

O investigador deve garantir que os dados são carregados no software já no formato mais protegido possível (minimizado, anonimizado ou pseudonimizado). Idealmente, o próprio software pode oferecer funcionalidades que facilitem ou reforcem estas medidas, como importação de dados pseudonimizados, anonimização automática de campos identificadores ou controlos de encriptação. Se o software não suportar estas formas de carregamento e tratamento de dados, deve-se considerar outro software ou acrescentar-lhe estas capacidades antes da utilização.

O software suporta funcionalidades/técnicas de proteção de dados pessoais?

É crucial que o software a ser utilizado ou desenvolvido possua as funcionalidades de proteção de dados adequadas aos riscos do projeto. Estas funcionalidades são particularmente importantes quando a licença de utilização não foi celebrada com a instituição, uma vez que a responsabilidade pelo cumprimento do RGPD recai sobre a equipa de investigação. As seguintes funcionalidades são requisitos de segurança e conformidade que a generalidade do software que trata dados pessoais deve incluir:

- Controlo de acessos granular: Essencial para limitar o acesso aos dados apenas ao pessoal estritamente necessário.
- Encriptação de dados em trânsito, e em repouso: A encriptação em repouso (no armazenamento) é essencial para dados sensíveis ou em cenários de risco moderado ou elevado.
- Atualizações de segurança: A aplicação regular de patches e correções é fundamental para a gestão contínua da segurança.
- Registo de acessos e atividades: Permite monitorizar quem acedeu aos dados, sendo crucial para o dever de demonstração de conformidade e para auditorias.
- Cópia de segurança (backup) e recuperação: Garante a disponibilidade e resiliência dos sistemas e serviços de tratamento em caso de incidente.
- Disponibilização de um aviso de privacidade, gestão da retenção de dados e gestão dos direitos dos titulares: Garantir o cumprimento dos direitos previstos no RGPD e documentar e gerir a base de licitude do tratamento (incluindo mecanismos de gestão de consentimento, quando esta for a base legal aplicável).

Dependendo do risco dos dados objeto de tratamento, outras funcionalidades podem ser ponderadas, por exemplo:

- Técnicas de anonimização ou pseudonimização: A sua inclusão deve ser ponderada quando se pretender que o software trate dados sensíveis, grandes volumes de dados ou em cenários de risco moderado ou elevado.

- Autenticação forte (MFA – Multi-Factor Authentication): Essencial para proteger acessos administrativos e de utilizadores privilegiados.

Se o software não suportar as funcionalidades consideradas necessárias, deve considerar a utilização de outro software ou a adição dessas funcionalidades ao sistema que está a desenvolver.

O software adquirido/desenvolvido será executado localmente, oferecido como SaaS, ou ambos?

- Se local: assegure que as configurações são adequadas e seguras e que os dados são devidamente armazenados.

- Se SaaS: confirme que existe um contrato válido e em conformidade com o RGPD (Acordo de Subcontratação – *Data Processing Agreement*). Se o contrato não for celebrado pela instituição, é da inteira responsabilidade do investigador garantir que o fornecedor cumpre o RGPD. Analise também se o SaaS irá armazenar dados e avalie os riscos de **transferências internacionais**, sobretudo se a empresa não estiver estabelecida na UE.

Note, contudo, que mesmo em software instalado localmente (on-premises), pode ocorrer uma transferência internacional de dados se os serviços de suporte, manutenção ou assistência técnica forem prestados por equipas ou fornecedores sediados fora do Espaço Económico Europeu. Nesses casos, devem ser avaliadas as garantias contratuais e as medidas de segurança aplicáveis, à semelhança do que sucede com soluções SaaS.

- Se híbrido: mapeie todos os fluxos de dados entre a parte local e a parte SaaS da aplicação, identifique quais os dados expostos ao prestador externo e repita esta análise nesse subconjunto de dados.

Esta análise deve também ser repetida para todos os subcontratantes em cenários de SaaS ou híbrido. Se detetar falta de conformidade com o RGPD ou inexistência de contrato de tratamento de dados, deve considerar outro software.

O software irá ligar-se a outro software de investigação (em conformidade com o RGPD)?

Se sim, assegure que os fluxos de dados entre softwares estão encriptados e que não existe risco de exposição acidental a terceiros durante a transmissão.

O software possui registos robustos (logs) e permite auditoria fácil?

Registos robustos e auditáveis são fundamentais para compreender o que ocorreu em caso de violação de dados e são exigidos pelo RGPD, em particular no que respeita ao acesso e às modificações de dados sensíveis. Estes registos devem ser imutáveis, ou seja, não podem ser alterados após a sua criação.

Se não, pode ser necessário considerar outro software ou incluir essa funcionalidade no que está a desenvolver.

Em caso de dúvidas, o investigador deve consultar os serviços de informática da instituição.

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Exposição a elevado risco ético (Nó 7j))

Carregue aqui para avançar para o nó seguinte – Subcontratação (Nó 9)

9. Existe subcontratação?

Clarificação de conceitos

A instituição, Responsável pelo Tratamento, pode recorrer a subcontratantes para poder desenvolver a sua atividade. Na prática, isto corresponde à contratação de prestadores de serviços que tratam dados pessoais em nome da instituição. A subcontratação no tratamento de dados pessoais ocorre quando uma entidade (o Subcontratante) trata dados pessoais em nome e por conta do Responsável pelo Tratamento, ou seja, sem decidir autonomamente as finalidades nem os meios essenciais do tratamento. O Subcontratante é assim um mandatário da instituição Responsável pelo Tratamento, isto é, atua praticando um ou mais atos, juridicamente regulados em contrato, por conta deste último.

O Subcontratante está obrigado a atuar sempre no melhor interesse do mandante, aqui a instituição Responsável pelo Tratamento. A instituição Responsável pelo Tratamento deve assegurar que os Subcontratantes escolhidos apresentem garantias suficientes para implementar, no exercício das suas funções, medidas técnicas e organizativas adequadas que garantam o cumprimento do RGPD.

Em caso de subcontratação, **deve ser celebrado um contrato ou documento normativo semelhante** entre a Instituição Responsável pelo Tratamento e o Subcontratante, no qual sejam claramente definidas as obrigações de cada parte.

Exemplos:

Exemplo 1: No âmbito de um projeto de investigação, o investigador necessita contratar uma empresa para realizar a tradução de um conjunto de depoimentos que contêm dados pessoais recolhidos durante a investigação. A empresa é contratada para proceder à tradução, utilizando os meios técnicos e humanos indicados pelo investigador, sem decidir autonomamente sobre as finalidades ou os métodos essenciais do tratamento dos dados. Neste contexto, a empresa atua como subcontratante, ou seja, trata os dados pessoais em nome e por conta da instituição do investigador (Responsável pelo Tratamento), cumprindo as suas instruções e obrigações contratuais.

Exemplo 2: Uma instituição de investigação contrata um prestador externo, como a Amazon Web Services ou o Google Cloud, para alojar uma base de dados que contém dados pessoais dos participantes de um estudo. Esse prestador externo não determina as finalidades do tratamento dos dados pessoais, limitando-se a fornecer o serviço de alojamento conforme as instruções da instituição. Neste caso, o prestador externo atua como subcontratante, tratando os dados pessoais em nome e por conta da instituição responsável pelo tratamento.

Exemplo 3: Uma equipa de investigação contrata uma empresa para realizar análises estatísticas com base em instruções pré-definidas**.** Se a empresa apenas executa as análises conforme instruções, sem autonomia científica, é um subcontratante.

Exemplo 4: Um investigador contrata uma empresa especializada para contactar potenciais participantes, recolher consentimentos e agendar entrevistas. Se atua segundo as instruções do responsável e não decide quem contactar nem para que finalidade, é subcontratante.

Exemplo 5: Duas instituições de investigação decidem colaborar num estudo conjunto, no qual ambas definem conjuntamente as finalidades e os meios do tratamento dos dados pessoais dos participantes. Ambas participam ativamente na tomada de decisões sobre quais dados recolher, como processá-los e para que propósitos específicos serão utilizados. Neste cenário, **não ocorre subcontratação**. As instituições são consideradas responsáveis conjuntos pelo tratamento dos dados pessoais, partilhando a responsabilidade pela conformidade com o RGPD. Devem estabelecer um acordo claro para definir as respetivas responsabilidades, inclusive perante os titulares dos dados. Neste caso, consulte o Nó Responsabilidade Conjunta.

Perguntas de controlo

1. No âmbito do desenvolvimento do seu projeto tem necessidade de contratar algum prestador de serviços para, sob as suas instruções, desempenhar alguma atividade no projeto que envolva o tratamento de dados pessoais?

2. Essa entidade irá tratar esses dados pessoais exclusivamente sob as suas instruções, sem autonomia para decidir sobre as finalidades e os meios essenciais do tratamento?

Se sim, se a resposta a ambas as questões anteriores foi afirmativa, a instituição responsável pelo tratamento deverá subscrever um contrato de subcontratação, nos termos do artigo 28º do RGPD. Para tal, o investigador deve contactar o serviço competente no domínio jurídico e de investigação da sua instituição, a fim de promover a celebração do referido acordo entre as instituições. Consulte também as **Orientações para minuta de acordo de subcontratação.**

Se não, não se verifica uma relação de subcontratação.

Caso trabalhe com outras entidades que participem ativamente na definição conjunta das finalidades e dos meios do tratamento de dados pessoais, as instituições envolvidas serão consideradas responsáveis conjuntas pelo tratamento, nos termos do RGPD, partilhando a responsabilidade pela conformidade com as normas aplicáveis. Deverá, por isso, ser estabelecido um acordo de responsabilidade conjunta, que clarifique as respetivas funções e obrigações, incluindo a forma como são assegurados os direitos dos titulares dos dados. Nestes casos, deve consultar-se o Nó relativo a **Responsabilidade Conjunta**.

Ligações úteis:

- Artigos 4º/alínea 8), 27º e 28º do RGPD. Disponíveis em https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

- European Data Protection Board. (2024). *Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)*. https://www.edpb.europa.eu/system/files/2024-10/edpb_opinion_202422_relianceonprocessors-sub-processors_en.pdf

Orientações para minuta de acordo de subcontratação

NOTA: Esta minuta é um template orientador, de caráter indicativo. A sua utilização deve ser precedida de consulta ao departamento jurídico da instituição, para análise da situação concreta. Cada acordo de subcontratação pode ter especificidades próprias, pelo que este documento não substitui a avaliação técnica e jurídica necessária.

Objeto	Este Acordo deve ser usado quando uma entidade, o Responsável pelo Tratamento, necessita de recorrer a um Subcontratante para poder desenvolver a sua atividade. A subcontratação no tratamento de dados pessoais ocorre quando uma entidade, o Subcontratante, trata dados em nome e por conta do Responsável pelo Tratamento, ou seja, sem decidir autonomamente as finalidades nem os meios essenciais do tratamento. O tratamento em subcontratação é regulado por acordo, contrato ou outro ato normativo que vincule o subcontratante ao responsável pelo tratamento. O tratamento em subcontratação deve estabelecer o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, as obrigações do subcontratante e os direitos do responsável pelo tratamento.
Legislação	Artigo 28º do Regulamento Geral de Proteção de Dados Pessoais

Conteúdo típico	O conteúdo típico de um Acordo de Subcontratação é o seguinte: - Identificação das entidades que são partes no acordo, o Responsável pelo Tratamento e o Subcontratante, designadamente: nome, morada, número de identificação de pessoa coletiva; - Identificação das finalidades do tratamento em regime de subcontratação, o que significa, a título de exemplo: a identificação do projeto de investigação e das tarefas nele compreendidas que implicam o tratamento de dados pessoais por um subcontratante; - Identificação dos dados pessoais que irão ser objeto de tratamento em regime de subcontratação; - Identificação das tarefas concretas e das condições técnicas e humanas fixadas pelo Responsável pelo Tratamento ao Subcontratante para que este proceda ao tratamento de dados pessoais; - O Subcontratante compromete-se a dar acesso aos dados pessoais apenas aos seus colaboradores afetos às tarefas associadas à prestação do serviço regulado pelo acordo; - O Subcontratante compromete-se a sujeitar os seus colaboradores, a quem dê acesso a dados pessoais, ao dever de confidencialidade; - O Subcontratante compromete-se a realizar os tratamentos de dados pessoais sob condições de segurança que assegurem, em permanência, a confidencialidade, integridade e disponibilidade desses dados; - O Subcontratante compromete-se a adequar as medidas técnicas e organizativas adotadas à natureza, âmbito, contexto e finalidades do tratamento, bem como aos riscos para os direitos, liberdades e garantias das pessoas singulares; - O Subcontratante compromete-se a notificar imediatamente o Responsável pelo Tratamento quando tome conhecimento de um incidente de violação de dados pessoais; - O Subcontratante compromete-se a colaborar com o Responsável pelo Tratamento, designadamente: assistindo o Responsável pelo Tratamento de forma diligente na resposta ao exercício de direitos pelos titulares de dados; fornecendo ao Responsável pelo Tratamento todas as informações de que este necessite para aferir a sua conformidade com os requisitos previstos neste acordo e na legislação aplicável; facilitando auditorias ou inspeções aos tratamentos por si realizados no âmbito do presente acordo - Identificação do Encarregado de Proteção de Dados de cada uma das entidades, se tiverem; - Lei aplicável e foro competente.
Modelo	A Comissão Europeia não impõe um modelo único de acordo de responsabilidade conjunta.
Âmbito de aplicação	Esta ficha de orientação é adequada para acordos a celebrar por entidades com domicílio no Espaço Económico Europeu (EEA).
Países Terceiros	Os acordos de subcontratação com entidades de países terceiros à União Europeia devem cumprir com o disposto no capítulo V do RGPD. Consulte também o Nó **Transferências Internacionais**.

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Software (Nó 8)

Carregue aqui para avançar para o nó seguinte – Medidas de proteção e mitigação de risco, técnicas e organizativas (Nó 10)

10. Planeie medidas de proteção e de mitigação de risco, técnicas e organizativas

Clarificação de conceitos

É essencial que os investigadores definam e implementem medidas técnicas e organizativas adequadas que garantam a proteção dos dados pessoais. Estas medidas visam salvaguardar os direitos e liberdades dos participantes, tanto do ponto de vista ético como legal, e incluem, por exemplo, formas de armazenamento seguro, controlo de acessos e procedimentos de eliminação de dados.

Quanto maior for o risco, em termos da probabilidade de ocorrência ou da gravidade do impacto de uma *violação de dados*, maior deve ser o cuidado na aplicação de medidas de mitigação do risco. Por exemplo, tratamentos que envolvem **dados sensíveis** — como categorias especiais de dados pessoais — ou **tratamentos realizados em larga escala** exigem mecanismos reforçados de proteção e monitorização tendo em vista a mitigação dos riscos identificados.

Dependendo da avaliação dos fatores críticos de risco e das políticas institucionais em vigor, o investigador deve ponderar submeter o projeto a uma comissão de ética, para apreciação dos riscos identificados e das medidas de mitigação propostas. Nos casos de projetos com risco elevado, será ainda necessária a emissão de parecer pelo Encarregado de Proteção de Dados.

O investigador deve aplicar as medidas definidas e também garantir que pode, em qualquer momento, demonstrar a conformidade legal do seu projeto (princípio da responsabilidade), seja se solicitado pela instituição, por um participante ou por uma autoridade competente, como a Comissão Nacional de Proteção de Dados (CNPD). Além disso, os investigadores têm o dever de comunicar estas medidas de forma clara e transparente aos participantes, informando-os sobre o que será feito com os seus dados pessoais ao longo do projeto.

Como abordar estas medidas num projeto?

Ao desenhar um projeto científico que trata dados pessoais, o investigador deve integrá-lo na perspetiva do que se designa por **proteção de dados desde a conceção e por defeito**, conforme previsto no artigo 25.º do RGPD. Isto significa que, logo na fase de planeamento, prévia à implementação, devem ser incorporadas salvaguardas técnicas e organizativas (por exemplo, escolha de metodologias que reduzam a recolha de dados pessoais, seleção de ferramentas seguras e definição prévia de regras de acesso). E que, na fase de implementação e utilização das ferramentas, por defeito, apenas sejam tratados os dados estritamente necessários, garantindo que não são recolhidos dados excessivos nem disponibilizados a pessoas não autorizadas.

Entre várias medidas aplicáveis, destacam-se as seguintes, tipicamente transversais **a qualquer projeto e nível de risco**:

- Armazenamento seguro em servidores institucionais ou serviços validados pela instituição, evitando soluções pessoais ou não verificadas (ex.: discos externos, serviços de nuvem sem contrato adequado com a instituição).
- **Minimização** dos dados, incluindo a **anonimização** e **pseudonimização**, sempre que possível.
- **Cifragem (encriptação) dos dados**, em particular dos dados brutos recolhidos e de informação que possa identificar diretamente os participantes.
- Utilização de **software adequado**, de preferência — ou obrigatoriamente, dependendo da política da instituição — com licença institucional válida e que cumpra requisitos de segurança e a legislação aplicável.
- Controlo rigoroso de acessos, garantindo que apenas pessoas devidamente autorizadas têm acesso aos dados.
- Se possível, registo de acessos e operações (logs), permitindo rastrear quem acedeu, quando e com que finalidade, de modo a prevenir usos indevidos e reforçar a responsabilização. No caso de dados sensíveis, e em **larga escala**, esta medida assumir carácter obrigatório.
- Acesso aos dados por membros da equipa de investigação apenas quando existam cláusulas contratuais de confidencialidade (no caso de docentes e investigadores da instituição) ou mediante a assinatura de um **termo de responsabilidade e confidencialidade** (no caso de alunos, colaboradores ou investigadores externos).
- **Definição de prazos de conservação**, estabelecendo o período máximo de retenção dos dados, findo o qual estes devem ser eliminados de forma segura ou anonimizados, de acordo com a finalidade do estudo e com as obrigações legais aplicáveis.

Exemplos:

Exemplo 1: Entrevistas a profissionais de saúde

Devem ser asseguradas medidas de confidencialidade através de termos assinados pelos investigadores que terão acesso aos dados. As gravações devem ser feitas em dispositivos encriptados e armazenadas em servidores institucionais protegidos, acessíveis apenas à equipa autorizada. As transcrições devem ser anonimizadas ou pseudonimizadas logo que possível, de forma a reduzir o risco de identificação de pessoas. Os consentimentos informados devem ser guardados em separado dos restantes dados, de forma igualmente segura, e eliminados no final do período de conservação definido. As mensagens trocadas no âmbito do recrutamento (SMS, e-mails, contactos, etc.) devem ser armazenadas de forma segura, separada dos restantes dados de investigação, e eliminadas assim que deixem de ser necessárias ou no momento da eliminação/anonimização dos demais dados.

Exemplo 2: Inquéritos online a estudantes

As medidas podem envolver o uso de plataformas validadas pela instituição, transmissão encriptada (HTTPS) e controlo de acessos à base de dados, garantindo que apenas o investigador responsável ou investigadores autorizados pode consultar as respostas.

Exemplo 3: Análise de diários de campo com informação pessoal

Implica aplicar, entre outras medidas, pseudonimização (substituir nomes por códigos), restringir o acesso apenas a investigadores com cláusulas de confidencialidade e definir procedimentos claros de eliminação dos registos após o prazo de conservação.

Exemplo 4: Reutilização de bases de dados existentes em larga escala

Exige, por exemplo, a aplicação do princípio da minimização (restringindo o acesso apenas aos dados relevantes para os objetivos do estudo), bem como a assinatura de termos de confidencialidade por todos os investigadores com acesso à base de dados.

Listas de verificação:

As listas de verificação que se seguem referem-se a aspetos fundamentais a ter em conta no tratamento de dados em formato digital. Caso utilize outros formatos que contenham dados pessoais (como arquivos em papel), as medidas aplicáveis dependem das condições dos espaços físicos e podem variar entre instituições. Nesses casos, recomenda-se o contacto com os serviços de apoio da sua instituição para definir as medidas técnicas e organizativas mais adequadas.

Checklist de minimização e necessidade dos dados

- Recolho apenas os dados pessoais estritamente necessários para os objetivos da investigação.
- Evito tratar dados desnecessários ou excessivos para a finalidade do projeto.
- Verifico se posso alcançar os objetivos do projeto apenas com dados anonimizados.
- Utilizo a pseudonimização sempre que a anonimização não é possível.

Checklist de armazenamento

- Não armazeno dados brutos (não anonimizados ou não pseudonimizados) em computadores pessoais.
- Se a recolha for feita com auxílio de computador pessoal, transfiro os dados para servidores ou dispositivos institucionais o mais rapidamente possível.
- Após a transferência, apago os dados do meu computador pessoal de forma segura.
- Armazeno os dados sensíveis apenas em computadores institucionais desligados da rede ou em serviços seguros da minha instituição, com acesso restrito.
- Não armazeno dados pessoais em serviços de nuvem não autorizados pela minha instituição ou, se utilizo um serviço de nuvem sem contrato com a minha instituição, asseguro-me de que as políticas institucionais o permitem e que (i) os dados estão cifrados com métodos robustos; (ii) o serviço de armazenamento em nuvem cumpre os princípios de proteção de dados.
- Evito replicar ficheiros com dados pessoais em vários dispositivos, a não ser quando estritamente necessário.
- Quando copio ficheiros, garanto que os elimino depois de deixar de precisar deles.
- As cópias de segurança (backups) são realizadas exclusivamente em servidores ou suportes institucionais autorizados, cifradas, protegidas por acesso restrito e eliminadas de forma segura quando deixam de ser necessárias.

Checklist de equipamentos

- Evito guardar dados em computadores não institucionais, salvo com autorização da instituição.
- Garanto que os dados são tratados com software licenciado pela minha instituição e em conformidade com a legislação aplicável.
- Caso a minha instituição permita o uso de software não institucionalmente licenciado, assumo responsabilidade pela conformidade legal do uso de equipamento ou software próprio no tratamento de dados.

Checklist de segurança técnica e organizativa

- Encripto os dados pessoais nos dispositivos onde estão armazenados, incluindo pens e discos externos.
- Guardo as chaves de encriptação de forma segura e separada dos dados.
- Utilizo sempre sessões de acesso autenticadas com credenciais pessoais.
- Nunca partilho as minhas senhas de acesso com terceiros.
- Encerro sempre a sessão antes de me ausentar do posto de trabalho.
- O computador onde trabalho tem todas as atualizações de segurança instaladas, software antivírus atualizado e firewalls ativos.
- Utilizo o navegador com configurações de segurança ajustadas.
- Todos os membros da equipa com acesso aos dados pessoais têm contrato de trabalho com cláusulas de proteção de dados e confidencialidade, ou assinaram um termo de confidencialidade e responsabilidade.
- Se trato dados sensíveis, utilizo preferencialmente sistemas que disponham de registos de acesso (logs) que permitam monitorizar, auditar e responsabilizar o acesso e as operações realizadas sobre os dados.

Checklist de partilha e comunicação de dados

- Não envio ficheiros com dados pessoais por e-mail sem proteção (ex.: sem ser com encriptação prévia ou com utilização de plataformas seguras).
- Utilizo apenas métodos de partilha protegida, evitando o envio de dados pessoais por correio eletrónico sempre que possível. Quando o recurso ao e-mail é inevitável, asseguro-me de que os ficheiros estão devidamente protegidos (ex.: encriptados) e verifico que não são criadas ou mantidas cópias desnecessárias nos servidores e nas aplicações de correio eletrónico do remetente e do destinatário.
- Não transmito dados pessoais através de plataformas como redes sociais.
- Evito o acesso remoto a dados pessoais através de redes inseguras (ex.: Wi-Fi público ou não protegido).

Checklist de eliminação de dados

- Após apagar dados pessoais, esvazio a reciclagem (ou pasta equivalente) em todos os dispositivos.
- Confirmo que todas as cópias dos dados foram igualmente apagadas.

Checklist de gestão ou eliminação de consentimentos e dados pessoais usados no recrutamento

- Os consentimentos contêm dados pessoais dos participantes: armazeno-os de forma segura, cifrada, separada dos restantes dados de investigação e acessível apenas a pessoas autorizadas, eliminando-os assim que deixem de ser necessários, mediante pedido do titular ou no momento da eliminação/anonimização dos restantes dados.
- Armazeno os dados pessoais usados para o recrutamento de participantes (SMSs, e-mails, contactos, etc.) de forma segura e separada dos restantes dados de investigação, eliminando-os logo após o fim do processo de recrutamento, quando deixem de ser necessários ou no momento da eliminação/anonimização dos restantes dados.

Checklist de medidas organizativas de controlo institucional ou de segurança jurídica

- Avalio os fatores críticos de risco do meu projeto, implemento medidas de mitigação adequadas e, consoante as políticas institucionais em vigor, submeto o meu projeto à apreciação da comissão de ética da instituição.
- Caso exista transferência de dados para outra instituição, responsabilidade conjunta ou subcontratação, asseguro-me de que foi celebrado entre as duas instituições protocolo em conformidade.

Ligações úteis:

- Artigo 25.º (Proteção de dados desde a conceção e por defeito) e 32º (Segurança do tratamento) do RGPD. Disponíveis em https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

- European Commission. (2021). *Ethics and data protection*. Directorate-General for Research and Innovation. Disponível em: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

- Iscte – Instituto Universitário de Lisboa. (2022). *Orientações aos investigadores sobre proteção de dados pessoais em atividades de investigação científica*. Disponível em: https://www.iscte-iul.pt/assets/files/2022/12/12/1670862303829_orientacoes_aos_investigadores_sobre_protecao_de_dados_pessoais.pdf

Orientações para redação do termo de responsabilidade e de confidencialidade do investigador

NOTA: Esta minuta é um template orientador, de caráter indicativo. A sua utilização deve ser precedida de consulta ao departamento jurídico da instituição, para análise da situação concreta. Cada termo de responsabilidade pode ter especificidades próprias, pelo que este documento não substitui a avaliação técnica e jurídica necessária.

Aplicável a investigadores que não tenham contrato de trabalho com a instituição que acolhe o projeto de investigação ou cujo contrato de trabalho não contenha cláusulas sobre confidencialidade.

Nome completo do investigador:

Número (se aplicável):

Unidade de Investigação/Faculdade/Escola/Departamento:

Título do projeto de investigação científica:

No desenvolvimento do projeto de investigação científica já identificado são obrigações do investigador as seguintes:

1. Garantir a prática de boas condutas no desenvolvimento do projeto de investigação aqui em causa, designadamente, assegurando o cumprimento da legislação e das orientações internas da instituição onde desenvolve o seu projeto, relativas ao tratamento de dados pessoais, promovendo a identificação e a prevenção de riscos.
2. Os dados pessoais a que o signatário tem acesso, no âmbito do desenvolvimento do projeto de investigação supra identificado, apenas podem ser tratados para esse fim.
3. Aceder apenas aos dados que sejam adequados, pertinentes e limitados ao que é estritamente necessário para o desenvolvimento do projeto de investigação, tendo em vista as finalidades legítimas e específicas do tratamento para os quais foram recolhidos, dando assim cumprimento ao princípio da minimização dos dados.
4. Adotar as melhores medidas técnicas e organizativas a fim de assegurar o respeito pelos princípios da proteção de dados pessoais, incluindo, quando possível, a sua anonimização ou pseudonimização, bem como a sua encriptação.
5. O investigador só poderá tratar os dados pessoais necessários para o desenvolvimento do projeto de investigação na medida em que se verifique, pelo menos, uma das condições de licitude para o tratamento previstas no artigo 6.º do RGPD, ou uma das exceções previstas no artigo 9.º do RGPD.
6. Caso o investigador trate dados pessoais em larga escala relacionados com condenações penais, infrações ou com medidas de segurança ao abrigo do artigo 10.º do RGPD, ou caso o tratamento seja suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares nos termos do artigo 35.º do RGPD, o investigador deve elaborar e submeter à coordenação do projeto, uma proposta de avaliação de impacto sobre a proteção de dados, antes de iniciar o tratamento.
7. Adotar as medidas de segurança técnicas e organizativas adequadas de forma que seja garantida a integridade e confidencialidade dos dados, aqui se incluindo a proteção contra o seu tratamento não autorizado ou ilícito, contra a sua perda, destruição ou danificação acidental, devendo ser evitado o tratamento, nomeadamente o acesso e utilização dos mesmos, por pessoas não autorizadas.

8. Comprometer-se a respeitar as normas de segurança, restrições de sistema e as boas práticas de segurança da informação em vigor na instituição onde desenvolve o seu projeto, designadamente:
    i. A não se ausentar do seu posto de trabalho sem encerrar a sessão de acesso ao sistema informático, garantindo assim a impossibilidade de acesso indevido por terceiros.
    ii. A não revelar a sua senha de acesso ao sistema informático a ninguém, garantindo, assim, a impossibilidade de acesso indevido por terceiros.
    iii. A alterar a sua senha de acesso ao sistema informático sempre que tal seja exigido pelo próprio sistema ou em caso de suspeita de conhecimento da mesma por parte de terceiros.
    iv. A encriptar os dados pessoais nos dispositivos onde estão armazenados e garantir a proteção das chaves adequadamente.
9. A obrigação de confidencialidade e de responsabilidade é extensível a quaisquer membros da equipa técnica do investigador, caso existam, devendo esta obrigação ser atestada por meio de documento escrito assinado por cada um dos membros.
10. Os titulares, cujos dados são objeto de tratamento pelo investigador, têm o direito de acesso, retificação, apagamento e oposição, limitação do tratamento e à portabilidade dos seus dados pessoais, nos termos definidos no projeto de investigação científica, de acordo com o disposto nos artigos 16.º a 20.º do RGPD e nas normas específicas previstas na Lei n.º 58/2019, de 8 de agosto, que assegura a execução do RGPD na ordem jurídica portuguesa.
11. Quando o investigador entender dever responder negativamente a um pedido de exercício de direitos pelos titulares dos dados, cujo tratamento tem a seu encargo no desenvolvimento do projeto de investigação, deve consultar previamente a coordenação do projeto.
12. O investigador tratará os dados pessoais a que tiver acesso por um período definido no projeto de investigação e não superior ao necessário para essa finalidade; caso exista norma legal aplicável que defina um prazo de retenção dos dados tratados superior ao prazo definido no projeto, os dados deverão ser conservados durante todo o período legalmente previsto.
13. Determinada a irrelevância da sua conservação no âmbito do projeto de investigação supra citado, ou terminado o período legal de retenção caso exista, quaisquer dados pessoais que estejam na posse do investigador são, de acordo com o que for definido no projeto de investigação:
    a) Apagados de forma segura ou destruídos;
    b) Anonimizados.
14. Caso o investigador tenha conhecimento de falhas, reais ou potenciais, relativas à segurança dos sistemas informáticos com os quais trabalha ou à proteção de dados pessoais deverá comunicá-las de imediato aos serviços competentes da instituição onde desenvolve o projeto de investigação e ao respetivo Encarregado de Proteção de Dados.

Este documento – termo de responsabilidade e confidencialidade – poderá ser alterado a qualquer momento por motivos de ordem legal, segurança ou qualquer outro que vise a melhoria dos interesses de todas as partes envolvidas.

... [Local] ..., … [dia] de … [mês] de 2025

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Subcontratação (Nó 9)

Carregue aqui para avançar para o nó seguinte – Informação ao participante ou consentimento (Nó 11)

11. Implemente a informação ao participante e/ou consentimento

Clarificação de conceitos

No Nó Responsáveis e Fontes dos Dados, foram identificados e registados o responsável, ou os responsáveis, pelo tratamento, bem como as fontes dos dados, ou seja, se os dados são obtidos diretamente junto dos participantes ou como dados secundários. Estes últimos correspondem à reutilização de dados já existentes para uma finalidade diferente daquela que motivou a sua recolha, provenientes de projetos anteriores, de outras fontes na instituição, de terceiros ou de fontes públicas.

Independentemente da origem, é obrigatório informar os participantes sobre o tratamento previsto através da **Ficha de Informação ao Participante (FIP),** sendo que as informações a prestar variam consoante os dados sejam recolhidos diretamente ou reutilizados como dados secundários.

Finalidade do tratamento e consentimento

Quando a base de licitude para o tratamento de dados é o consentimento, a finalidade deve, sempre que possível, ser formulada de forma específica e delimitada, correspondendo a um objetivo claro de um projeto concreto.

Cada consentimento deve estar associado a uma única finalidade. Um mesmo *formulário de consentimento* pode abranger várias finalidades, cada uma correspondente a um consentimento distinto — por exemplo, a participação na investigação, o contacto para novos estudos e reutilização dos dados, a publicação em ciência aberta após anonimização. Cada um desses consentimentos deve ser apresentado em campo próprio, permitindo ao participante escolher apenas as finalidades que pretende autorizar.

Cada projeto constitui um conjunto definido de atividades de investigação, enquanto a sua finalidade corresponde ao propósito científico do tratamento dos dados pessoais dos participantes. Apenas em estudos de natureza exploratória, em que não seja possível antecipar com rigor o objeto ou a direção da investigação, admite-se que a finalidade seja delimitada de forma mais ampla, podendo abranger diversas áreas ou domínios científicos.[6] Essa amplitude deve ser claramente comunicada aos participantes.

Reutilização de dados e modelo de consentimento dinâmico

A reutilização de dados para uma finalidade diferente da originalmente prevista — mesmo que ocorra no âmbito do mesmo projeto — ou a sua utilização em projeto distinto deve ser tratada como uma nova finalidade de tratamento.

Reutilizar dados num novo projeto equivale, portanto, a definir, uma nova finalidade e, consequentemente, a exigir um novo consentimento. Assim, se um projeto prevê recolher dados para os seus objetivos principais, mas também a possibilidade de reutilização futura noutros projetos, há duas formas de estruturar o formulário de consentimento:

- **Consentimentos prévios múltiplos:** o formulário de consentimento deve incluir tantos consentimentos específicos e autónomos quantos os projetos que recolham ou se prevê virem a utilizar os dados. Cada projeto deve ser apresentado em caixas de seleção separadas, permitindo que o participante aceite colaborar no projeto inicial, mas possa aceitar ou recusar a utilização em investigações posteriores. Cada consentimento exige a disponibilização de uma Ficha de Informação ao Participante (FIP) própria, o que pode tornar o processo mais complexo quando as informações relativas aos futuros projetos ainda não estão totalmente definidas.

[6] Artigo 5.º, n.º 1 da Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do RGPD.

- **Consentimento dinâmico:** em alternativa, o participante pode ser convidado a consentir previamente a possibilidade de ser contactado novamente no futuro, de modo a ser informado sobre cada nova reutilização e forma de tratamento específicos e, nesse momento, decidir se consente ou não na reutilização dos seus dados. Este modelo garante que cada decisão é tomada de forma informada, contextualizada e atualizada, assegurando sempre a possibilidade de aceitação ou recusa.

Ciência Aberta e Consentimento

O depósito de dados pessoais em repositórios institucionais, com vista à sua reutilização em novos projetos, exige o consentimento específico do participante para cada um desses novos projetos. Nestes casos, o acesso ao repositório é restrito e sujeito a controlo institucional, sendo os dados apenas acessíveis às equipas autorizadas e de acordo com as finalidades definidas. Se, contudo, os dados forem irreversivelmente anonimizados **antes** do depósito, deixam de ser considerados dados pessoais. Nesse caso, distinguem-se duas situações:

- Anonimização e depósito em repositório institucional, sem acesso público – Quando os dados são apenas anonimizados para fins internos do projeto ou para cumprir requisitos de conservação, não é necessário um consentimento específico e autónomo. Basta informar os participantes, no consentimento do projeto inicial, que os dados serão conservados em formato anonimizado. Ainda que anonimizados, a eventual partilha desses dados com outras instituições deve ser avaliada caso a caso, considerando a robustez da anonimização e se a partilha foi prevista no consentimento inicial, recomendando-se celebrar um protocolo entre as instituições, tendo em vista estabelecer responsabilidades e garantias de proteção.

- Anonimização e depósito em repositório institucional, com acesso aberto – Quando a intenção é disponibilizar os dados anonimizados em repositórios institucionais no **âmbito da Ciência Aberta**, é necessário obter um consentimento específico para esse efeito no formulário de consentimento. A anonimização, por si só, não dispensa este consentimento, pois o acesso aberto:

  - Amplia o uso potencial dos dados, sem controlo sobre os fins para os quais poderão ser utilizados;
  - Aumenta os riscos de reidentificação devido ao possível cruzamento com outras bases públicas ou privadas.

  Deve ser possível a um participante autorizar a sua participação no estudo inicial, mas optar por não consentir com a disponibilização pública dos seus dados, apesar de anonimizados, no **âmbito da ciência aberta**.

Conteúdo da Ficha de Informação ao Participante

A informação a prestar ao participante subsume-se às seguintes situações:

1. Quando os dados são recolhidos diretamente dos participantes, com base em consentimento

1.1 Informações a facultar

a) **Quem é responsável pelo tratamento**, i.e., a instituição que determina a finalidade e os meios do tratamento desses dados, sendo, geralmente, a instituição onde o projeto está sediado; ou, no caso de **responsabilidade conjunta**, quem são os responsáveis pelo tratamento.

   E ainda, breve identificação do projeto de investigação, identificação do investigador e os seus contactos institucionais.

b) **Os contactos** do Encarregado de Proteção de Dados da instituição.

c) **A base legal do tratamento dos dados, especificando que se trata do consentimento do participante**, nos termos do artigo 6.º, n.º 1, alínea a) do RGPD; no caso de categorias especiais de dados (**dados sensíveis**), deve referir-se ainda o artigo 9.º, n.º 2, alínea a).

d) **A finalidade da recolha**, ou seja, para que fins os dados vão ser utilizados; essa finalidade deve ser específica, explícita e legítima.

Em projetos exploratórios, onde não se mostra possível definir de antemão uma finalidade específica, a finalidade pode ser definida de forma mais ampla. Em qualquer caso, devem ser respeitados os padrões éticos reconhecidos pela comunidade científica, mantendo os participantes informados à medida que a finalidade da investigação se clarifica. Sempre que houver alterações relevantes, os participantes devem receber informação atualizada para poderem exercer, de forma informada, os seus direitos.

e) **Os destinatários, isto é, se os dados serão partilhados com outras entidades ou categorias de entidades**, designadamente a **subcontratantes** (prestadores de serviços) ou a quaisquer outras entidades, e com que finalidade;

f) Se houver **recolha de dados fora do Espaço Económico Europeu (EEE), ou transferência para fora do EEE**, deve ser indicado o país e/ou organização de origem ou destino, e se existe ou não uma "decisão de adequação" da Comissão Europeia. Caso não exista uma decisão de adequação, deve ser verificada a existência de garantias adequadas, designadamente: cláusulas contratuais-tipo de proteção de dados ou outros mecanismos previstos no art. 46.º RGPD. Nesse caso o consentimento deve fazer referência às garantias adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas. Na ausência de garantias adequadas, o consentimento deve ser explícito e informar o participante dos riscos dessas transferências, devido à falta de decisão de adequação e garantias adequadas, conforme indicado no Nó **Transferências Internacionais**.

g) Os **direitos do participante**, e os meios para o seu exercício — normalmente exercidos através de um endereço de email criado pela equipa do projeto. Estes incluem o direito de acesso, retificação, apagamento, retirada do consentimento a qualquer momento, limitação do tratamento e o direito a apresentar reclamação junto da Comissão Nacional de Proteção de Dados (CNPD); se os dados forem recolhidos por meios automatizados (e.g., através de um formulário online), o participante tem ainda o direito de portabilidade dos dados;

h) **Se existirem decisões tomadas exclusivamente de forma automatizada**, sem intervenção humana significativa, abordadas no Nó **Decisões automatizadas por algoritmos** (isto é, com recurso a algoritmos ou sistemas de computador), deve ser indicado:

- que essas decisões existem e em que situações são aplicadas;
- a lógica subjacente, entendida como a explicação dos critérios ou fatores principais que influenciam a decisão exclusivamente automatizada, de forma inteligível para o participante, ainda que sem necessidade de divulgar código-fonte, fórmulas complexas ou informação proprietária;
- a importância e as consequências previstas de tal tratamento para o titular dos dados.

i) **O prazo de conservação dos dados** ou, se não for possível, os critérios usados para defini-lo, e o destino após esse período (eliminação ou anonimização irreversível).

j) Se além dos dados a recolher junto do participante, **vão ser recolhidos informações pessoais acessíveis publicamente** (como redes sociais)?

k) **Quaisquer outros riscos associados ao tratamento**, descritos de forma clara e compreensível.

1.2 Informação a facultar e consentimento para reutilização dos dados

Quando, num determinado projeto, são recolhidos dados com base em consentimento e se prevê a sua utilização noutro projeto distinto deve existir um consentimento específico para cada um dos projetos.

O formulário de consentimento pode adotar duas abordagens.

Na primeira, o participante decide, no momento da recolha dos dados, se autoriza ou não o tratamento no âmbito de cada um dos projetos. Para tal, o formulário deve:

- Detalhar as informações relativas à utilização dos dados correspondentes às alíneas 1.1.a)–k), para cada um dos projetos, ou sempre que estas diferirem do projeto original;
- Identificar claramente ambos os projetos e as equipas envolvidas;
- Fazer constar o consentimento específico para o outro projeto em caixa de seleção autónoma, permitindo que o participante aceite colaborar no projeto inicial, mas possa recusar a utilização dos seus dados no outro projeto.

Em alternativa, pode ser adotado o modelo de **consentimento dinâmico**, no qual o participante é convidado a consentir previamente a ser novamente contactado. Deste modo, será informado sobre cada nova reutilização, caso a caso, e poderá consentir ou não na reutilização dos seus dados. Caso os dados destinados a esse efeito sejam conservados em repositório institucional, este deve ser claramente identificado. As informações relativas às alíneas 1.1.a)–k) devem, tanto quanto possível, ser fornecidas no formulário de consentimento inicial, e complementadas caso a caso com a totalidade da informação exigida quando é solicitada a decisão de consentir ou recusar o novo tratamento.

1.3 Informação a facultar e consentimento para depósito de dados no âmbito da ciência aberta

A possibilidade de depósito em acesso aberto, inclusive após um eventual período de acesso embargado, só é admissível para dados irreversivelmente anonimizados e que, antes da anonimização, tenham obtido consentimento específico para a sua divulgação pública. O consentimento deve constar em caixa de seleção autónoma, permitindo que o participante possa participar no estudo inicial, mas decidir se autoriza ou não o depósito dos seus dados em regime de acesso aberto. Todavia, uma vez que os dados disponibilizados publicamente já não constituem dados pessoais, não se aplicam as informações a facultar previstas nas alíneas 1.1.a)–k).

2. Informações a facultar no caso de tratamento secundário de dados

2.1 Quando os dados são provenientes de projetos anteriores ou de outras fontes na instituição

Se, no projeto inicial, os dados tiverem sido recolhidos com base em consentimento, a sua reutilização noutro projeto pode não ser admissível. A utilização dos dados em outro projeto apenas será possível se o formulário de consentimento do projeto inicial tiver adotado:

- o modelo de múltiplos consentimentos prévios — abrangendo já a equipa do outro projeto, a finalidade e as demais informações necessárias ao participante; ou
- o modelo de consentimento dinâmico.

Neste último caso, ao participante devem ser prestadas apenas as informações complementares em falta — correspondentes às alíneas 1.1.a)–k) — relativamente à nova reutilização, permitindo-lhe decidir, nesse momento, se consente ou não na utilização dos seus dados.

Há casos, porém, em que os dados não foram recolhidos com base em consentimento, mas sim com outro fundamento legal. Por exemplo, num estudo institucional que reutiliza dados pessoais de funcionários, inicialmente recolhidos no âmbito da sua relação contratual de trabalho. Nestas situações, que se enquadram na possibilidade de tratamento posterior, prevista no n.º 4 do art.º 6.º do RGPD, deve assegurar-se que os participantes já foram ou serão informados sobre o novo tratamento e a sua finalidade. A informação deve ser prestada o mais rapidamente possível e, no máximo, um mês após o início do novo tratamento. Deve incluir todos os elementos indicados no ponto 1.1 e, adicionalmente:

i. A base de licitude, indicando tratar-se de tratamento posterior para efeitos de investigação científica, nos termos do artigo 6.º, n.º 4, do RGPD (em vez do consentimento referido no ponto 1.1.c)).

ii. A origem dos dados pessoais, isto é, como foram inicialmente obtidos;

iii. As categorias de dados pessoais em questão (por exemplo, dados identificativos, dados sociodemográficos, entre outros);

iv. Os direitos do titular dos dados. Além dos referidos no ponto 1.1, deve ser incluído o direito de oposição. (Na medida em que a base legal para o novo tratamento não é consentimento, o direito de retirar o consentimento não se aplica.)

2.2 Quando os dados são provenientes de repositórios de acesso aberto

Se vai reutilizar dados anonimizados disponíveis num repositório de acesso aberto, as obrigações do RGPD, inclusive as informações previstas nas alíneas 1.1.a)-k) não se aplicam, uma vez que não há tratamento de dados pessoais. A responsabilidade pela conformidade da anonimização, bem como do consentimento para o depósito e disponibilização pública dos dados, é da equipa que os anonimizou e depositou, ou da instituição que gere o repositório. No entanto, a equipa que reutiliza os dados deve garantir que a anonimização é irreversível antes de os utilizar.

3. Quando os dados são obtidos de fontes públicas

Quando há reutilização de informações pessoais obtidas em fontes acessíveis ao público — como bases de dados, registos públicos, redes sociais ou plataformas online — o dever de informar os titulares dos dados mantém-se. Devem ser prestadas as informações aplicáveis das alíneas 1.1.a)–k), e adicionalmente:

i. A origem dos dados, indicando haver recolha de informação disponível publicamente, e as categorias de dados pessoais em questão (por exemplo, dados identificativos, dados sociodemográficos, entre outros);

ii. A base de licitude, indicando tratar-se de tratamento posterior para efeitos de investigação científica, nos termos do artigo 6.º, n.º 4, do RGPD (em vez do consentimento referido no ponto 1.1.c)).

Nos casos que envolvam **categorias especiais de dados**, e quando os dados tenham sido manifestamente tornados públicos pelo titular – por exemplo opiniões políticas publicadas numa rede social – deve ainda indicar-se o artigo 9.º, n.º 2, alínea e) do RGPD.

iii. Os direitos do titular dos dados. Além dos referidos no ponto 1.1, deve ser incluído o direito de oposição. (Na medida em que a base legal para o novo tratamento não é consentimento, o direito de retirar o consentimento não se aplica.)

4. Dispensa do dever de informação

A obrigação de informar os participantes pode ser dispensada nos casos mencionados nos pontos 2.1 e 3, desde que uma das seguintes condições seja devidamente fundamentada:

- A pessoa em causa já tem conhecimento da informação;
- É impossível contactar os titulares ou o esforço necessário é desproporcionado, o que comprometeria ou prejudicaria seriamente os objetivos do projeto.

Nestas situações, devem ser adotadas medidas adequadas para proteger os direitos e interesses dos participantes, como a disponibilização pública das informações essenciais sobre o tratamento (por exemplo, no site do projeto ou da instituição responsável).

A dispensa do dever de informação constitui, por si só, um fator de risco adicional. Por esse motivo, deve ser incluída na avaliação global de riscos, no Nó **Fatores críticos de risco**. Projetos que recorram a dispensa de informação devem ser classificados, no mínimo, como de **risco moderado**, sendo recomendada a submissão à Comissão de Ética.

Quando a dispensa é combinada com outros fatores críticos de risco, o projeto pode ser considerado de **risco elevado**. Dependendo dos fatores críticos de risco identificados, ou das políticas da instituição, pode ser obrigatório a formalização de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD). O ponto 3 do Regulamento 1/2018 da CNPD estabelece a obrigatoriedade da realização de uma AIPD nos casos de dispensa do dever de informação envolvendo o tratamento de **dados sensíveis**, situação em que, além da eventual apreciação pela Comissão de Ética, é obrigatório o parecer do Encarregado de Proteção de Dados.

Exemplos:

Exemplo 1: Duas finalidades distintas no formulário de consentimento

Um projeto de investigação sobre estilos de vida recolhe dados pessoais para analisar hábitos alimentares (primeira finalidade). Simultaneamente, os investigadores preveem vir a reutilizar os mesmos dados, mais tarde, para estudar padrões de sono em populações semelhantes (segunda finalidade). Neste caso, o formulário de consentimento integra a Ficha de Informação ao Participante e dois consentimentos autónomos, em caixas de seleção separadas, permitindo que o participante autorize a participação no estudo inicial sem ter de autorizar, obrigatoriamente, a reutilização dos seus dados na investigação futura.

Exemplo 2: Reutilização de dados

Uma equipe de investigação decide usar dados pessoais de um anterior projeto de saúde mental, ainda disponíveis na instituição, num novo projeto sobre stress no trabalho. Como se trata de uma finalidade diferente, a equipa responsável deve fornecer nova Ficha de Informação ao Participante e obter um consentimento adicional, específico para a reutilização dos dados no segundo projeto.

Exemplo 3: Tratamento posterior de dados controlados pela instituição

Uma instituição universitária decide utilizar, para fins de investigação em gestão de recursos humanos, dados contratuais já detidos sobre os seus funcionários. Neste caso a base legal do tratamento inicial não foi o consentimento, mas a execução da relação contratual. Estes dados podem ser tratados posteriormente para efeitos de investigação científica, sendo, contudo, obrigatório fornecer uma Ficha de Informação ao Participante com todos os elementos relevantes, no prazo máximo de um mês após o início do novo tratamento.

Exemplo 4: Utilização de informação pública e dispensa de informação

Uma equipa de investigação em ciência política analisa mensagens publicadas em redes sociais de acesso público para estudar a propagação de desinformação. Embora, em princípio, se deva informar os titulares dos dados, a obrigação de informação pode ser dispensada se tal se revelar impossível ou implicar um esforço desproporcionado, comprometendo seriamente os objetivos do projeto. Nesta situação, a dispensa deve ser devidamente fundamentada, o projeto deve ser submetido à Comissão de Ética e é recomendada a publicação, no site institucional do projeto, da Ficha de Informação ao Participante com os elementos essenciais do tratamento.

Exemplo 5: Ciência Aberta com dados anonimizados

Uma equipa de investigação em saúde pública recolhe dados pessoais de participantes para um projeto sobre hábitos de atividade física. Após o término do projeto, os dados são irreversivelmente anonimizados e a equipa pretende disponibilizá-los no seu repositório institucional em **acesso aberto**. É obrigatório obter consentimento autónomo e específico para essa finalidade antes da anonimização, dado que a disponibilização pública amplia as possibilidades de reutilização dos dados e aumenta os riscos de reidentificação pelo cruzamento com outras fontes. Deve ser possível que um participante consinta em participar no projeto, mas não consinta em que os seus dados anonimizados sejam disponibilizados publicamente.

Perguntas de controlo

- **A FIP Inclui todos os itens de informação obrigatórios a fornecer ao participante?**
- **Se os dados são recolhidos diretamente junto dos participantes e a base legal para o tratamento for o consentimento**:

  - A FIP integra todas as informações referidas no ponto 1.1, e está integrada no formulário de consentimento?
  - Se se prevê a utilização dos dados em outros projetos, por outras equipas ou para outras finalidades, e se adota o modelo de múltiplos consentimentos prévios:
    - O formulário de consentimento fornece informações sobre a identificação das outras equipas ou outras finalidades, bem como os demais elementos da FIP aplicáveis ao tratamento de dados em cada projeto?
    - Para cada projeto, equipa ou finalidade, existe um consentimento específico e autónomo, garantindo que o participante possa escolher em quais projetos deseja participar, podendo consentir apenas num projeto sem ser obrigado a autorizar a utilização dos seus dados noutros?
  - Se se adota o modelo de consentimento dinâmico:
    - O formulário de consentimento inicial assegura o consentimento autónomo e específico para a reutilização dinâmica dos dados e a autorização de contacto para esse efeito, garantindo que o participante possa participar no projeto sem ser obrigado a consentir com esse contacto futuro?
    - O formulário de consentimento fornece, tanto quanto possível, informações sobre as novas equipas ou finalidades e demais elementos da FIP aplicáveis ao tratamento de dados nos futuros projetos?
    - A plataforma de gestão do consentimento dinâmico ou, quando aplicável, o repositório institucional onde os dados serão conservados, está claramente identificado? Estão previstos procedimentos ou mecanismos de registo e auditoria das decisões de consentimento dadas ou retiradas pelos participantes?
  - Se se prevê a anonimização e posterior disponibilização dos dados em regime de ciência aberta:
    - É obtido consentimento prévio para essa finalidade, antes da anonimização?
    - Esse consentimento é específico e autónomo, permitindo ao participante participar no projeto sem ser obrigado a autorizar a disponibilização posterior em acesso aberto?
  - Havendo tratamento de **dados sensíveis**, designadamente categorias especiais de dados, **transferências internacionais** para países sem decisão de adequação ou **decisões automatizadas por algoritmos**:
    - O consentimento é **explícito**, requerendo ato afirmativo expresso e verificável (ex.: assinatura manuscrita, assinatura digital autenticada, ou manifestação equivalente)?
  - No caso de participantes menores:
    - O consentimento é solicitado aos representantes legais?
    - É ponderada igualmente a recolha de assentimento dos menores, sempre que possível?
  - As informações e os riscos do tratamento estão descritos de forma compreensível para os participantes? No caso de menores ou pessoas vulneráveis, a linguagem é adequada à sua capacidade de compreensão?

- **Dados secundários: reutilização de dados provenientes de outros projetos, de fontes institucionais ou informação pessoal disponível publicamente**

  - Se a base legal do projeto inicial é o consentimento:

    No modelo de múltiplos consentimentos prévios:

    - O formulário de consentimento inicial contemplou o consentimento específico para o projeto inicial e o outro projeto em questão, incluindo as informações da Ficha de Informação ao Participante (FIP) correspondentes a cada um dos projetos?

    No modelo de consentimento dinâmico:

    - O formulário de consentimento inicial assegurou o consentimento específico para a reutilização dinâmica dos dados e a autorização de contacto para esse efeito?
    - O participante é notificado, para a nova reutilização, sobre a identidade e os contactos da equipa responsável, a nova finalidade e demais informações da FIP em falta no âmbito do novo tratamento? Tem possibilidade efetiva de decidir sobre cada reutilização?

  - Se a base legal **não** foi o consentimento, mas outra prevista no art. 6.º ou 9.º do RGPD (ex.: dados já detidos pela instituição; informações contratuais; dados de colaboradores/utentes; informações recolhidas em fontes públicas):

    - Os participantes já foram (ou serão) informados sobre o novo tratamento e a sua finalidade, incluindo as informações do ponto 1.1; as informações adicionais do ponto 2.1; ou, no caso de informação pessoal disponível publicamente, as do ponto 3?
    - Essa informação foi disponibilizada logo que possível ou, no máximo, até um mês após o início do novo tratamento?
    - Entre as informações facultadas, inclui-se o direito do participante a opor-se ao novo tratamento?
    - Nos casos em que informar diretamente os participantes se mostre impossível ou implique esforço desproporcionado, comprometendo seriamente os objetivos do projeto:
      - ◊ São adotadas medidas alternativas de transparência (ex.: publicação da FIP no site do projeto ou da instituição)?
      - ◊ Antes do tratamento, a fundamentação para a dispensa da informação foi documentada e submetida à apreciação de uma comissão de ética ou, em caso de risco elevado, ao Encarregado de Proteção de Dados?

MODELO PROPOSTO PARA O FORMULÁRIO DE CONSENTIMENTO INFORMADO

PARTE I – Ficha de Informação ao Participante

I.1 Sobre o projeto de investigação

O presente documento enquadra-se no projeto de investigação [nome do projeto] a decorrer no/a [nome da instituição de ensino superior ou outra instituição do sistema científico e tecnológico nacional] (caso seja financiado, indicar a entidade e as respetivas referências).

Este projeto de investigação pretende [descrição do objetivo do projeto[1]].

[1] Em alguns projetos científicos não é possível identificar completamente a finalidade do tratamento de dados pessoais no momento da recolha, caso em que o consentimento do titular de dados pode ser elaborado para uma finalidade mais abrangente, isto é, para diversas áreas de investigação ou ser dado unicamente para determinados domínios ou projetos de investigação. Exemplo: "O presente documento enquadra-se no âmbito dos estudos da doença Anemia Hemolítica que

esta instituição irá desenvolver no decurso da próxima década. Estes estudos irão centrar-se na análise dos fatores que causam a destruição dos glóbulos vermelhos.".

No entanto, devem ser respeitados os padrões éticos reconhecidos pela comunidade científica, mantendo os participantes informados. À medida que a finalidade da investigação se clarifica e/ou sempre que houver alterações relevantes, os participantes devem receber informação atualizada para poderem exercer, de forma informada, os seus direitos.

I.2 Participação no estudo e contactos dos responsáveis do projeto

A sua participação no nosso estudo, que será muito valorizada e irá contribuir para o avanço do conhecimento neste domínio, consiste em conceder [descrição do modo como vai decorrer a participação do signatário, exemplo: entrevista, questionário, uso de imagens, etc.] à nossa equipa. Estimamos que a sua participação tenha a duração de [..] horas.

O/A [nome da instituição de ensino superior ou outra instituição do sistema científico e tecnológico nacional] é o responsável pelo tratamento dos seus dados pessoais, recolhidos e tratados exclusivamente para as finalidades do estudo, tendo como base legal o seu consentimento, conforme [escolher conforme aplicável artigo 6.º, n.º 1, alínea a] ou [artigo 9.º, n.º2, alínea b) do Regulamento Geral de Proteção de Dados].

O estudo é realizado por [nomes dos investigadores e endereço de correio eletrónico], que poderá contactar caso pretenda esclarecer uma dúvida, partilhar algum comentário ou exercer os seus direitos relativos ao tratamento dos seus dados pessoais. Poderá utilizar o contacto indicado para solicitar o acesso, a retificação, o apagamento ou a limitação do tratamento dos seus dados pessoais.

I.3 Confidencialidade e participação voluntária

A sua participação neste estudo é **confidencial**. Os seus dados pessoais serão sempre tratados por pessoal autorizado vinculado ao dever de sigilo e confidencialidade. O/A [nome da instituição de ensino superior ou outra instituição do sistema científico e tecnológico nacional] garante a utilização das técnicas, medidas organizativas e de segurança adequadas para proteger as informações pessoais. É exigido a todos os investigadores que mantenham os dados pessoais confidenciais.

Além de confidencial, a participação no estudo é estritamente **voluntária**: pode escolher livremente participar ou não participar.

Se tiver escolhido participar, pode interromper a participação e retirar o consentimento para o tratamento dos seus dados pessoais em qualquer momento, sem ter de prestar qualquer justificação, usando o contacto referido acima. A retirada de consentimento não afeta a legalidade dos tratamentos anteriormente efetuados com base no consentimento prestado.

I.4 Partilha de dados com outras entidades

O/A [nome da instituição de ensino superior ou outra instituição do sistema científico e tecnológico nacional] não divulga ou partilha com terceiros a informação relativa aos seus dados pessoais, salvo com o seu consentimento[2].

[2] Caso exista partilha de dados com outras entidades ou caso haja partilha de dados com prestadores de serviços (subcontratação) dever-se-á acrescentar:

Para a prossecução deste estudo, é necessário partilhar os seus dados com as seguintes entidades (ou equipas de investigação) que colaboram no mesmo projeto e com a mesma finalidade:

[Nome e Contacto do Investigador 1] - [Instituição de Ensino Superior ou outra Instituição]

[Nome e Contacto do Investigador 2] - [Instituição de Ensino Superior ou outra Instituição]

[Adicionar aqui qualquer prestador de serviços ou subcontratado, se aplicável]

I.5 Transferências internacionais (se aplicável)[3]

[3] Caso ocorram transferência (importação ou exportação) de dados pessoais para fora do Espaço Económico Europeu incluir essa informação e assinalar a existência ou não de uma decisão de adequação adotada pela Comissão Europeia (art. 45º RGPD).
Caso não exista decisão de adequação, nem garantias adequadas (cláusulas contratuais-tipo ou outro mecanismo previsto no art. 46º do RGPD), deve ser incluída informação sobre os riscos que podem decorrer para os participantes e, se possível, das medidas adotadas para os mitigar.
Exemplo:

"*No âmbito deste estudo, os seus dados pessoais poderão ser transferidos para fora do Espaço Económico Europeu (EEE), nomeadamente para a Universidade XTPO na Turquia. Atualmente, não existe uma decisão de adequação da Comissão Europeia relativamente à Turquia, nem estão implementadas as garantias previstas nos artigos 46.º do RGPD.*

Isto significa que os seus dados poderão estar sujeitos a riscos de proteção maiores do que na UE, uma vez que a Turquia não oferece legislação nem direitos equivalentes aos da União Europeia. Para mitigar este risco, a equipa de investigação implementou medidas técnicas e organizacionais rigorosas: os dados serão cifrados (encriptados com segurança forte) em trânsito e em repouso, e serão pseudonimizados antes da transferência, garantindo que a sua identificação direta só é possível por meio de uma chave de código mantida em segurança dentro do EEE."

I.6 Decisões automatizadas (se aplicável)[4]

[4] Caso o tratamento de dados pessoais envolva decisões automatizadas, incluindo a definição de perfis, referida no art. 22º, nº1 e nº4 do RGPD, incluir informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o participante.

I.7 Anonimato dos resultados científicos

Os resultados deste estudo serão sempre apresentados de forma agregada e anonimizada, garantindo-se o seu anonimato nos resultados, apenas divulgados para efeitos estatísticos, de ensino, comunicação em encontros ou artigos científicos.

I.8 Destino final dos dados recolhidos (Escolha conforme aplicável):

<u>Opção 1:</u> Destruição dos dados pessoais
Os seus dados pessoais recolhidos serão conservados por [especificar o tempo, os critérios ou o momento do estudo após o qual serão destruídos].

<u>Opção 2:</u> Anonimização dos dados pessoais e conservação
Os seus dados pessoais recolhidos serão conservados por [especificar o tempo, os critérios ou o momento do estudo], após o qual serão anonimizados. Os dados anonimizados serão conservados na [identificar a infraestrutura institucional, ex: servidor do Instituto X].

<u>Opção 3:</u> Depósito de dados anonimizados em repositório institucional no âmbito da Ciência Aberta
Os seus dados pessoais recolhidos são conservados por [especificar o tempo, os critérios ou o momento do estudo], após o qual serão anonimizados. Caso consinta nas opções em baixo, esses dados anonimizados serão disponibilizados no âmbito da ciência aberta na [identificar o repositório institucional] sob as condições [indicar as condições de acesso aberto: aberto, com embargo, restrito]. Este procedimento assegura o depósito em repositórios confiáveis e reconhecidos pela comunidade científica, de acordo com os princípios FAIR (*Findable, Accessible, Interoperable, Reusable*).

<u>Opção 4:</u> Consentimento dinâmico: Conservação e reutilização dos dados pessoais em outros projetos com diferentes finalidades e/ou por outras equipas de investigação

Os seus dados pessoais recolhidos serão conservados por [especificar o tempo, os critérios ou o momento do estudo]. Após esse período, e caso manifeste o consentimento nas opções em baixo, os dados serão [escolher conforme aplicável: reutilizados pelo [nome do projeto][5] ou depositados de forma segura no [identificar o repositório institucional desta instituição][6] para posterior reutilização por outros projetos com diferentes finalidades científicas e/ou equipas de investigação autorizadas. Para esse efeito, será novamente contactado com vista a ser informado sobre a nova finalidade específica e o tratamento proposto, antes de qualquer reutilização dos seus dados. Nessa altura, terá sempre a possibilidade de recusar a utilização dos seus dados para a nova finalidade.

[5,6] Por cada nova finalidade, projeto ou equipa de investigação, devem ser fornecidas as informações que difiram do projeto inicial. Estas informações devem ser, tanto quanto possível fornecidas no formulário de consentimento inicial ou, caso não seja possível, posteriormente, mas antes do novo tratamento, incluindo:

- A nova finalidade do projeto
- Equipa envolvida e contactos para dúvidas ou exercício de direitos
- Partilha de dados com outras entidades
- Transferências Internacionais, se aplicável
- Decisões automatizadas, se aplicável
- Destino final dos dados no novo projeto
- Se existem riscos de participação no novo projeto.

I.9 Riscos da participação

Não existem riscos significativos expectáveis associados à participação no estudo [caso existam, referir em que consistem e quais as medidas adotadas para minorar/controlar os seus efeitos].

O/A [nome da instituição de ensino superior ou outra instituição do sistema científico e tecnológico nacional] tem um Encarregado de Proteção de Dados, contactável através do email […]. Caso considere necessário tem ainda o direito de apresentar reclamação à autoridade de controlo competente, a Comissão Nacional de Proteção de Dados.

PARTE II – Consentimentos

Consentimento explícito para participar no estudo

Declaro ter compreendido os objetivos de quanto me foi proposto e explicado pelo/a investigador/a, tendo-me sido dada a oportunidade de fazer todas as perguntas sobre o estudo e para todas elas ter obtido resposta esclarecedora. Aceito participar no estudo, e autorizo, de forma livre, esclarecida e informada, a recolha e utilização dos meus dados pessoais para efeitos deste estudo.

Sim ☐ Não ☐

Outros consentimentos específicos[7]

[7] Se a ficha de informação ao participante incluiu o depósito de dados anonimizados em ciência aberta ou a reutilização de dados pessoais em outros projetos, deve ser incluído o consentimento respetivo:

Consentimento para depósito de dados anonimizados em repositório institucional no âmbito da Ciência Aberta

Autorizo que os dados recolhidos, após tratamento e anonimização que garante de forma irreversível a minha privacidade e anonimato, possam ser preservados e depositados num repositório institucional seguro e de confiança, o [indicar o repositório onde os dados anonimizados serão depositados], de acordo com as políticas institucionais de gestão de dados de investigação e os requisitos europeus da ciência aberta, que assegurará a sua preservação a longo prazo e o acesso regulado para outros fins.

Sim ☐ Não ☐

Consentimento dinâmico: reutilização dos dados pessoais em outros projetos com diferentes finalidades e/ou por outras equipas de investigação

Autorizo que os meus dados pessoais recolhidos no âmbito deste projeto possam ser reutilizados ou depositados no repositório institucional [indicar o repositório institucional desta instituição] para posterior reutilização por outros projetos e/ou equipas de investigação com diferentes finalidades científicas. Para esse efeito, autorizo que essas equipas de investigação me contactem para me informarem sobre as novas finalidades específicas, a forma como os meus dados serão tratados nesse novo projeto e para obter o meu consentimento.

Sim ☐ Email: _____

Não ☐

Consentimento para contactar o participante

Se autoriza que a equipa de investigação o contacte para lhe transmitir os resultados da investigação, preencha o seu email ou telefone:

Email: _____

Telefone: _____

_____ (local),

_____/____/_____ (data)

Nome: _____

Assinatura: _____

(se não for o próprio a assinar em razão da idade ou de incapacidade e tiver capacidade de compreensão deve também assinar o documento, exprimindo seu assentimento)

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Medidas de proteção e mitigação de risco, técnicas e organizativas (Nó 10)

Carregue aqui para avançar para o nó seguinte – Recolha e tratamento de dados (Nó 12)

12. Implemente a recolha e tratamento de dados

Clarificação de conceitos

Na fase de recolha de dados, deve garantir-se que a informação obtida é adequada, pertinente e limitada ao necessário para os objetivos definidos, em conformidade com o princípio da **minimização de dados**. A recolha deve estar sustentada numa base legal adequada, que na maioria dos casos é o consentimento. Independentemente da base adotada, é obrigatório a **informação ao participante**. Desde o início, sempre que possível, devem ser consideradas medidas de **anonimização** ou **pseudonimização**, de modo a **reduzir riscos para os participantes**. É importante documentar o contexto da recolha, por exemplo, num **plano de gestão de dados**, identificando os **responsáveis pelo tratamento e as fontes dos dados**, a finalidade do uso dos dados e os instrumentos utilizados.

Na fase de tratamento, os dados devem ser processados com **software adequado**, e apenas para as finalidades previamente **comunicadas aos participantes**, garantindo a sua exatidão, atualização e eliminação de informações incorretas ou desnecessárias. Devem ser aplicadas **medidas técnicas e organizativas** adequadas de proteção e mitigação de risco, assegurando a confidencialidade, bem como limitando o acesso apenas a pessoas autorizadas. A recolha de dados pressupõe ainda o planeamento prévio do ciclo de vida dos dados, incluindo as etapas de **publicação, conservação ou eliminação**, de forma a garantir a continuidade da conformidade e a minimização dos riscos.

Deve ter reparado que o texto anterior está repleto de links para os vários Nós deste Toolkit, evidenciando que o processo de recolha e tratamento exige uma articulação cuidada de várias etapas, antes, durante e após a sua execução. Importa reforçar que estes procedimentos não são estáticos: devem ser revisitados ao longo de todo o processo, de modo a garantir a conformidade legal, ética e técnica perante eventuais mudanças de contexto, novos riscos identificados ou incidentes inesperados. Para apoiar esse acompanhamento contínuo, este Toolkit pode ser utilizado como um instrumento prático de preparação e monitorização, permitindo aos investigadores rever sistematicamente os procedimentos adotados, detetar fragilidades e implementar melhorias que assegurem uma gestão responsável, segura e transparente dos dados.

Exemplos:

Exemplo 1: Exercício de direitos durante a recolha

Num estudo em Psicologia, que envolvia várias entrevistas a um mesmo participante sobre a sua experiência de agressões sofridas, de forma repentina e inesperada, um dos participantes retirou o consentimento para a gravação e tratamento das suas entrevistas a meio do estudo. Perante esta decisão do participante, e sem exigir qualquer tipo de justificação ou fundamentação, a equipa de investigação ativou os procedimentos previstos relativos ao **exercício de direitos**, assegurando a eliminação das gravações e a suspensão de qualquer utilização futura dos dados recolhidos até então desse participante.

Exemplo 2: Violação de dados pessoais durante a recolha

Um investigador em serviço social, após realizar várias entrevistas no âmbito de um trabalho de campo, foi assaltado no regresso ao seu centro de investigação e teve o computador roubado. O dispositivo continha dados pessoais ainda não transferidos para o servidor institucional seguro, pelo que a situação configurou uma **violação de dados pessoais**. O investigador acionou de imediato os procedimentos previstos no seu **plano de gestão de dados**, comunicando o incidente aos contactos definidos nas políticas institucionais e ao Encarregado de Proteção de Dados. A instituição, em articulação com o EPD, avaliará a necessidade de notificação à autoridade de controlo e aos participantes afetados.

Exemplo 3: Alterações na informação ao participante e na recolha de dados

Durante um estudo em educação realizado em 2020, uma equipa de investigação tinha definido no protocolo inicial que as entrevistas seriam realizadas presencialmente nas escolas. Contudo, devido à pandemia de COVID-19, tornou-se necessário alterar o procedimento e realizar parte das entrevistas online. Esta mudança obrigou a revisitar os Nós relativos à **informação ao participante** e **às medidas de proteção e mitigação de risco**, ajustando o **pedido de consentimento** e garantindo a segurança na recolha e armazenamento dos dados em ambiente digital.

Exemplo 4: Alteração de software durante o tratamento

Durante um projeto de investigação, uma equipa utilizava um software adquirido pelo seu centro de investigação para o processamento de dados. A meio do estudo, a empresa responsável por esse software anunciou a descontinuação do produto, deixando de disponibilizar atualizações de segurança e suporte técnico. Perante esta situação, tornou-se necessário selecionar e implementar uma nova solução tecnológica. Para tal, a equipa revisitou o Nó relativo ao **software**, avaliando os riscos associados à migração dos dados, garantindo ainda a proteção, a integridade e a continuidade do tratamento dos dados.

Exemplo 5: Alteração de um membro da equipa

Durante um estudo em farmacovigilância, um dos investigadores encarregue do tratamento de dados pessoais mudou-se para uma Unidade de Investigação no estrangeiro antes da conclusão do projeto. Esta situação exigiu a revisão e atualização da lista de investigadores com acesso aos dados pessoais, tendo sido celebrado um **termo de responsabilidade** com o doutorando/investigador que passou a integrar a equipa e assumiu essas funções. A equipa aproveitou para rever os procedimentos de acesso aos dados, nomeadamente as credenciais (*passwords*), assegurando que todas as responsabilidades e salvaguardas continuavam claramente definidas e em conformidade com a legislação e as normas éticas aplicáveis.

Exemplo 6: Combinação de bases de dados durante o tratamento

Durante um estudo em saúde pública, uma equipa de investigação passou a ter acesso a dados administrativos e decidiu **combinar a sua base de dados com essa nova base de dados administrativos** para análise de padrões de comportamento. A combinação não estava inicialmente prevista e aumentou o risco de reidentificação de participantes, apesar dos dados estarem pseudonimizados. A equipa revisitou os **fatores críticos de risco**, identificou medidas de mitigação, incluindo novas **medidas adicionais de proteção e mitigação de risco**, de modo a garantir a proteção, confidencialidade e conformidade ética e legal dos dados. Os participantes, por seu turno, foram informados do tratamento decorrente da combinação das bases de dados, bem como das novas medidas de proteção e de mitigação de risco que foram implementadas.

Implemente a recolha e tratamento de dados

Não se esqueça que durante a recolha e o tratamento de dados, é fundamental verificar que os procedimentos planeados e adotados em cada fase do ciclo de vida dos dados são os adequados. Para tal, deve rever periodicamente as práticas de recolha e tratamento dos dados, garantindo que continuam a cumprir os requisitos legais, éticos e técnicos, mesmo perante alterações de contexto, surgimento de novos riscos ou incidentes inesperados. Esta monitorização contínua permitir-lhe-á identificar falhas, ajustar salvaguardas e assegurar a proteção, confidencialidade e integridade dos dados ao longo de todo o processo investigativo.

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Informação ao participante ou consentimento (Nó 11)

Carregue aqui para avançar para o nó seguinte – Publicação, conservação ou eliminação e licenças (Nó 13)

13. Publicação, conservação ou eliminação, e licenças

Clarificação de conceitos

A gestão do ciclo de vida dos dados de investigação pode considerar duas dimensões distintas:

Gestão de dados e apagamento no plano científico-operacional

O plano científico-operacional abrange os dados pessoais recolhidos junto dos participantes e utilizados diretamente nas atividades de investigação. Inclui ainda outros elementos ou documentos associados, como os formulários de consentimento, e os registos resultantes de contactos com os participantes ou do seu processo de recrutamento (e.g., SMSs, emails, anotações de campo que identifiquem os participantes) —, que devem ser armazenados de forma segura e conservados apenas durante o período necessário para cumprir a finalidade que justificou a sua recolha.

Ultrapassado esse prazo, os dados devem ser eliminados de forma adequada, ou **irreversivelmente anonimizados**, garantindo a conformidade com a **Ficha de Informação ao Participante (FIP) e/ou o Consentimento** e com os requisitos legais ou institucionais aplicáveis.

A definição do período de conservação deve ter em conta a finalidade científica, o enquadramento ético-jurídico e as políticas internas de proteção de dados, de gestão de dados de investigação e de conservação arquivística. No caso de projetos financiados, os organismos financiadores podem estabelecer regras próprias relativas à conservação e eliminação dos dados dos participantes.

Os prazos de conservação, ou os critérios que permitam determiná-los, devem constar de forma clara na **FIP, integrante do formulário de consentimento**. Na ausência de regras específicas da instituição, os dados devem ser apagados ou irreversivelmente anonimizados logo que deixem de ser necessários para a prossecução dos objetivos da investigação.

Nos casos em que se preveja a publicação ou partilha em repositórios de ciência aberta, apenas podem ser disponibilizados dados devidamente anonimizados, acompanhados da licença adequada de utilização, de acordo com as políticas institucionais de acesso aberto.

Gestão de dados no plano administrativo-arquivístico

O plano administrativo-arquivístico compreende os documentos processuais e administrativos produzidos no âmbito da gestão do projeto (por exemplo, modelos formais, dados administrativos, artigos, contratos, relatórios, correspondência, pedidos de autorização, prémios ou pareceres), sujeitos às regras de conservação da Administração Pública. Estes documentos, ainda que contenham dados pessoais, integram os arquivos de interesse público e estão sujeitos às regras de conservação e eliminação definidas pela Direção-Geral do Livro, dos Arquivos e das Bibliotecas (DGLAB). Nesses casos, não se aplica a eliminação ou anonimização dos documentos administrativos, podendo, contudo, admitir-se a pseudonimização reversível durante o prazo de conservação administrativa.

Os conteúdos que se seguem neste nó centram-se exclusivamente no âmbito dos dados tratados no plano científico-operacional, remetendo-se a gestão arquivística dos documentos administrativos para as políticas e portarias de gestão documental e arquivística da instituição.

Auto de eliminação ou anonimização

A equipa de investigação deve conservar, no **plano de gestão de dados**, no arquivo do projeto ou em registo próprio, de acordo com as políticas da instituição, os registos relativos ao apagamento ou à anonimização irreversível dos dados pessoais dos participantes.

Este registo deve incluir, pelo menos:

- a data em que ocorreu a eliminação ou anonimização;
- se anonimizados, o local onde ficam conservados;
- a identificação dos conjuntos de dados ou categorias de dados eliminados ou anonimizados;
- o tamanho aproximado dos dados apagados (por exemplo, em kilobytes ou megabytes);
- a identificação da pessoa responsável pela operação de eliminação ou anonimização;
- o método utilizado (ex.: eliminação segura, destruição física de suportes, sobrescrita de dados, anonimização irreversível, etc.);
- e, quando aplicável, a referência à norma ou à política interna que determinou o prazo e o procedimento de eliminação.

Os registos devem ser mantidos pelo período necessário para efeitos de auditoria, conformidade e rastreabilidade, nos termos das políticas de gestão de dados, de proteção de dados e de conservação arquivística da instituição.

Curadoria, reutilização e ciência aberta

A conservação, eliminação de dados e/ou a sua publicação e reutilização, constituem fases do ciclo de vida da gestão de dados, que inclui e se articula com as práticas de curadoria e preservação digital adotadas por cada instituição.

A reutilização refere-se à possibilidade de utilizar dados previamente recolhidos no âmbito de outras finalidades científicas ou novos projetos. Inclui, por exemplo, a aplicação dos dados em novos contextos de investigação, a replicação de estudos, a realização de meta-análises, a exploração de novas hipóteses ou desenvolvimento de aplicações práticas. Para que possam ser reutilizados, os dados devem ter passado por um processo de curadoria, ou seja, documentados com metadados, acessíveis em repositórios institucionais, temáticos ou generalistas, e preservados em formatos interoperáveis, preferencialmente formatos abertos e reconhecidos, como CSV, TXT, XML ou JSON. A curadoria de dados desempenha um papel fundamental na aplicação dos princípios FAIR, ao garantir que os dados sejam localizáveis, acessíveis, interoperáveis e reutilizáveis, promovendo a ciência aberta, a transparência científica e o potencial de reutilização responsável no ecossistema científico.

A reutilização, incluindo no âmbito da Ciência Aberta, deve cumprir os requisitos previstos no Nó **Informação ao participante e/ou Consentimento**, garantindo que os participantes foram devidamente informados e/ou prestaram consentimento específico para essa reutilização, conforme aplicável.

Em conformidade com as políticas de Ciência Aberta e os princípios FAIR, a disponibilização dos dados pode assumir diferentes modalidades de acesso, a documentar no **plano de gestão de dados**, e pode obedecer a eventuais restrições legais, éticas ou contratuais. Os dados, desde que **irreversivelmente anonimizados** e cujos participantes tenham dado consentimento prévio para o seu depósito, podem ser disponibilizados num repositório de acesso aberto, segundo uma das seguintes modalidades.

- acesso aberto sem restrições, o que permite a reutilização imediata por terceiros;
- acesso com embargo, ficando acessíveis em acesso aberto apenas após o decurso do período definido para o embargo; ou
- depositados no repositório com restrições de acesso, só acessíveis mediante pedido justificado e autorização institucional específica.

A escolha da modalidade deve respeitar os princípios FAIR, as políticas institucionais e as exigências dos financiadores em matéria de gestão e partilha de dados, assegurando, contudo, a conformidade, por um lado, com o regime de direitos de autor e, por outro, com o RGPD.

Direitos de autor e licenciamento

A publicação ou partilha de dados pode estar sujeita a direitos de autor, uma forma de propriedade intelectual reconhecida internacionalmente. Estes direitos surgem automaticamente como resultado da criação de uma obra original, abrangendo, por exemplo, publicações científicas, bases de dados, relatórios, software ou outros resultados de investigação.

A proteção por direitos de autor é matéria distinta do RGPD, sendo regulada por legislação específica, designadamente a Diretiva da EU relativa aos direitos de autor e direitos conexos no mercado único digital, e pela sua transposição para o ordenamento jurídico português através do Código do Direito de Autor e dos Direitos Conexos (CDADC), na sua redação atual. A proteção jurídica das bases de dados é atualmente assegurada pela Diretiva 96/9/CE do Parlamento Europeu e do Conselho de 11 de março de 1996 e a sua transposição para o ordenamento jurídico português através do DL n.º 122/2000, de 04 de julho.

Quer pretenda publicar ou partilhar dados reutilizados, quer esteja a planear disponibilizar os dados recolhidos no âmbito da sua investigação, é importante questionar-se sobre quem detém os direitos de autor dos conjuntos de dados por si utilizados e que licenças, autorizações ou obrigações podem estar associadas. A resposta depende de vários fatores, como quem contribuiu para a criação dos dados de investigação, de que tipo de dados se tratam[7], se foram utilizados dados provenientes de outros conjuntos de dados ou o que está estipulado no contrato de trabalho do investigador e/ou no regulamento de propriedade intelectual da instituição.

Por depender de múltiplos fatores, recomenda-se a consulta atenta das políticas institucionais e, em caso de dúvida, o apoio dos serviços competentes — nomeadamente o serviço responsável pela gestão de dados de investigação, que poderá acionar o gabinete jurídico se necessário. Ao disponibilizar dados, a equipa de investigação deve assegurar que possui os direitos necessários ou as autorizações adequadas para a sua partilha. Além disso, deve indicar claramente as condições de utilização através da atribuição de uma licença apropriada (por exemplo, uma licença Creative Commons ou equivalente), em conformidade com a legislação, as políticas institucionais e dos financiadores em matéria de acesso aberto e gestão de dados de investigação.

Licenças

Se vai publicar os seus dados de investigação num repositório de dados, deve aplicar uma licença aos dados. Uma licença é um acordo jurídico entre o criador/depositante do conjunto de dados e o repositório, que define o que os utilizadores estão autorizados a fazer com esses dados. Declarar claramente os direitos de reutilização dos dados é como colocar um acolhedor "Bem-vindo" à porta do seu conjunto de dados. Trata-se de garantir que os dados cumprem o princípio R (Reutilizáveis) da gestão de dados FAIR. Para maximizar as possibilidades de reutilização, recomenda-se a escolha de uma licença que torne os dados acessíveis ao maior número possível de utilizadores e permita a mais ampla variedade de utilizações — como a CC0, das licenças Creative Commons.

As licenças Creative Commons (CC) constituem um conjunto de licenças de direito de autor que permitem aos titulares dos direitos de autor definir de forma clara e padronizada as condições de reutilização das suas obras. Estas licenças permitem equilibrar a proteção da autoria com a disseminação e reutilização dos resultados de investigação.

[7] Dados em bruto, factos ou informações isoladas não são protegidos por direito de autor (mas podem ser protegidas por confidencialidade ou segredo comercial), porque não resultam de uma criação intelectual, e não contêm expressão criativa ou subjetiva. A proteção só surge quando os dados: (1) estão integrados numa obra original (ex.: um artigo científico, relatório de investigação, software, visualização de dados criativa, etc.), ou (2) fazem parte de uma base de dados que seja protegia nos termos da Diretiva 96/9/CE sobre proteção das bases de dados.

Existem seis licenças *Creative Commons* e dois instrumentos de domínio público. As licenças são perpétuas, gratuitas e universais. Cada licença combina diferentes condições de uso, oferecendo níveis graduais de abertura, estando acompanhada de um documento que permite facilmente entender os direitos que são licenciados ao utilizador:

- a CC BY (Atribuição): permite copiar, criar obras derivadas/compósitas e explorar comercialmente a obra, desde que seja dado crédito. A atribuição da autoria é o requisito mínimo, estando presente em todas as licenças;
- a CC BY-SA (Atribuição – CompartilhaIgual): permite qualquer utilização desde que seja dado crédito, mas exige que qualquer criação de obras derivadas/compósitas sejam licenciadas sob a mesma licença;
- a CC BY-ND (Atribuição – SemDerivações): permite qualquer utilização, desde que seja dado crédito, e sem modificações da obra;
- a CC BY-NC (Atribuição – NãoComercial): permite copiar, criar obras derivadas/compósitas, desde que seja dado crédito, mas impede a exploração comercial;
- a CC BY-SA-NC (Atribuição – CompartilhaIgual – NãoComercial): permite qualquer utilização desde que seja dado crédito, mas não permite a exploração comercial e exige que qualquer criação de obras derivadas/compósitas sejam licenciadas sob a mesma licença;
- a CC BY-ND-NC (Atribuição – SemDerivação – NãoComercial) - permite qualquer utilização, desde que seja dado crédito, sem modificações da obra e sem exploração comercial;
- e a CC0 (Domínio Público) – é um instrumento que permite ao criador intelectual renunciar a todos os direitos patrimoniais, permitindo a utilização sem restrições. Em Portugal, é obrigatório creditar a autoria da obra, mesmo em domínio público.

Para além da flexibilidade face a diferentes níveis de abertura, outros atributos da utilização das licenças CC incluem a facilidade de uso, ampla adoção pela comunidade científica, e a disponibilidade em formatos legíveis por humanos e por máquinas, permitindo que tanto investigadores como sistemas informáticos compreendam de forma imediata o que é permitido fazer com os dados.

Para facilitar a disponibilização de conjuntos de dados no domínio público, a CC criou o instrumento CC0. Com a CC0, o titular dos direitos renuncia a todos os seus direitos patrimoniais, incluindo o direito sobre a base de dados. Informação detalhada sobre as licenças Creative Commons está disponível no portal oficial: https://creativecommons.org/licenses

Metadados e documentação

A reutilização dos dados depende da existência de metadados completos, consistentes e atualizados, que descrevam o contexto da recolha, o conteúdo, a estrutura, as variáveis, bem como as condições de acesso, utilização e preservação. Os metadados são parte integrante do processo de curadoria de dados e devem ser armazenados e preservados juntamente com os conjuntos de dados, assegurando a conformidade com os princípios FAIR.

Por exemplo, ainda que um conjunto de dados não possa ser disponibilizado em acesso aberto por não cumprir as condições de anonimização ou por conter informações sensíveis e/ou sujeitas a direitos de terceiros, a publicação dos metadados continua a ser necessária pois permite dar visibilidade à existência do estudo, identificar o responsável pela investigação e promover a transparência e a possibilidade de contacto para eventuais pedidos de acesso controlado, a ser regulado por acordo formal.

Os metadados devem permitir compreender como e em que contexto os dados foram produzidos e processados, garantindo a interpretação correta, a rastreabilidade das versões e o suporte à validação científica dos resultados. Devem igualmente documentar transformações efetuadas, processos de anonimização e restrições de uso aplicáveis.

Sempre que possível, devem ser adotados padrões reconhecidos de metadados, como Dublin Core, DataCite ou CERIF, em conformidade com as recomendações do repositório institucional e das políticas institucionais de gestão de dados. A adoção destes esquemas facilita a interoperabilidade entre sistemas, melhora a descoberta e o acesso aos dados, e promove a reutilização responsável por outros investigadores e projetos.

Exemplos

Exemplo 1: Anonimização e publicação em acesso aberto de um conjunto de dados de entrevistas semiestruturadas

Um investigador em ciências sociais realizou entrevistas semiestruturadas com emigrantes acerca da sua experiência de integração. Após a transcrição dos testemunhos, procedeu à anonimização dos dados, removendo todos os elementos que pudessem identificar direta ou indiretamente os participantes, incluindo nomes, locais específicos e outras referências contextuais, e eliminando os dados brutos. Atendendo à sensibilidade dos dados, foram aplicadas técnicas de anonimização robustas, incluindo a generalização e agregação. Foi elaborado um auto de anonimização, no qual se registaram a data, a descrição dos dados anonimizados e o método utilizado, em conformidade com as políticas institucionais de gestão de dados. Os participantes tinham sido informados, através da Ficha de Informação ao Participante (FIP), de que os dados recolhidos seriam tratados de forma confidencial e que, após a anonimização, poderiam ser publicados para fins de investigação, tendo sido obtido consentimento específico para a publicação dos dados num repositório confiável, em acesso aberto, distinto do consentimento concedido para a participação nas entrevistas. Atendendo a que os dados anonimizados derivavam de dados pessoais sensíveis, o investigador solicitou a análise de um especialista em proteção de dados, garantindo a anonimização irreversível antes da publicação. Com o apoio dos serviços de curadoria de dados da instituição, e após a confirmação do processo de anonimização, o conjunto de dados foi publicado em acesso aberto no repositório institucional, sob uma licença CC BY, permitindo a sua reutilização para outros fins, desde que seja atribuída a devida autoria.

Exemplo 2: Conservação, eliminação da gravação de aulas e documentação de auto de eliminação

Um projeto de ciências da educação grava aulas de professores em escolas primárias para estudar metodologias pedagógicas. As gravações originais das aulas, que também contêm imagem e voz dos alunos, são guardadas em servidores encriptados e apenas acessíveis à equipa pelo tempo necessário à investigação. Os encarregados de educação e os professores observados foram informados na FIP, que integrava o formulário de consentimento, sobre o destino das gravações, as condições de armazenamento e os prazos de conservação após o qual as gravações seriam eliminadas. Após esse prazo, os investigadores eliminaram as gravações e registaram no arquivo do projeto um auto de eliminação com a data em que ocorreu, as categorias de dados eliminadas, o tamanho dos dados e o método de eliminação utilizado.

Exemplo 3: Limitações à partilha de dados anonimizados quando o consentimento inicial não previu essa possibilidade

Um projeto na área da saúde recolheu dados de diários alimentares de pacientes com doenças metabólicas, com base em consentimento. Os participantes forneceram informação detalhada sobre os seus hábitos alimentares e estilos de vida. Durante o estudo, os investigadores procederam à anonimização dos dados, conforme se tinham comprometido na Ficha de Informação ao Participante (FIP). No entanto, a FIP não mencionava a possibilidade de outras utilizações dos dados para além dos objetivos imediatos da investigação, designadamente a partilha em acesso aberto dos dados anonimizados. Assim, uma vez que os participantes não tinham dado consentimento específico para essa finalidade, o conjunto de dados anonimizados não pôde ser disponibilizado em acesso aberto no repositório institucional. Além disso, a natureza da informação recolhida — hábitos alimentares muito específicos, combinações de alimentos pouco comuns e enquadramento cultural ou geográfico particular — implicava um risco residual de reidentificação, reforçando a impossibilidade de publicação ou partilha sem consentimento adicional dos participantes. Dado que a anonimização já tinha sido concluída, implicando a eliminação dos dados brutos e identificadores, não era possível contactar novamente os participantes para obter o consentimento necessário, o que tornou inviável a disponibilização dos dados em acesso aberto.

Exemplo 4: Direitos de autor e licenciamento de software e dados derivados

Uma equipa de engenharia desenvolveu um software para análise de imagens de satélite que produziu um conjunto de dados derivados. De acordo com os regulamentos institucionais, os direitos de autor sobre o software pertencem à instituição. Para proteger o código e os algoritmos proprietários, a equipa publicou apenas os dados derivados, devidamente documentados, sob licença CC BY-NC-SA, permitindo a sua reutilização não comercial com atribuição. O software foi disponibilizado separadamente sob licença **EUPL (European Union Public Licence)**, que permite a sua reutilização e modificação, desde que se mantenha a mesma licença e se reconheça a autoria institucional. Desta forma, assegurou-se a proteção da propriedade intelectual e a conformidade com o enquadramento jurídico europeu, promovendo simultaneamente a transparência e a ciência aberta.

Listas de verificação:

Gestão e conservação de dados

- Definiu um prazo de conservação dos dados pessoais estritamente necessário à prossecução dos objetivos da investigação, em conformidade com as políticas institucionais em vigor? Foram definidos critérios objetivos para determinar o termo dos prazos (por exemplo, conclusão do relatório final, entrega ao financiador ou publicação dos resultados)?
- Indicou na Ficha de Informação ao Participante (FIP) os prazos de conservação previstos?
- Indicou na FIP se, após os prazos de conservação, os dados seriam eliminados ou anonimizados?

Após o termo do prazo de conservação

- Procedeu à eliminação segura dos dados, utilizando métodos adequados e irreversíveis?
- Assegurou a eliminação de todas as cópias, incluindo versões locais, temporárias e pastas de reciclagem? Verificou se a eliminação foi realizada também em cópias de segurança (backups) ou em suportes externos (pen drives, discos, nuvem)?
- Caso a FIP tenha informado que destino final dos dados era a anonimização, verificou que esta foi realizada de forma irreversível, cumprindo os requisitos do Nó **Anonimização**?
- Confirmou que todos os consentimentos informados, bem como os dados e mensagens de contacto com os participantes (e.g., emails, SMS, registos de recrutamento), foram devidamente apagados?
- Elaborou e arquivou o Auto de Eliminação ou Anonimização, contendo todos os elementos exigidos pelas políticas institucionais?

Depósito, publicação e reutilização de dados

- No caso de pretender reutilizar dados anonimizados, verificou se o consentimento inicial incluía autorização específica para esse efeito, de acordo com o Nó **Dever de Informação e Consentimento**?
- Avaliou que tipo de licença (por exemplo, Creative Commons) é mais adequada à disponibilização dos dados, considerando a titularidade dos direitos de autor, as políticas institucionais nessa matéria e as exigências dos financiadores?

- O depósito e publicação dos dados obedecem aos princípios FAIR? Ponderou a modalidade de acesso mais apropriada para o depósito dos dados (acesso aberto, com embargo ou restrito), tendo em conta a sensibilidade dos dados, eventuais direitos de terceiros ou condicionalismos éticos ou legais?

- Assegurou que o depósito dos dados foi acompanhado pela documentação necessária (metadados, descrições, contexto metodológico), exigidas pelos regulamentos ou políticas institucionais em vigor?

Ligações úteis:

- CESSDA Training Team. (n.d.). *Licensing your data*. Data Management Expert Guide. CESSDA. Disponível em: https://dmeg.cessda.eu/Data-Management-Expert-Guide/6.-Archive-Publish/Publishing-with-CESSDA-archives/Licensing-your-data

- Creative Commons. (n.d.). *About CC licenses*. Creative Commons. Disponível em: https://creativecommons.org/licenses

- Decreto-Lei n.º 15/2000, de 29 de fevereiro. Disponível em: https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2000-124444219-124445326

- Decreto-Lei n.º 344/85, de 23 de agosto. Disponível em: https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1985-34475475

- ISCTE-IUL Biblioteca. (n.d.). *Guia Creative Commons*. Bibliosubject. Disponível em: https://bibliosubject.iscte-iul.pt/sp4/subjects/guide.php?subject=CCguide

- Open Data Commons. (n.d.). *Public Domain Dedication and License (PDDL) v1.0*. Open Knowledge Foundation. Disponível em: https://opendatacommons.org/licenses/pddl/

- Parlamento Europeu e Conselho da União Europeia. (1996). *Diretiva 96/9/CE de 11 de março de 1996 relativa à proteção jurídica das bases de dados*. Jornal Oficial das Comunidades Europeias, L 77, 20–28. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:31996L0009

- Parlamento Europeu e Conselho da União Europeia. (2019). *Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC*. Official Journal of the European Union, L 130, 92–125. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32019L0790

- União Europeia. (2016). *Licença Pública da União Europeia v. 1.2 (EUPL)*. Disponível em: https://eupl.eu/1.2/pt.

- European Data Protection Supervisor (EDPS) (2020). Opinion 3/2020 on the European strategy for data and the European Research Area – scientific research and data protection. Brussels, 6 January 2020. Disponível em https://www.edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf.

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Recolha e tratamento de dados (Nó 12)

Carregue aqui para avançar para o nó seguinte – Resposta ao exercício de direitos (Nó 14)

14. Resposta ao exercício de direitos

Clarificação de conceitos

O tratamento de dados pessoais confere aos titulares desses dados direitos que lhes permitem zelar pela sua proteção, assegurando o controlo sobre os seus dados pessoais. Cada instituição, no seu papel de **Responsável pelo Tratamento (RT)**, deve, por isso, dispor de procedimentos claros e eficazes para a receção e tramitação dos pedidos de exercício de direitos, de forma facilmente acessível e que garanta a sua efetividade.

No contexto dos projetos de investigação, esta responsabilidade cabe, em regra, aos coordenadores dos projetos, que devem assegurar que existem mecanismos internos adequados para responder a pedidos de acesso, retificação, apagamento ou oposição.

A Ficha de Informação ao Participante (FIP) deve incluir um contacto específico para o efeito, designadamente um endereço de email da equipa ou do projeto, para o qual os participantes possam dirigir os seus pedidos relativos aos seus dados pessoais.

Quais são os direitos dos titulares dos dados?

1. Direito à informação (RGPD, Artigos 12º, 13.º e 14.º) – Direito a receber informações sobre o tratamento dos seus dados pessoais. Essas informações deverão ser concisas, transparentes, inteligíveis e de fácil acesso, utilizando uma linguagem clara e simples, em conformidade com o princípio da Lealdade e Transparência. Em investigação realizada sob o consentimento dos participantes, essa informação deve ser prestada junto à restante informação ao participante. Para informações sobre os conteúdos a incluir consulte o Nó **Informação ao Participante ou Consentimento**.

2. Direito de acesso (RGPD, artigo 15.º) – Direito a questionar se os seus dados pessoais são ou não objeto de tratamento e, se em caso afirmativo, o direito de aceder aos seus dados pessoais e a informações sobre o tratamento.

3. Direito de retificação (RGPD, artigo 16.º) – Direito a obter a retificação dos seus dados pessoais que se provem inexatos.

4. Direito ao apagamento dos dados | «direito a ser esquecido» (RGPD, artigo 17.º) – Direito ao apagamento dos seus dados pessoais. A satisfação deste direito do titular depende dos direitos e obrigações do Responsável pelo Tratamento (RT). Genericamente o RT só terá de apagar os dados se já não tiver base de licitude para os tratar. Isto significa que, se a base legal para o tratamento for o consentimento, a retirada desse consentimento por parte do participante implica, em regra, a obrigação de se proceder ao apagamento dos dados.

5. Direito à limitação do tratamento (RGPD, artigo 18.º) – Direito a condicionar o tratamento dos dados pessoais quando haja fundadas razões que o justifique, nos termos do artigo 18.º do RGPD.

6. Direito de portabilidade dos dados (RGPD, artigo 20.º) – Direito, em determinados casos, de receber os dados pessoais num formato estruturado, de uso corrente e de leitura automática.

7. Direito de oposição (RGPD, artigo 21.º) – Direito de se opor a tratamentos realizados no âmbito de tratamentos posteriores de dados, exercício de funções de interesse público, ou para efeitos da prossecução de interesses legítimos do responsável ou de terceiros.

8. Direito de retirar o consentimento (RGPD, artigo 7.º, n.º 3) – Direito a retirar o consentimento para o tratamento dos seus dados pessoais, a qualquer momento e sem apresentação de motivo.

9. Direito a contactar o Encarregado da Proteção de Dados (RGPD, artigo 38.º, n.º 4) – Os titulares dos dados podem contactar o encarregado da proteção de dados sobre todas as questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo RGPD.

10. Direito de apresentar reclamação à autoridade de controlo (RGPD, artigo 77.º) – Direito a apresentar reclamação a uma autoridade de controlo se considerar que o tratamento dos dados pessoais que lhe diga respeito viola o regime de proteção de dados.

A resposta ao exercício de direitos pelos Participantes deve ser fornecida o mais rapidamente possível, não podendo, em qualquer caso, exceder o prazo máximo de um mês a contar da data de receção do pedido. Esse prazo pode ser prorrogado por até um mês, quando a complexidade do pedido ou o número de pedidos recebidos o justifiquem. As razões da prorrogação devem ser comunicadas ao Participante dentro do prazo inicial.

Prazos, obrigações e exceções

- Os direitos dos titulares dos dados cessam a partir do momento que os dados sejam irreversivelmente anonimizados, porque deixará de ser possível saber de quem são os dados.

- Perante um pedido de exercício de direitos, deve ser verificada a identidade do titular dos dados antes de lhe ser dada resposta, de acordo com as políticas da instituição, e de modo a garantir que o acesso ou a alteração das informações não é efetuado por pessoa não autorizada.

- No caso da equipa de investigação tiver a intenção de recusar, total ou parcialmente, um pedido de exercício de direitos, recomenda-se a consulta ao Encarregado de Proteção de Dados (EPD) e que verifique as políticas internas da instituição relativas ao tratamento desses pedidos, incluindo eventual necessidade de parecer da Comissão de Ética antes da decisão final.

- Em casos devidamente justificados, os direitos de acesso, retificação, apagamento, limitação do tratamento e oposição, previstos nos artigos 15.º, 16.º, 17.º, 18.º e 21.º do RGPD, podem ser limitados na medida do necessário, se o seu exercício for suscetível de tornar impossível ou prejudicar gravemente a realização dos fins da investigação [Lei 58/2019, artigo 31.º, n.º 2, e RGPD, artigo 17.º, n.º 3, alínea d)].

    - Os titulares devem receber explicação clara sobre a limitação desses direitos, juntamente com as restantes informações sobre o tratamento.

    - **Importa salientar que esta possibilidade de limitação deve ser abordada com especial cautela**, representando um fator de risco adicional, que deve ser expressamente considerado na identificação e avaliação dos **fatores críticos de risco** do projeto.

    - Na eventualidade de limitação de direitos, recomenda-se a consulta ao Encarregado de Proteção de Dados (EPD), a qual poderá ser obrigatória, dependendo das políticas internas da instituição.

Exemplos:

Exemplo 1: Uma participante num estudo de psicologia sobre hábitos de sono solicita acesso aos dados que forneceu num questionário online. A equipa de investigação confirma a identidade da participante e, no prazo de um mês, envia-lhe um ficheiro com as suas respostas individuais, acompanhado de uma explicação sobre como esses dados estão a ser tratados e protegidos.

Exemplo 2: Um participante num estudo em saúde pública nota que a sua data de nascimento foi registada incorretamente. Ele exerce o seu direito de retificação e a equipa de investigação corrige o dado na base de dados, documentando a alteração e confirmando ao participante, por escrito, a atualização realizada.

Exemplo 3: Uma estudante que participou numa investigação sobre metodologias de ensino solicita a eliminação da sua entrevista gravada, invocando o direito de retirar o consentimento. A equipa elimina o ficheiro de áudio e as transcrições associadas, regista a eliminação nos relatórios internos e informa a participante de que os dados foram apagados de forma irreversível.

Exemplo 4: Uma participante de um estudo de ciências sociais solicita o apagamento dos seus dados um ano após a recolha. Contudo, a equipa informa que os dados já tinham sido anonimizados de forma irreversível e que, por esse motivo, deixou de ser possível identificar quais eram os dados da participante. A resposta é enviada de forma clara e transparente, explicando a limitação prevista no RGPD e nas normas éticas de investigação.

Perguntas de controlo

Tem preparados instrumentos e procedimentos para resposta ao exercício de direitos dos titulares?

Se sim, quando receber um pedido de exercício de direitos garanta que o atende sem demora injustificada, no prazo máximo de um mês.

Em casos excecionais, o prazo pode ser prorrogado até dois meses, quando a complexidade do pedido ou o número de pedidos recebidos o justifique. As razões da prorrogação devem ser comunicadas ao titular dentro do prazo inicial de um mês.

Nos casos excecionais ou de maior complexidade, recomenda-se a consulta prévia ao serviço competente no domínio de investigação da sua instituição, para avaliar a melhor forma de resposta, e, quando o pedido envolva questões sensíveis de proteção de dados ou potenciais limitações de direitos, a consulta ao Encarregado de Proteção de Dados (EPD) antes da decisão final.

Se não, determine os direitos que se aplicam ao seu tratamento. Deverá ainda:

- Estabelecer os instrumentos para receber os pedidos dos titulares e os procedimentos para lhes dar resposta.

- Informar os titulares dos direitos disponíveis e de eventuais limitações.

- Informar os titulares da forma como exercer os seus direitos.

Ligações úteis:

- Artigos 7.º, 12.º, 13.º, 14.º, 15.º, 16.º, 17.º, 18.º, 20.º, 21.º, 38.º, 77.º do RGPD. Disponíveis em: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Publicação, conservação ou eliminação e licenças (Nó 13)

Carregue aqui para avançar para o nó seguinte – Resposta a incidentes de segurança de violação de dados (Nó 15)

15. Resposta a incidentes de segurança e violação de dados

Clarificação de conceitos

Uma violação de dados pessoais é uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. A violação de dados pessoais não diz respeito a não conformidades com o RGPD, mas sim a incidentes de segurança com dados pessoais que afetem a sua confidencialidade, integridade ou disponibilidade.

Sempre que ocorrer uma ou mais violações de dados pessoais, esses incidentes devem ser documentados, registando os factos que caraterizam essa violação de dados, os efeitos dessa violação e as medidas de mitigação. Garanta que conhece os procedimentos da instituição que acolhe a sua investigação para comunicação de violações de dados pessoais à equipa competente na sua instituição. Tipicamente, este processo envolve informar de imediato a direção da instituição, a equipa de segurança operacional (SOC) e o Encarregado de Proteção de Dados (EPD).

As violações de dados pessoais que possam representar risco para os titulares dos dados devem ser notificadas à Comissão Nacional de Proteção de Dados (CNPD) sem demora injustificada e, sempre que possível, no prazo máximo de 72 horas após a sua deteção.

Essa notificação é decidida e realizada pela direção da instituição, em articulação com o Encarregado de Proteção de Dados (EPD), de acordo com os procedimentos internos definidos para a gestão de incidentes de segurança e violações de dados pessoais.

Exemplos:

Exemplo 1: Se perdeu, ou lhe foi roubado um computador portátil onde estivessem dados pessoais de investigação, isso constitui uma violação de dados pessoais, por violação da sua confidencialidade.

Exemplo 2: Se se enganou no destinatário de um e-mail, e enviou para o destinatário errado dados pessoais da sua investigação, isso constitui uma violação de dados pessoais.

Exemplo 3: A *password* da sua conta de correio eletrónico foi comprometida, e na sua caixa de mensagens enviadas estava um ficheiro não cifrado e não anonimizado com dados pessoais de investigação. Isso constitui uma violação de dados pessoais.

Perguntas de controlo

Sofreu um incidente com os seus dados que tenha resultado em acesso ou divulgação, destruição, perda ou alteração não autorizados?

Se não, não se aplicam orientações a esse respeito.

Se sim, deverá comunicar de imediato o incidente ao serviço competente da sua instituição, que procederá à sua análise e classificação, em articulação com o Encarregado de Proteção de Dados (EPD).

De acordo com os procedimentos institucionais, caberá à direção da instituição, em articulação com o Encarregado de Proteção de Dados, notificar a autoridade de controlo (CNPD) sempre que o incidente possa representar risco para os titulares dos dados.

Quando o incidente possa implicar um risco elevado para os titulares, estes serão igualmente informados, de forma clara e tempestiva, sobre a natureza da violação e as medidas adotadas para mitigar os seus efeitos.

Ligações úteis:

- Artigos 4.º 12), 33.º e 34.º do RGPD. Disponíveis em: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

NAVEGADOR

Carregue aqui para voltar ao menu inicial

Carregue aqui para voltar ao nó anterior – Resposta a exercício de direitos (Nó 14)

GLOSSÁRIO

Anonimização

Conversão irreversível de dados pessoais em dados anónimos de forma que deixem de poder ser atribuídos a titulares de dados identificados ou identificáveis, tendo em conta todos os meios razoáveis suscetíveis de serem utilizados para reidentificação. Admite-se apenas um risco residual ou negligenciável de reidentificação, resultante de meios técnica ou economicamente desproporcionais.

Base Legal do Tratamento

É o fundamento jurídico que torna legítimo o tratamento de dados pessoais, ou seja, a razão reconhecida por lei que autoriza uma entidade – como um investigador, uma universidade ou uma empresa – a recolher e tratar esses dados. Na investigação científica, a base legal mais comum é o consentimento do participante, mas podem também aplicar-se outras, como o interesse público, o cumprimento de obrigação legal, a execução de contrato, ou o interesse legítimo do responsável pelo tratamento, desde que cumpridos os requisitos legais aplicáveis.

Categorias especiais de dados

São dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, os dados genéticos, dados biométricos que identifiquem uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

Consentimento do titular de dados

Uma manifestação de vontade, livre, específica, informada e inequívoca ou explícita pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento para uma determinada finalidade.

Dados de natureza altamente pessoal

Trata-se de dados pessoais ligados a atividades privadas ou familiares (tais como comunicações eletrónicas cuja confidencialidade deve ser protegida) ou porque afetam o exercício de um direito fundamental (tais como dados de localização cuja recolha põe em causa a liberdade de circulação) ou porque a sua violação implica claramente que a vida quotidiana do titular dos dados será

gravemente afetada (tais como dados financeiros que possam ser utilizados numa fraude de pagamentos).

Dados Pessoais

Informação relativa a uma pessoa singular identificada ou identificável ("Titular dos Dados"); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Dados Secundários

Informações já recolhidas previamente por outras pessoas, instituições, estudos ou dados disponíveis publicamente, e que são reutilizadas para uma nova investigação, análise ou finalidade diferente da original.

Decisões individuais automatizadas (DIA) ou Decisões automatizadas por algoritmos

As decisões individuais *exclusivamente* automatizadas ocorrem quando são tomadas decisões sobre uma pessoa singular por meios tecnológicos e sem envolvimento humano. Podem ser efetuadas mesmo sem definição de perfis. Se uma pessoa controlar a decisão final fornecida pelo algoritmo, com efetiva competência ou possibilidade de influenciar o resultado final, a decisão pode ser considerada não "exclusivamente" automatizada. Mas a contribuição ou viés do tratamento automático na decisão pode não ser fácil de distinguir.

Definição de perfis

Qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

Ficha de Informação ao Participante (FIP)

Uma ficha com informações a facultar aos titulares de dados sobre a finalidade do tratamento de dados, o fundamento legal para o tratamento, o que acontece aos dados e os riscos envolvidos, de acordo com os arts. 13º e 14º do RGPD.

Finalidade legítima
Os fins para os quais os dados pessoais podem ser utilizados.

Formulário de Consentimento
Documento através do qual é recolhido um ou mais consentimentos dos participantes, cada um relativo a uma finalidade do projeto, integrando as informações previstas na Ficha de Informação ao Participante (FIP). Constitui o meio formal de registo da manifestação de vontade do titular dos dados, devendo assegurar que todos os consentimentos considerados válidos são prestados de forma livre, informada, específica e inequívoca, e que cada um deles se encontra devidamente documentado.

Proteção de Dados Pessoais
Um direito fundamental, protegido não apenas pela legislação nacional, mas pela legislação europeia.

Pseudonimização
O tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico 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.

Reidentificação
Processo de transformar dados que se creem anonimizados novamente em dados pessoais por meio de correspondência de dados ou técnicas semelhantes.

Responsável pelo Tratamento
A pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outros, determina as finalidades e os meios do tratamento de dados pessoais. Em contexto de investigação científica ou académica, o responsável pelo tratamento é, regra geral, a instituição onde o projeto está sediado, uma vez que é esta que define as finalidades e os meios essenciais do tratamento e assegura o cumprimento das obrigações legais e institucionais em matéria de proteção de dados. **Assim, o investigador ou a equipa de investigação não são o responsável pelo tratamento.** Atuam, sob a autoridade da instituição, no quadro das suas políticas internas de proteção de dados e ética na investigação.

Subcontratante

Uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

Titular dos Dados

Qualquer pessoa singular identificada ou identificável que seja objeto de dados pessoais detidos pelo responsável pelo tratamento. No contexto deste Toolkit, e em particular na investigação científica, utiliza-se igualmente o termo “participante” para designar o titular dos dados que colabora ou fornece informações no âmbito de um estudo ou projeto de investigação.

Tratamento de Dados Pessoais

Uma operação ou um conjunto de operações efetuadas sobre Dados Pessoais ou sobre conjuntos de Dados Pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Violação de dados pessoais

Uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

NOTAS FINAIS

Este *Toolkit* foi elaborado com recurso a uma utilização responsável de ferramentas de Inteligência Artificial, mais concretamente *Large Language Models* (LLMs), que apoiaram a revisão de texto e a criação de exemplos ilustrativos. O uso destas ferramentas foi sempre entendido como complementar ao trabalho dos autores, sendo sujeito a uma supervisão crítica e cuidadosa, de forma a assegurar rigor, clareza e adequação.

Convidamos o utilizador deste *Toolkit* a acompanhar novos desenvolvimentos e atualizações que venham a surgir no âmbito do Fórum GDI, espaço privilegiado de reflexão contínua e partilha de boas práticas sobre a gestão e tratamento de dados em investigação. Neste espaço, será possível acompanhar também o debate e a clarificação de questões jurídicas, de proteção de dados e de licenciamento, fundamentais para um exercício responsável e sustentável da atividade científica.