

FÓRUM
GESTÃO DE DADOS
DE INVESTIGAÇÃO

Instituto Politécnico de Bragança

27 e 28 de novembro de 2025

Toolkit sobre questões jurídicas, proteção de dados e licenças



Re.Data
Rede para a Gestão de
Dados de Investigação



Universidade do Minho



UNIVERSIDADE D
COIMBRA



INSTITUTO
UNIVERSITÁRIO
DE LISBOA



BRAGANÇA INSTITUTO POLITÉCNICO
DE BRAGANÇA



UNIVERSIDADE NOVA
DE LISBOA



serviços
digitais
fct



Fundação
para a Ciência
e a Tecnologia



Plano de Recuperação
e Resiliência



REPÚBLICA
PORTUGUESA



Financiado pela
União Europeia
NextGenerationEU

Toolkit sobre questões jurídicas, proteção de dados e licenças



Re.Data

Rede para a Gestão de
Dados de Investigação

Versão preliminar
setembro | 2025

Autoria:

Nuno David, Marta Cordeiro, Gabriel Cipriano, Clara Boavida,
Jorge Figueiredo, Cláudia Conceição, Paula Ochôa, Kevin
Gallagher e Carina Cunha

Concebido para apoiar investigadores no planeamento e execução de
projetos de investigação com recurso a dados pessoais.

Principal objetivo:

Criação de uma ferramenta de fácil utilização, orientada para a ação
e adaptada ao contexto académico real, alinhada com o

Regulamento Geral sobre a Proteção de Dados.



Re.Data

Rede para a Gestão de
Dados de Investigação

TOOLKIT SOBRE QUESTÕES JURÍDICAS, PROTEÇÃO DE DADOS E LICENÇAS

novembro | 2025

Apolo
FCCN

serviços
digitais
fct

fct
Fundação
para a Ciência
e a Tecnologia

Financiamento
PRR

REPÚBLICA
PORTUGUESA

Financiado pela
União Europeia
NextGenerationEU

workshop

QUESTÕES JURÍDICAS, PROTEÇÃO DE
DADOS E LICENÇAS



16 DE OUTUBRO



Iscte – Instituto Universitário
de Lisboa

Revisão técnica e contributos de especialistas em proteção de dados, nomeadamente:

- Encarregados de Proteção de Dados (DPO) de IES
- Membros de Comissões de Ética de IES
- Juristas em proteção de dados
- Direção-Geral do Livro, dos Arquivos e das Bibliotecas
- Associação dos Profissionais de Proteção de Dados
- Creative Commons Portugal
- Data Stewards
- Investigadores



Toolkit sobre questões jurídicas, proteção de dados e licenças

Planeamento da Investigação	1. Considere elaborar um plano de gestão de dados	1
	2. Recolhe dados pessoais?	3
	3. Identifique os responsáveis e as fontes dos dados:	6
	a) Avalie a existência de responsabilidade conjunta	10
	4. Planeie a minimização de dados	13
	5. Planeie a anonimização	16
	6. Planeie a pseudonimização	21
	7. Identifique e avalie os fatores críticos de risco:	25
	a) Dados sensíveis?	29
	b) Transferências internacionais de dados pessoais?	32
Investigação e Pós-Investigação	c) Menores de idade ou populações vulneráveis?	36
	d) Tratamento em larga escala?	39
	e) Definição de perfis?	41
	f) Decisões automatizadas por algoritmos?	43
	g) Controlo sistemático?	45
	h) Combinam-se bases de dados?	47
	i) Envolve inteligência artificial ou outras novas soluções tecnológicas?	48
	j) Exposição a elevado risco ético?	54
	8. Escolheu software adequado?	57
	9. Existe subcontratação?	61
Direitos e Deveres	10. Planeie medidas de proteção e de mitigação de risco, técnicas e organizativas	64
	11. Implemente a informação ao participante e/ou consentimento	69
	12. Implemente a recolha e tratamento de dados	81
	13. Publicação, conservação ou eliminação, e licenças	83
	14. Resposta a exercício de direitos	90
	15. Resposta a incidentes de segurança de violação de dados	93

Existe uma **Árvore de decisão** inicial que permite explorar os diversos nós do toolkit.

A **azul** estão identificados os nós principais

A **cinzento**, quando necessário, os nós complementares associados.

O utilizador pode percorrer todos os nós pela ordem proposta ou, em alternativa, pode clicar diretamente em cada título para ser reencaminhado para o respetivo conteúdo.


Dentro de cada nó há ligações para os outros nós.

No final de cada nó, existe sempre um navegador que permite ao utilizador voltar à árvore de decisão inicial, regressar ao nó anterior ou avançar para o nó seguinte.

Todos os nós da Árvore de decisão têm:

1) Clarificação de conceitos; 2) Exemplos concretos e práticos, 3) Perguntas direcionadas sobre o projeto de investigação, 4) Respostas adequadas em função das perguntas, 5) Ligações úteis (quando necessário), 6) Navegador.

29



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.

30




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: Num 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.

31


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 \(Nó 7b\)](#) 



Re.Data

Rede para a Gestão de
Dados de Investigação

641.52

555.74

TOOLKIT SOBRE QUESTÕES JURÍDICAS, PROTEÇÃO DE DADOS E LICENÇAS

411.08

64.85

81.79

novembro | 2025

Apoio
FCCN

serviços
digitais
fct

fct

Fundação
para a Ciência
e a Tecnologia

Financiamento
PRR

REPÚBLICA
PORTUGUESA

Financiado pela
União Europeia
NextGenerationEU

764.77

921.54

Consulte o toolkit em
www.redata.pt



<https://doi.org/10.5281/zenodo.17632500>