

ORIENTAÇÕES AOS INVESTIGADORES SOBRE PROTEÇÃO DE DADOS PESSOAIS EM ATIVIDADES DE INVESTIGAÇÃO CIENTÍFICA NO ISCTE – INSTITUTO UNIVERSITÁRIO DE LISBOA

Constituem atribuições do Iscte-Instituto Universitário de Lisboa (adiante designado Iscte) realizar investigação científica e ciclos de estudo, incluindo mestrados e doutoramentos, onde se desenrolam atividades de investigação científica ou histórica que tratam dados pessoais.

O tratamento de dados pessoais para fins de investigação científica entende-se em sentido lato, abrangendo, por exemplo, o desenvolvimento tecnológico e a demonstração, a investigação fundamental ou aplicada, a investigação histórica, a investigação para fins genealógicos ou a investigação financiada pelo setor privado.¹

São deveres dos investigadores, e também dos docentes, funcionários, alunos e colaboradores envolvidos em atividades de investigação do Iscte, cumprir padrões éticos de respeito pela privacidade dos participantes em trabalhos de investigação e a legislação de proteção de dados em vigor.

Este documento resume a perspetiva do Iscte relativamente à legislação de proteção de dados para a investigação científica e histórica, em particular o enquadramento decorrente do Regulamento Geral sobre a Proteção de Dados (RGPD) e da Lei 59/2019, de 08/08 – Lei de Execução, na ordem jurídica nacional, do RGPD.

As orientações expressas neste documento não prejudicam a autonomia científica dos investigadores, nem dispensam os investigadores da consulta da [Política de Proteção de Dados do Iscte](#), demais orientações dos órgãos competentes do Iscte, legislação aplicável e do [Código de Conduta Ética na Investigação do Iscte](#).

¹ RGPD, considerando 159º.

| | | |
|-----|---|----|
| A. | A proteção de dados, a investigação e o princípio da responsabilidade | 3 |
| B. | Estou a usar dados pessoais? | 4 |
| B.1 | O conceito de dados pessoais | 4 |
| B.2 | Categorias especiais de dados pessoais | 5 |
| B.3 | Dados de natureza altamente pessoal | 6 |
| B.4 | Registo de imagem, voz ou vídeo | 6 |
| C. | Anonimização ou pseudonimização? | 6 |
| C.1 | Anonimização | 6 |
| C.2 | Pseudonimização | 7 |
| D. | Papeis e responsabilidades | 8 |
| D.1 | Responsável pelo tratamento | 8 |
| D.2 | A quem incumbe a obrigação de assegurar a conformidade de projetos de investigação científica com o RGPD? | 8 |
| D.3 | A quem incumbe a obrigação de assegurar a conformidade dos trabalhos de teses e dissertações com o RGPD? | 8 |
| D.4 | Responsabilidade conjunta pelo tratamento | 8 |
| D.5 | Subcontratantes do Iscte | 9 |
| D.6 | O Iscte como subcontratante | 9 |
| E. | Medidas técnicas e organizativas | 9 |
| E.1 | Medidas de carácter geral | 10 |
| E.2 | Medidas adicionais para tratamentos suscetíveis de maior risco (e.g. categorias especiais de dados) | 11 |
| F. | Finalidade do tratamento, princípios e direito do participante a ser informado | 11 |
| F.1 | Finalidade do tratamento, limitação das finalidades, licitude e transparência | 11 |
| F.2 | Ficha de Informação ao Participante (FIP) | 12 |
| G. | Tratamento com fundamento legal em consentimento dos titulares de dados | 13 |
| G.1 | Manifestação de vontade, livre, específica, informada e inequívoca ou explícita | 13 |
| G.2 | E quando a finalidade do tratamento não for inteiramente conhecida? | 14 |
| G.3 | Consentimento dos titulares de dados vs. consentimento de participantes humanos na investigação | 15 |
| H. | Tratamento com fundamento legal baseado em funções de interesse público ou Prosecução de interesses legítimos | 16 |
| H.1 | Exercício de funções de interesse público | 16 |

| | | |
|-----|---|----|
| H.2 | Prossecação de interesses legítimos..... | 16 |
| H.3 | Que informações devem ser providenciadas ao participante? | 17 |
| H.4 | Interesse público no âmbito de tratamento de categorias especiais de dados | 17 |
| I. | Prazos de conservação | 18 |
| I.1 | Prazos máximos de conservação no Iscte | 18 |
| J. | Direitos dos titulares de dados | 19 |
| J.1 | Quais os direitos dos titulares de dados e a quem se devem dirigir?..... | 19 |
| J.2 | É possível não satisfazer pedidos relativamente a direitos dos titulares de dados?.. | 19 |
| J.3 | Prazos para resposta a pedidos de exercício de direitos | 20 |
| K. | Aplicação de inquéritos à comunidade Iscte para efeitos de investigação científica..... | 20 |
| L. | Uso de dados pessoais de outras fontes..... | 20 |
| M. | Transferências para países fora do Espaço Económico Europeu e recolha fora do EEE..... | 21 |
| M.1 | Transferências para países com «decisão de adequação» | 22 |
| M.2 | Transferências para países sem «decisão de adequação» | 22 |
| N. | Acesso a arquivos com dados pessoais de pessoas falecidas | 23 |
| O. | Avaliação de impacto na proteção de dados | 23 |
| O.1 | Quando é necessário realizar uma avaliação de impacto? | 23 |
| O.2 | A quem incumbe realizar a avaliação de impacto?..... | 26 |
| P. | Violação de dados pessoais..... | 27 |
| Q. | Comissão de Ética e Encarregado de Proteção de Dados | 27 |
| R. | Documentos e ligações úteis..... | 27 |
| S. | Definições..... | 28 |

A. A PROTEÇÃO DE DADOS, A INVESTIGAÇÃO E O PRINCÍPIO DA RESPONSABILIDADE

A proteção de dados desempenha um papel ético e legal central na investigação científica.² Está intimamente ligada ao direito que os sujeitos da investigação têm à proteção da sua vida privada, conferindo-lhes controle sobre a forma como as suas informações pessoais são recolhidas e usadas.

² O direito à proteção de dados está consagrado na Carta dos Direitos Fundamentais da União Europeia (UE), no Tratado sobre o Funcionamento da UE e no artigo 35º da Constituição da República Portuguesa.

A inadequada conduta ética no tratamento de dados e/ou o não cumprimento da legislação pode ter consequências devastadoras para os titulares de dados e consequências legais, reputacionais e financeiras para o Iscte e/ou demais responsáveis pelo tratamento.

São dois os principais articulados a ter em conta no cumprimento da legislação de proteção de dados em Portugal: o RGPD e a Lei de Execução, na ordem jurídica nacional, do RGPD.³ O RGPD aplica-se a todo o Espaço Económico Europeu e diretamente a Portugal enquanto membro da União Europeia (UE). A Lei de Execução dispõe sobre um conjunto de normas do RGPD com particularidades de concretização em Portugal.

O regime do RGPD para a investigação científica prevê algumas derrogações relativas às obrigações dos responsáveis pelo tratamento, em particular o artigo 89º, conferindo maior flexibilidade na aplicação de algumas normas. Esta flexibilização reflete a intenção de adaptar as regras de proteção de dados às circunstâncias específicas e de interesse público da investigação científica, mas tem como consequência um maior peso e relevância do *princípio da responsabilidade*.

O *princípio da responsabilidade*⁴ reflete a ênfase na auto-regulação, atribuindo ao responsável pelo tratamento o dever de assegurar e poder comprovar o cumprimento dos princípios da proteção de dados, avaliar os riscos para os direitos e liberdades dos titulares de dados e implementar garantias técnicas e organizativas adequadas a essa proteção. Quanto maior o risco para os titulares de dados, maior deve ser o nível de proteção, as obrigações e as garantias a serem implementadas.

Em Portugal, as derrogações sugeridas pelo artigo 89º do RGPD são reguladas pela Lei de Execução do RGPD. O RGPD e a Lei de Execução são ambos referências indispensáveis para a consulta e familiarização dos investigadores com a legislação em vigor.

Outros quadros regulamentares mais específicos podem aplicar-se em alguns projetos de investigação, tais como o tratamento de dados pessoais relacionados com condenações penais e infrações, o tratamento de informação genética, a proteção de dados pessoais no sector das comunicações eletrónicas, a videovigilância, entre outros. Uma compilação da legislação pode ser consultada no sítio web da Comissão Nacional de Proteção de Dados (CNPD).

B. ESTOU A USAR DADOS PESSOAIS?

B.1 O conceito de dados pessoais

O RGPD e a Lei de Execução aplicam-se a qualquer projeto de investigação que faça uso de dados pessoais.

Por *dados pessoais* entende-se qualquer informação, de qualquer natureza e em qualquer suporte (e.g. registo de voz ou imagem), relativa a uma pessoa singular identificada ou identificável (designada o 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

³ Lei nº 58/2019, de 8 de agosto, publicada no D.R. nº 151/2019, I Série, de 08/08/2019.

⁴ RGPD, art. 5º, nº2.

eletrónica (e.g. IP), ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Por *tratamento de dados pessoais* entende-se qualquer operação efetuada sobre dados pessoais, incluindo desde logo a recolha, ou o registo, a organização, a conservação, a alteração, a consulta, a divulgação ou disponibilização, a comparação ou interconexão, o apagamento ou a destruição etc.

O facto de um estudo não reportar respostas individuais de participantes não é por si só indicador de não haver tratamento de dados pessoais. Pode considerar-se que um estudo nunca trata dados pessoais apenas na condição de que o investigador não tenha acesso a nenhum suporte com registos de dados pessoais durante a recolha e posterior tratamento. Sempre que o investigador tenha acesso a dados que contenham informação relativa a uma pessoa identificada ou que possa ser identificada direta ou indiretamente por referência a identificadores, esses dados devem ser tratados como informação pessoal até ao momento da sua anonimização ou destruição.

O processo de anonimização converte dados pessoais em anónimos (ver secção C). Se a anonimização ocorrer numa fase posterior à recolha de dados, por exemplo, quando são removidas informações de identificação pessoal de uma transcrição áudio de uma entrevista, ou quando os dados pessoais recolhidos são transferidos para outra base de dados, os dados brutos ainda são pessoais e todos os dados do estudo devem ser tratados como pessoais até ao ponto em que os dados brutos são apagados ou também anonimizados.

B.2 Categorias especiais de dados pessoais

O RGPD reconhece existirem categorias de dados pessoais que são sensíveis, na medida em que o seu tratamento é suscetível de maiores riscos para os titulares de dados. O regulamento identifica como *categorias especiais de dados pessoais* aqueles 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 uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.⁵

O tratamento de categorias especiais de dados não é proibido se houver consentimento *explícito*⁶ do titular de dados.

Não é também proibido para fins de investigação científica ou histórica, com base em legislação europeia ou portuguesa que preveja medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados, e desde que o tratamento de dados cumpra as garantias enunciadas no nº1 do artigo 89º do RGPD, referentes ao tratamento para investigação científica.⁷

⁵ RGPD, art. 9º.

⁶ O requisito explícito é descrito na secção G.1.

⁷ RGPD, art. 9º, nº2, j).

B.3 Dados de natureza altamente pessoal

Embora não categorizados como especiais, alguns dados pessoais são considerados com uma *natureza altamente pessoal*⁸, cujo tratamento é suscetível de maiores riscos para os titulares de dados. Tratam-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 para a prática do crime de fraude).

B.4 Registo de imagem, voz ou vídeo

O retrato físico de uma pessoa (fotografia ou outro) e o registo de voz ou vídeo são dados pessoais e estão sujeitos enquanto tal às regras de proteção de dados.⁹

Note-se que a mera assunção a partir de um retrato físico de características possivelmente categorizáveis como dados especiais (e.g. a etnia a partir da cor), não implica estar-se perante tratamento de categorias especiais de dados. Contudo, se houver tratamento de informação com base em tais assunções, tal pode ser considerado como tratamento de categorias especiais de dados. Por exemplo, o tratamento de fotografias por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular, corresponde a tratamento de dados biométricos e, por conseguinte, ao tratamento de categorias especiais de dados.

C. ANONIMIZAÇÃO OU PSEUDONIMIZAÇÃO?

C.1 Anonimização

Uma maneira de atenuar as preocupações éticas e riscos jurídicos do uso de dados pessoais é anonimizá-los por forma a que não se relacionem com pessoas identificáveis.¹⁰ Sempre que os fins do tratamento de dados em investigação científica ou história possam ser atingidos com conjuntos de dados que não permitam, ou já não permitam, a identificação dos titulares de dados, os fins devem ser atingidos desse modo. Por *anonimização* entendem-se as técnicas de conversão de dados pessoais em dados anónimos, tais como a supressão de atributos, a codificação, a generalização ou introdução de ruído.

Os dados que não se relacionam com pessoas identificáveis, como dados agregados e estatísticos, ou dados que de outra forma foram anonimizados, não são, em princípio, dados pessoais e estão fora do âmbito do RGPD. Porém, tal só é válido quando o investigador tem acesso apenas aos

⁸ Grupo de trabalho do artigo 29.º para a proteção de dados: 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, 2017, *in* https://www.cnpd.pt/home/rgpd/docs/wp248rev.01_pt.pdf.

⁹ O retrato de uma pessoa é ainda protegido pelo direito à imagem, não podendo ser exposto sem o consentimento dos visados. Contudo, nesse contexto, não é necessário o consentimento da pessoa retratada quando, entre outras situações, assim o justifiquem a sua notoriedade, o cargo que desempenhe, finalidades científicas, quando a reprodução da imagem vier enquadrada na de lugares públicos, ou na de factos de interesse público ou que hajam decorrido publicamente, de acordo com o artigo 79º do Código Civil.

¹⁰ RGPD, art. 89º.

dados anonimizados, e/ou se o processo de recolha garantir desde logo a anonimização. Se o investigador recolher dados pessoais e posteriormente criar um conjunto de dados anonimizados a partir dos primeiros, os novos dados poderão ser considerados ainda dados pessoais, na medida em que o investigador tiver acesso aos dados brutos iniciais. Assim, por exemplo, a criação de um conjunto de dados fruto de informação recolhida junto de participantes através de entrevistas, ainda que posteriormente subtraída de informações de identificação pessoal, pode não traduzir-se em anonimização, até que os dados brutos sejam destruídos ou também anonimizados.

Interessa notar que a anonimização é uma área desafiadora dado o potencial de *re-identificação*. Por re-identificação entende-se o processo de transformar dados anonimizados novamente em dados pessoais por meio de correspondência de dados ou técnicas semelhantes. Um crescente número de estudos mostra ser possível identificar indivíduos a partir de conjuntos de dados anónimos, por exemplo através de técnicas de correspondência em big data, revelando limitações das técnicas de anonimização em proteger a privacidade dos indivíduos. É difícil avaliar o risco de re-identificação com absoluta certeza. Em caso de dúvida, ou se houver uma perspetiva significativa de re-identificação dos indivíduos cujos dados foram recolhidos, o investigador deve tratar os dados como pessoais.

O grupo de trabalho para o Artigo 29 para a proteção de dados, designado pelo Parlamento e pelo Conselho Europeu, disponibiliza um conjunto de boas práticas, técnicas, riscos e erros frequentes na aplicação de técnicas de anonimização.¹¹

C.2 Pseudonimização

A anonimização é sempre preferível à pseudonimização. Porém, há projetos onde é necessário manter um vínculo entre os sujeitos da investigação e os seus dados pessoais. Nesse caso, o tratamento de dados para fins de investigação deve ser sujeito a garantias para proteger a privacidade dos sujeitos e minimizar riscos de acessos acidentais ou não autorizados, incluindo a adoção de medidas técnicas e organizativas, tais como a pseudonimização.

A anonimização e a pseudonimização não são a mesma coisa. O RGPD define pseudonimização como 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.¹² Ou seja, a pseudonimização não remove o carácter pessoal dos dados: diminui o vínculo de um conjunto de dados com as informações originais que identificam os titulares de dados. Por exemplo, criando uma cópia do conjunto de dados, mas onde as informações de identificação pessoal (e.g. o nome de um indivíduo) foram substituídas por identificadores codificados, e prosseguindo o tratamento no novo conjunto de dados que, por si só e sem a chave de decodificação, não permite a identificação dos titulares de dados.

¹¹ Article 29 data protection working party, Opinion 05/2014 on Anonymisation Techniques, http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

¹² RGPD, art. 4º, nº5.

O grupo de trabalho para o Artigo 29 para a proteção de dados, designado pelos Parlamento e Conselho Europeus, disponibiliza um documento acima citado com um conjunto de boas práticas, técnicas, riscos e erros frequentes na aplicação de técnicas de pseudonimização.¹³

D. PAPEIS E RESPONSABILIDADES

D.1 Responsável pelo tratamento¹⁴

O termo *Responsável pelo Tratamento* denomina a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais.

O Iscte é o responsável pelo tratamento nos projetos de investigação sediados no Iscte, independentemente do tratamento de dados decorrer ou não fora do território português ou do Espaço Económico Europeu, quer o tratamento seja ou não feito por terceiros, dentro ou fora de instalações do Iscte e em equipamentos pertencentes ou não pertencentes ao Iscte.

O Iscte é igualmente o responsável pelo tratamento de qualquer trabalho que trate dados pessoais no âmbito dos cursos que ministra, tais como as dissertações de mestrado ou teses de doutoramento.

O princípio da responsabilidade consagrado no RGPD exige que o Iscte, como responsável pelo tratamento, documente a conformidade dos meios de tratamento de dados pessoais concretamente utilizados com os princípios e regras constantes do RGPD, e têm o dever de comprová-la.

D.2A quem incumbe a obrigação de assegurar a conformidade de projetos de investigação científica com o RGPD?

No caso de projetos de investigação, incumbe ao coordenador do projeto no Iscte assegurar a execução do projeto de acordo com a legislação e as orientações em vigor no Iscte sobre proteção de dados pessoais.

D.3A quem incumbe a obrigação de assegurar a conformidade dos trabalhos de teses e dissertações com o RGPD?

No caso de orientação de trabalhos académicos, tais como trabalhos em unidades curriculares, dissertações de mestrado ou teses de doutoramento, incumbe ao(s) orientador(es), com a colaboração do estudante, assegurarem a execução dos trabalhos de acordo com a legislação e as orientações em vigor no Iscte sobre proteção de dados pessoais.

D.4 Responsabilidade conjunta pelo tratamento

Quando outras pessoas singulares ou coletivas determinam, em conjunto com o Iscte, as finalidades e os meios de tratamento, ambos são *responsáveis conjuntos pelo tratamento*.¹⁵

Assim, se o Iscte e alguma outra instituição são parceiros num projeto de investigação, é possível que ambos sejam responsáveis conjuntos pelo tratamento. Nessa situação, deve ser realizado um

¹³ Article 29 data protection working party, Opinion 05/2014 on Anonymisation Techniques, http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

¹⁴ Em inglês o responsável pelo tratamento designa-se *data controller*.

¹⁵ RGPD, art. 26º.

acordo entre as partes, que determina de modo transparente as respetivas responsabilidades no projeto pela conformidade do tratamento de dados com a legislação. Para esse efeito, sugere-se que os responsáveis do projeto contactem o Gabinete de Apoio à Investigação (GAI).

D.5 Subcontratantes do Iscte

O termo *subcontratante*¹⁶ denomina a pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta de um responsável pelo tratamento.

A relação entre o responsável pelo tratamento e um subcontratante é obrigatoriamente regulada por contrato. Assim, quando num projeto de investigação do Iscte são transferidos dados pessoais para um terceiro para a realização de um serviço ou trabalho por subcontratação, a transferência deve ser regulada por um contrato, que vincula o subcontratante ao Iscte e estabelece as condições de tratamento.¹⁷ Para esse efeito, sugere-se que os responsáveis do projeto contactem o Gabinete de Apoio à Investigação.

Note-se que a transferência de dados pessoais para um terceiro, por exemplo, para um projeto de investigação de outra instituição, nem sempre implica uma relação de subcontratação. É possível que um responsável pelo tratamento transfira, em determinadas circunstâncias, dados para outra entidade, sem que incumba a esta última tratar os dados por conta do primeiro. Por exemplo, no âmbito de *utilização secundária* de dados para fins de investigação científica é possível transferir dados entre projetos de investigação, desde que asseguradas garantias adequadas (ver secção L - Uso de dados pessoais de outras fontes).

D.6 O Iscte como subcontratante

Nos casos em que o Iscte trata dados pessoais por conta de um terceiro, este último age como responsável pelo tratamento e o Iscte como subcontratante. Ao Iscte não cabe determinar a finalidade e os meios de tratamento, mas as obrigações de proteção de dados decorrentes do RGPD e da Lei de Execução continuam a verificar-se, tais como a utilização de medidas técnicas e organizativas que garantam os requisitos da legislação e assegurem a defesa dos direitos dos titulares de dados.

E. MEDIDAS TÉCNICAS E ORGANIZATIVAS

O *princípio da integridade e confidencialidade* implica que os responsáveis pelo tratamento garantam que os dados são tratados com segurança, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas.¹⁸ As medidas a implementar devem garantir um nível de segurança adequado aos riscos identificados.

No âmbito de investigação científica desenvolvida no Iscte devem incluir-se, pelo menos, entre outras, as seguintes.¹⁹

¹⁶ Em inglês o subcontratante designa-se *data processor*.

¹⁷ RGPD, art. 28º.

¹⁸ RGPD, art. 5º, nº1, alínea f).

¹⁹ Uma checklist de medidas pode ser consultada no documento da Comissão Europeia "Ethics and Data Protection", 2018, https://ec.europa.eu/info/sites/info/files/5_h2020_ethics_and_data_protection_0.pdf.

E.1 Medidas de carácter geral

- a) Minimizar os dados: O *princípio da minimização* implica que os dados devem ser adequados, pertinentes e limitados ao que é necessário, relativamente às finalidades para as quais são tratados.²⁰ Deve usar-se o mínimo de dados pessoais necessários para a finalidade do tratamento, não tratando, nessa medida, mais dados do que o necessário.
- b) Usar apenas dados anonimizados, se for possível atingir os objetivos do projeto dessa forma.
- c) Usar dados pessoais pseudonimizados, sempre que possível, quando não for possível usar dados anonimizados.
- d) Encriptar os dados pessoais nos dispositivos onde estão armazenados e garantir a proteção das chaves adequadamente. Esta é uma medida obrigatória de carácter geral, e crucial no caso de categorias especiais de dados ou qualquer tipo de dados pessoais conservados em computadores portáteis ou dispositivos amovíveis (e.g. *pens*, discos externos, etc.).
- e) Assegurar que trabalha numa sessão de acesso ao sistema devidamente protegida e autenticada com as credenciais pessoais, e não revelar senhas de acesso pessoal ao sistema a ninguém. Não se ausentar da sessão ou posto de trabalho sem encerrar a sessão, evitando possibilidade de acessos indevidos por terceiros.
- f) Assegurar-se que os computadores com dados pessoais têm todas as atualizações de segurança, que se encontram protegidos contra softwares nocivos (tais como vírus ou outro software malicioso), que as barreiras de segurança (firewalls) estão ativas e que os programas de navegação são executados com configurações seguras.
- g) Não armazenar dados pessoais em serviços de armazenamento em nuvem, salvo aqueles com empresas que tenham acordo contratualizado com o Iscte. Caso o investigador opte por usar o armazenamento em nuvem sem contrato com o Iscte, os dados pessoais aí tratados devem estar cifrados, usando métodos de cifra robustos, recorrendo a criptografia simétrica e/ou assimétrica.
- h) Não replicar ficheiros de dados pessoais em diversos dispositivos (*pens*, portáteis, PCs), salvo na medida do estritamente necessário e do tempo estritamente necessário e/ou exclusivamente para garantir cópias de segurança.
- i) Quando se apagam dados pessoais, assegurar-se que esvazia a reciclagem ou pasta equivalente após apagá-los, e assegurar que todas cópias são apagadas em todos os dispositivos.
- j) Evitar conservar dados em computadores não institucionais.²¹ Quando tal não é possível, i.e. quando o investigador armazena dados em computador próprio, certificar-se que os dados pessoais que têm o Iscte como responsável pelo tratamento são tratados com software licenciado para uso no Iscte e que, quando não é o caso, cabe ao investigador a responsabilidade de verificar a conformidade do software com os princípios de proteção de dados.
- k) Não enviar ficheiros de dados pessoais por correio eletrónico desprotegido, usando ao invés um método de partilha protegida. Note que o envio de correspondência e ficheiros por correio eletrónico cria cópias nos servidores e nos aplicativos de correio eletrónico do remetente e do destinatário.

²⁰ RGPD, art. 5º, nº1, alínea c).

²¹ Computadores institucionais são aqueles que são adquiridos pelo Iscte com verbas próprias. Os computadores não institucionais são aqueles adquiridos pelo próprio utilizador, ainda que possam também ser usados como computador de trabalho.

- l) Usar ou implementar políticas e protocolos de segurança de informação adequados. Em particular, não se deve: enviar conjuntos de dados pessoais por correio eletrónico; recolher dados pessoais ou comunicar com titulares de dados através de plataformas (e.g. redes sociais) sem averiguar as implicações no domínio da proteção de dados; expor dados pessoais a acessos não autorizados, tais como aceder-lhes remotamente através de redes sem fios em aberto, etc.
- m) Garantir que os membros da equipa de projeto com acesso aos dados pessoais estão sujeitos a obrigações de confidencialidade e responsabilidade, atestado por meio de documento escrito (cláusulas no contrato de trabalho ou, no caso de estudantes, termo de confidencialidade e responsabilidade).

E.2 Medidas adicionais para tratamentos suscetíveis de maior risco (e.g. categorias especiais de dados)

- n) Se o tratamento de dados pessoais envolve pelo menos um dos critérios suscetíveis de elevar o risco de tratamento, citados na secção O.1²², como por exemplo o tratamento de categorias especiais de dados, as seguintes medidas adicionais devem ser cumpridas:
- Os dados brutos, não pseudonimizados, não devem ser armazenados em computadores pessoais. Se necessário, a recolha de dados pode dar-se com o auxílio de computadores pessoais, e logo que possível apagada no computador pessoal e transferida para servidores ou serviços institucionais do Iscte ou computadores institucionais desligados da rede, onde devem permanecer com acesso restrito.
 - Sempre que possível, implementar regras de acesso e registos de acesso (logs) aos dados.

F. FINALIDADE DO TRATAMENTO, PRINCÍPIOS E DIREITO DO PARTICIPANTE A SER INFORMADO

F.1 Finalidade do tratamento, limitação das finalidades, licitude e transparência

O tratamento de dados pessoais é sempre realizado para uma ou mais finalidades e está sujeito a determinados princípios²³, incluindo os *princípios da licitude*, da *lealdade*, da *transparência* e da *limitação das finalidades*.

Por *finalidade do tratamento*, entende-se os fins para os quais os dados pessoais podem ser utilizados. O *princípio da limitação das finalidades* implica que os dados são recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades. A investigação científica tem, contudo, um estatuto diferenciado, não sendo incompatível o tratamento posterior para fins de investigação (uso secundário de dados), desde que asseguradas medidas adequadas (ver secção L - Uso de dados pessoais de outras fontes).

²² Designadamente os critérios citados no documento do Grupo de trabalho do artigo 29.º para a proteção de dados: 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, https://www.cnpd.pt/home/rgpd/docs/wp248rev.01_pt.pdf.

²³ RGPD, art. 5º.

Para ser *licito* o tratamento tem de ser realizado com base em um ou mais *fundamentos legais* do artigo 6º do RGPD e/ou, no caso de tratamento das categorias especiais de dados com base num dos fundamentos previstos no nº 2 do artigo 9º.

Os *princípios da lealdade e transparência* requerem aos investigadores a obrigação de facultar aos participantes na investigação informações sobre a finalidade do tratamento de dados, o fundamento legal para o tratamento, o que acontece aos dados e quais os riscos envolvidos. A informação deve ser fornecida de forma inteligível, numa linguagem clara e simples.

F.2 Ficha de Informação ao Participante (FIP)

Uma forma de facultar a informação aos participantes na investigação pode ser através de uma [Ficha de Informação ao Participante \(FIP\)](#) ou, quando o fundamento jurídico para o tratamento de dados é o consentimento do titular de dados, integrando essas informações num consentimento informado.

Quando os dados pessoais são recolhidos junto do titular dos dados, a informação a facultar deve incluir obrigatoriamente:²⁴

- A informação de que o Iscte é o responsável pelo tratamento de dados pessoais (identificar outros responsáveis pelo tratamento caso haja responsabilidade conjunta);
- O nome do investigador ou responsável no Iscte pelo estudo;
- A finalidade do tratamento;
- O fundamento legal para o tratamento (e.g. consentimento do titular de dados, exercício de funções de interesse público, interesses legítimos ou outra base legal dos arts. 6º ou 9º do RGPD);
- Os direitos que o participante titular de dados pode exercer e a forma e contactos do investigador ou responsável pela investigação a quem o dirigir; e ainda o direito de apresentar reclamação à CNPD;
- Se o fundamento legal for baseado no consentimento dos titulares de dados, a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
- O prazo de conservação dos dados pessoais, após o qual são destruídos ou anonimizados;
- Informações se os dados são transferidos para terceiros e para que fins, por exemplo, para subcontratantes (pessoas ou entidades que tratam os dados pessoais por conta do Iscte), outras equipas de investigação ou quaisquer outras entidades autorizadas a tratar os dados pessoais;
- Caso haja transferências para um país terceiro ou organização internacional fora do Espaço Económico Europeu, a existência ou não de uma «decisão de adequação»²⁵ adotada pela Comissão Europeia e demais informações sobre as transferências e identificação das organizações, de acordo com o art.13º, nº1, alínea f) do RGPD;
- Caso o tratamento de dados envolva potencial risco para os direitos e liberdades dos participantes, a importância e as consequências previstas de tal tratamento para os participantes;

²⁴ RGPD, arts. 13º e 14º.

²⁵ Ver secção M - Transferências para países fora do Espaço Económico Europeu e recolha fora do EEE.

- Caso existam decisões automatizadas²⁶, incluindo a definição de perfis referida no art. 22º, nº1 e nº4 do RGPD, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o participante;
- Os contactos do Encarregado de Proteção de Dados do Iscte.

A informação pode ainda incluir uma descrição das garantias adotadas, incluindo as medidas técnicas e organizativas adotadas pelo investigador, tais como:

- Se os dados pessoais são pseudonimizados ou anonimizados em alguma fase da investigação;
- A informação de que todos os investigadores pertencentes ao projeto estão obrigados ao dever de sigilo e confidencialidade.

Se no decorrer do projeto as condições de tratamento se alteram, é necessário informar os participantes.

G. TRATAMENTO COM FUNDAMENTO LEGAL EM CONSENTIMENTO DOS TITULARES DE DADOS

G.1 Manifestação de vontade, livre, específica, informada e inequívoca ou explícita

Numa boa parte dos casos, para fins de investigação científica, o fundamento legal para o tratamento de dados pessoais é o consentimento.

O [consentimento dos titulares de dados](#) é dado com base na FIP, e refere-se à manifestação de vontade pelo qual os participantes titulares de dados aceitam que os dados pessoais que lhe dizem respeito no projeto de investigação sejam objeto de tratamento.²⁷ Deve assumir a forma de declaração escrita, e pode ser recolhida por meios eletrónicos, por exemplo:

- (1) Consinto em que os meus dados pessoais sejam utilizados no âmbito do projeto de investigação [*identificar qual o projeto de investigação*] de acordo com a finalidade e demais informações que me foram disponibilizadas na Ficha de Informação ao Participante.
Sim Não

Somente após a disponibilização da FIP aos participantes e a manifestação positiva de consentimento podem os dados ser tratados (incluindo a recolha). A manifestação de vontade tem de ser *livre, específica, informada e inequívoca*. Em certos casos, deve ser não apenas inequívoca, mas explícita:

²⁶ Decisões individuais 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. Por exemplo, se a decisão de um banco em conceder um empréstimo bancário a uma pessoa singular for exclusivamente tomada por um algoritmo, sem intervenção humana. 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.

²⁷ RGPD, art. 6º, nº1, alínea a); art. 7º; e art. 9º, nº2, alínea a). Vide ainda orientações relativas ao consentimento na aceção do Regulamento (eu) 2016/679, Grupo de trabalho do artigo 29.º para a proteção de dados, https://www.cnpd.pt/home/rgpd/docs/wp259rev0.1_PT.pdf.

i) o requisito *livre* significa que existe uma verdadeira escolha e controlo para os titulares dos dados. Se o participante não puder exercer uma verdadeira escolha, se houver uma relação de desequilíbrio com o responsável de tratamento (e.g. uma relação entre empregado e empregador, entre docente e estudante), se o participante se sentir coagido a dar o consentimento, ou sofrer consequências negativas caso não consinta, então o consentimento não é válido.

ii) o requisito *inequívoco* significa que o consentimento é realizado mediante declaração ou ato positivo inequívoco, pelo qual o participante aceita que os dados que lhes dizem respeito sejam objeto de tratamento. O silêncio, opções pré-validadas ou omissões não são métodos aceites no consentimento.

iii) O requisito *explícito* reforça o carácter inequívoco do consentimento. É obrigatório no caso do tratamento de categorias especiais de dados, bem como no caso de transferências internacionais para países sem «decisão de adequação» e que não pertençam ao Espaço Económico Europeu.²⁸ Para ser explícito, o titular dos dados tem que manifestar *expressamente* o consentimento, por exemplo através de declaração escrita e da assinatura do titular dos dados ou, no contexto digital, através do preenchimento de um formulário eletrónico, seguido de envio de mensagem de correio eletrónico para carregamento de documento digitalizado com a assinatura do titular dos dados ou assinatura eletrónica.²⁹

iv) o requisito *específico* implica que o consentimento do titular dos dados deve ser dado em relação a uma ou mais finalidades específicas e que um titular de dados tem uma escolha em relação a cada uma delas. Um consentimento pode abranger operações diferentes, desde que essas operações sirvam a mesma finalidade. Os titulares dos dados darão o seu consentimento sabendo que detêm controlo sobre os seus dados e que esses dados apenas serão tratados para as finalidades especificadas. Se o responsável tratar os dados com base no consentimento e pretender tratar os dados também para outra finalidade, deve procurar obter outro consentimento para a nova finalidade exceto se existir outro fundamento legal para esse tratamento que reflita melhor a situação.

Nem sempre é possível cumprir os requisitos de consentimento do titular de dados. Por exemplo, se os titulares de dados são estudantes no Iscte o consentimento *livre* pode ser questionado. Caso haja dificuldade em cumprir os requisitos, sugere-se que o investigador avalie a possibilidade de invocar em alternativa o fundamento legal do exercício de funções públicas ou a prossecução de interesses legítimos. Tal não impede, porém, de obter, no plano ético, um *consentimento informado de participantes na investigação*. As diferenças entre este consentimento e o consentimento do titular de dados no plano legal da proteção de dados são explicadas abaixo.

G.2 E quando a finalidade do tratamento não for inteiramente conhecida?

Em alguns projetos de investigação, pode não ser possível identificar completamente a finalidade do tratamento no momento da recolha. Nesses casos, o consentimento do titular de dados pode ser elaborado para uma finalidade mais abrangente, para diversas áreas de investigação ou ser

²⁸ Sobre o significado de *decisões de adequação* consultar a secção M-Transferências para países fora do Espaço Económico Europeu e recolha fora do EEE.

²⁹ A secção 4 das Orientações do GT29 relativas ao consentimento na aceção do Regulamento (UE) 2016/679, de 28 de Novembro de 2018, fornece vários exemplos de consentimento explícito.

dado unicamente para determinados domínios ou projetos de investigação específicos.³⁰ Esta possibilidade deve ser usada com moderação, devendo ser respeitados os padrões éticos reconhecidos pela comunidade científica.

A menor especificidade da finalidade pode ser compensada pelo fornecimento regular aos participantes de informações sobre a evolução da finalidade, à medida que o projeto de investigação avança, para que, com o tempo, o consentimento possa ser mais específico. Os participantes devem conseguir compreender em termos básicos a situação do projeto, e avaliar se pretendem ou não exercer, por exemplo, o direito de retirada do consentimento nos termos do art. 7.º, n.º3 do RGPD.³¹

G.3 Consentimento dos titulares de dados vs. consentimento de participantes humanos na investigação

O *consentimento dos titulares de dados* pessoais deve ser distinguido do uso do *consentimento informado* de participantes humanos na investigação, tal como, por exemplo, o consentimento prestado nos termos do Código de Ética na Investigação do Iscte.

O primeiro refere-se ao consentimento para tratamento de dados pessoais no plano da proteção de dados pessoais consagrada no RGPD e da Lei de Execução, o último ao consentimento do sujeito de investigação para participar no projeto, nos planos da ética e das boas práticas na investigação científica, consagrado no Código de Ética na Investigação do Iscte.

Assim, um projeto que não trate dados pessoais (e.g. recolhe dados anónimos junto de participantes, através de meios digitais que garantem o anonimato) não carece da FIP nos termos atrás enunciados nem do consentimento dos titulares de dados, mas pode não dispensar no plano ético a disponibilização de informação ou algum tipo de consentimento elaborados nos termos do Código de Ética de Investigação do Iscte. Este último não se referirá ao tratamento de dados pessoais, mas apenas à participação no projeto e/ou a outras eventuais circunstâncias do projeto no plano ético.

Quando um projeto trata dados pessoais com fundamento legal distinto do consentimento dos titulares de dados, continua a ser obrigatório, no plano legal, facultar a FIP. Como garantia adicional para os direitos e liberdades do titular de dados, aconselha-se, no plano ético, um consentimento informado dos participantes nos termos do Código de Ética na Investigação do Iscte. Este último não deve ser explícito relativamente ao tratamento de dados pessoais, mas apenas à participação no projeto e/ou a outras eventuais circunstâncias do projeto no plano ético.

Finalmente, um projeto que trate dados pessoais e que opta pelo fundamento legal do consentimento dos titulares de dados, não está dispensado, no plano ético, de requisitos adicionais de informação ao participante e da obtenção de consentimento nos termos do Código de Ética na Investigação do Iscte. Neste caso, o investigador pode optar por fundir os dois consentimentos num só, que deve ser explícito relativamente ao tratamento de dados pessoais.

³⁰ Lei de Execução do RGPD, art. 31º, nº4.

³¹ Vide as orientações do grupo de trabalho do artigo 29.º para a proteção de dados relativas ao consentimento, na secção 7.2 referente à investigação científica, pp. 33, https://www.cnpd.pt/home/rgpd/docs/wp259rev0.1_PT.pdf.

A relação entre os dois consentimentos pode ser resumida da seguinte forma:

1. Projeto que não trata dados pessoais (e.g. recolhe dados anónimos junto de participantes, através de meios digitais que garantem o anonimato):

Plano legal da proteção de dados: não carece da FIP nem de consentimento dos titulares de dados.

Plano ético: Pode requerer disponibilização de informação ou algum tipo de consentimento informado nos termos do Código de Ética de Investigação do Iscte.

2. Projeto que trata dados pessoais com fundamento legal distinto do consentimento dos titulares de dados, e.g. interesses legítimos:

Plano legal da proteção de dados: obrigatória a FIP; não é obrigatório nem deve ser usado um consentimento dos titulares de dados.

Plano ético: Pode sugerir, como garantia adicional, ou requerer em função das circunstâncias específicas do projeto, a aplicação de consentimento informado nos termos do Código de Ética de Investigação do Iscte. Este não deve referir-se ao tratamento de dados pessoais, mas apenas dizer respeito à participação no projeto e/ou a outras circunstâncias do projeto no plano ético.

3. Projeto que trata dados pessoais com base em fundamento legal de consentimento dos titulares de dados:

Plano legal da proteção de dados: obrigatória a FIP e consentimento do titular de dados.

Plano legal e ético: não está dispensado, no plano ético, de eventuais requisitos adicionais de informação ao participante e da obtenção de consentimento nos termos do Código de Ética na Investigação do Iscte. Neste caso, o investigador pode optar por fundir os dois consentimentos num só, que deve ser explícito relativamente ao tratamento de dados pessoais.

H. TRATAMENTO COM FUNDAMENTO LEGAL BASEADO EM FUNÇÕES DE INTERESSE PÚBLICO OU PROSECUÇÃO DE INTERESSES LEGÍTIMOS

H.1 Exercício de funções de interesse público

O *exercício de funções de interesse público* pode constituir fundamento legal para o tratamento de dados. Este fundamento pode ter vantagens em relação ao consentimento dos titulares de dados, como por exemplo, no caso de se verificar que o consentimento não poderia cumprir o requisito de ser *livre*. Contudo, tal só possível com base no direito nacional ou da UE, e requer evidências de que os fins da investigação são do interesse público.³² O caso de projetos revistos por painéis e financiados por agências públicas pode ser um indicador do seu interesse público.

H.2 Prosecação de interesses legítimos

Nos casos em que a investigação é necessária para efeito dos *interesses legítimos* prosseguidos pelo Iscte ou por terceiros, o fundamento legal de interesses legítimos pode ser invocado, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável

³² RGPD, art. 6º, alínea e). Vide ainda A Preliminary Opinion on data protection and scientific research, European Data Protection Supervisor, January 2020. <https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific-en>.

pelo tratamento, e desde que os interesses e direitos e liberdades dos titulares de dados não devam prevalecer sobre os interesses do responsável pelo tratamento. A existência de interesse legítimo requer uma avaliação cuidada da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade.

Por outras palavras, a base legal do interesse legítimo permite o tratamento sob reserva da aplicação de um teste de ponderação, que pondere os interesses legítimos do responsável pelo tratamento – ou de terceiros a quem os dados sejam comunicados – em relação aos interesses e aos direitos e liberdades das pessoas em causa.

Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o Iscte como responsável pelo tratamento como, por exemplo, a relação com um aluno, um docente ou um funcionário. O tratamento de dados de alunos do Iscte para investigar formas de melhorar processos pedagógicos na instituição, desde que autorizado superiormente, pode ser candidato a um interesse legítimo da instituição. O tratamento de dados estritamente necessário aos objetivos de prevenção e controlo da fraude constitui um interesse legítimo reconhecido pelo RGPD.³³

H.3 Que informações devem ser providenciadas ao participante?

Note-se que em ambos os fundamentos legais, o exercício de funções de interesse público e a prossecução de interesses legítimos:

1. O dever de informação ao participante mantém-se, por exemplo, através da disponibilização da FIP, onde consta o fundamento legal para o tratamento de dados e demais informações referidas na secção F.2 - Ficha de Informação ao Participante (FIP).
2. Como garantias adicionais para os direitos e liberdades do titular de dados, é recomendado, sempre que possível, obter um consentimento informado de participação de humanos na investigação, e.g. nos termos do Código de Ética na Investigação do Iscte. Este refere-se ao consentimento de participação no projeto e não ao tratamento de dados pessoais, uma vez que o fundamento legal para o tratamento de dados será outro.

No caso do investigador entender que a finalidade do projeto se enquadra no exercício de funções de interesse público ou em interesses legítimos, e pode beneficiar da aplicação de um desses fundamentos legais para o tratamento de dados pessoais, sugere-se que o investigador solicite, antes de realizar qualquer tratamento, orientações ao Gabinete de Apoio à Investigação e à Equipa de Proteção de Dados do Iscte.

H.4 Interesse público no âmbito de tratamento de categorias especiais de dados

As categorias especiais de dados podem ainda ser tratadas com base nos seguintes fundamentos jurídicos de interesse público, entre outros: i) ao abrigo de motivos de interesse público no domínio da saúde pública, com base na legislação europeia ou portuguesa que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional³⁴; ii) desde que o tratamento cumpra as medidas do nº1 do art. 89º

³³ RGPD, considerando 47º.

³⁴ RGPD, art. 9º, alínea i).

do RGPD, para fins de investigação científica ou histórica, com base na legislação europeia ou portuguesa, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.³⁵

I. PRAZOS DE CONSERVAÇÃO

De acordo com o princípio da *limitação da conservação*, os dados pessoais devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados.³⁶

Quando cessa a finalidade que motivou o tratamento, o responsável pelo tratamento procede à sua destruição ou anonimização.³⁷

O prazo de conservação é aquele que estiver fixado por norma legal ou regulamentar ou, na falta deste, o que se revele necessário para a prossecução da finalidade.

Contudo, para efeitos de investigação científica ou histórica, caso não seja possível determinar antecipadamente o momento em que os dados pessoais deixam de ser necessários, é lícita a conservação dos dados, desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados, designadamente a informação da sua conservação.³⁸

I.1 Prazos máximos de conservação no Iscte

No Iscte adotam-se os seguintes prazos máximos de conservação para efeitos de investigação científica:

- a) Dissertações de Mestrado - 6 meses após as provas de defesa da dissertação do Mestrado;
- b) Teses de Doutoramento - 12 meses após as provas de defesa da tese do Doutoramento;
- c) Projetos financiados pela FCT - 10 anos após o prazo de conclusão do projeto (execução);
- d) Projetos financiados por outras fontes de financiamento (incluindo europeus) – 10 anos após o prazo de conclusão do projeto.

Sempre que se justifique a necessidade de prorrogação destes prazos, ou a possibilidade de reutilização dos dados pessoais para outras finalidades de investigação científica (uso secundário de dados, vide secção L - Uso de dados pessoais de outras fontes), os prazos podem ser prorrogados. Essa prorrogação necessita de aprovação superior, que deve ser requerida junto do Gabinete de Apoio à Investigação.

³⁵ RGPD, art. 9º, alínea j).

³⁶ RGPD, art. 5º, alínea e).

³⁷ Lei de Execução, art. 21º, nº4.

³⁸ Lei de Execução, art. 21º, nº2.

Aquando da destruição dos dados, e em particular quando são usados provedores de serviços de armazenamento, interessa verificar se os dados foram todos excluídos com segurança, juntamente com eventuais *backups*. Se os dados foram partilhados com terceiros, deve garantir-se que foram igualmente destruídos, salvo se houver base legal para os manter.

J. DIREITOS DOS TITULARES DE DADOS

J.1 Quais os direitos dos titulares de dados e a quem se devem dirigir?

O caráter voluntário de participação num estudo é um requisito ético fundamental da investigação científica. O avanço científico depende em boa parte da disponibilidade, voluntariedade e boa vontade de participantes em submeterem-se a estudos, no pressuposto da contribuição para o avanço científico e o interesse público. Havendo tratamento de dados pessoais num estudo, a resposta atempada a pedidos de exercício de direitos dos titulares de dados é condição fundamental para a proteção dos seus direitos, liberdades e garantias, e é, paralelamente, uma condição fundamental do próprio funcionamento do sistema de investigação científica.

Para o exercício de direitos dos titulares de dados, a FIP deve especificar a forma e contactos do responsável a quem o dirigir.

Além do direito do titular de dados a ser informado, outros direitos incluem o direito de acesso aos dados (art. 15º do RGPD), de retificação (art. 16º), de apagamento (art. 17º), limitação do tratamento (art. 18º) e direito à portabilidade (art. 20º).

Caso o fundamento legal para o tratamento seja a prossecução de interesses legítimos, o titular de dados tem o direito de se opor ao tratamento (art. 21º do RGPD), incluindo a definição de perfis.

O titular de dados tem ainda o direito de se opor sempre que os dados pessoais forem tratados para fins de investigação científica ou histórica, nos termos do art. 89º, nº1, por motivos relacionados com a sua situação particular, salvo se o tratamento for necessário para a prossecução de atribuições de interesse público.³⁹

Caso o fundamento legal para o tratamento seja o consentimento, o titular de dados tem o direito de retirar o seu consentimento a qualquer momento, embora tal não comprometa a licitude do tratamento efetuado com base no consentimento previamente dado.⁴⁰

J.2 É possível não satisfazer pedidos relativamente a direitos dos titulares de dados?

Na medida em que os dados pessoais sejam tratados para fins de investigação científica ou histórica, o RGPD prevê a possibilidade de não aplicação do direito ao apagamento de dados, inclusive após retirada do consentimento, na medida em que esse direito seja suscetível de tornar impossível ou prejudicar gravemente a realização desses fins.⁴¹

³⁹ RGPD, art. 21º, nº6.

⁴⁰ RGPD, art. 4º, nº 3.

⁴¹ RGPD, art. 17º, nº3, alínea d).

A Lei de Execução do RGPD prevê ainda que os direitos de acesso, retificação, limitação do tratamento e de oposição podem ficar prejudicados, na medida do necessário, se esses direitos forem suscetíveis de tornar impossível ou prejudicar gravemente a realização desses fins.⁴²

A não satisfação de pedidos relativos ao exercício de direitos é uma solução de última instância e deve ser abordada com especial cautela. Caso o investigador entenda necessário não satisfazer um pedido de exercício de direitos de titulares de dados, é obrigatório o investigador requerer uma autorização para esse efeito, submetendo junto do Gabinete de Apoio à Investigação o pedido de exercício de direitos com uma explicação fundamentada das razões pelas quais o investigador entende que o mesmo não deve ser atendido, podendo ser ainda necessário juntar o parecer da Comissão de Ética e/ou do Encarregado de Proteção de Dados.

J.3 Prazos para resposta a pedidos de exercício de direitos

O RGPD determina que as informações ao titular de dados sobre as medidas tomadas, mediante pedido apresentado para o exercício de direitos, sejam realizadas sem demora injustificada. Embora os prazos máximos previstos sejam mais alargados⁴³, recomenda-se, em contexto de investigação científica, um prazo máximo de vinte dias corridos, a contar da data da receção do pedido, salvo casos em que a complexidade ou o número de pedidos justifique prazos mais alargados.

K. APLICAÇÃO DE ÍNQUÉRITOS À COMUNIDADE ISCTE PARA EFEITOS DE INVESTIGAÇÃO CIENTÍFICA

A comunidade do Iscte pode representar um universo relevante e útil para aplicação de inquéritos em contexto de investigação científica. A [política de proteção de dados do Iscte](#) prevê a possibilidade de distribuição de inquéritos via listas de correio eletrónico, realizável de acordo com diferentes fundamentos jurídicos. Os critérios para a distribuição de inquéritos à população estudantil são definidos na [política de aplicação de inquéritos à população estudantil](#).

L. USO DE DADOS PESSOAIS DE OUTRAS FONTES

Ainda que sob condições e garantias adequadas, é possível realizar tratamento de dados pessoais não recolhidos diretamente junto dos titulares de dados, tais como dados recolhidos por terceiros, inclusive dados obtidos por empresas ou por outros projetos (uso secundário de dados).

É necessário confirmar que existe permissão do responsável pelo conjunto de dados original e o tratamento deve estar sujeito a garantias adequadas, devendo assegurar-se as medidas técnicas e organizativas do nº1 do art. 89º do RGPD, consonantes com o tratamento para investigação científica, incluindo a pseudonimização.

Fazer uso de um conjunto de dados de terceiros implica uma análise da *compatibilidade* entre a finalidade inicial e a nova finalidade do tratamento.

Se a nova finalidade for compatível, o tratamento não precisa de um novo fundamento legal para o tratamento adicional. A investigação científica tem um estatuto especial, na medida em que o

⁴² Lei de Execução, art. 31º, nº2.

⁴³ RGPD, art. 11º, nº3.

tratamento posterior para fins de investigação científica ou histórica não é considerado incompatível com as finalidades iniciais.⁴⁴ Contudo, caso os dados de outras fontes tenham sido recolhidos com base em consentimento do titular de dados, a re-utilização desses dados não dispensa novo consentimento.

Qualquer que seja o fundamento legal, mantém-se a necessidade de fornecer aos participantes a FIP, permitindo o eventual *opt-out* dos participantes. Na FIP deve ainda acrescentar-se as seguintes informações: a origem e as categorias de dados pessoais recolhidas e, eventualmente, se provêm de fontes acessíveis ao público.⁴⁵

Existem duas exceções a esta última condição:

- 1) Se os participantes já tiverem essas informações.
- 2) Se se comprovar a impossibilidade de disponibilizar a informação aos participantes, ou que o esforço envolvido seja desproporcionado para o tratamento para fins de investigação.⁴⁶ Essa possibilidade é ponderada sob reserva de condições e garantias adequadas⁴⁷, e na medida em que a obrigação de disponibilização de informação seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento.

Ao determinar o que constitui impossibilidade ou esforço desproporcional, o considerando 62 do RGPD refere-se ao número de titulares de dados, à idade dos dados e às garantias adequadas em vigor como possíveis fatores indicativos. Para esse efeito, recomenda-se que o responsável do projeto realize, documente e submeta à Equipa de Proteção de Dados do Iscte uma avaliação do esforço envolvido em fornecer as informações aos titulares de dados *versus* o impacto e os efeitos sobre os mesmos caso não recebam as informações.

Caso o responsável pelo tratamento entenda não ser possível assegurar o direito do titular de dados a ser informado, toma as medidas adequadas para defender os direitos, liberdades e interesses legítimos do titular dos dados, inclusive através da divulgação da informação ao público, por exemplo, através do sítio web do projeto. Cumulativamente, caso o tratamento envolva categorias especiais de dados, dados relacionados com condenações penais e infrações ou dados de natureza altamente pessoal, o Regulamento n.º 1/2018 da CNPD determina ainda que o responsável pelo tratamento realize uma avaliação de impacto na proteção de dados.⁴⁸

M. TRANSFERÊNCIAS PARA PAÍSES FORA DO ESPAÇO ECONÓMICO EUROPEU E RECOLHA FORA DO EEE

O RGPD aplica-se aos responsáveis pelo tratamento estabelecidos no Espaço Económico Europeu, independentemente de o tratamento de dados pessoais ocorrer dentro ou fora do Espaço Económico Europeu (EEE).

⁴⁴ RGPD, art. 5º, alínea b).

⁴⁵ RGPD, art. 14º.

⁴⁶ RGPD, art. 14º, nº5.

⁴⁷ Designadamente, as reservas e garantias previstas no nº1 do artigo 89º do RGPD.

⁴⁸ Regulamento n.º 798/2018, Diário da República n.º 231/2018, Série II de 2018-11-30; Regulamento n.º 1/2018 da CNPD relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados, <https://dre.pt/home/-/dre/117182365/details/maximized>.

O tratamento de dados fora do EEE pode ter riscos acrescidos para os titulares de dados, caso o ordenamento jurídico do país onde é realizado não ofereça um nível de proteção equivalente ao RGPD. Por conseguinte, o RGPD prevê disposições específicas para transferências ou tratamentos de dados pessoais realizados fora do EEE. Caso um projeto do Iscte transfira dados pessoais para fora do EEE, ou recolha e trate dados fora do EEE, a coordenação deve assegurar, e ser capaz de demonstrar, a conformidade dessa transferência com o RGPD.

Analogamente, se um parceiro de um projeto ou subcontratante estabelecido fora do EEE aceder a dados pessoais conservados pelo Iscte, isto equivale a uma transferência para fora do EEE, devendo a coordenação do projeto assegurar e ser capaz de demonstrar que a transferência cumpre o RGPD.

M.1 Transferências para países com «decisão de adequação»

Em certos casos, pode considerar-se que um país terceiro fora do EEE oferece um nível adequado de proteção através de uma decisão da Comissão Europeia («decisão de adequação»), significando que é possível transferir dados para uma instituição situada no país terceiro sem que o exportador dos dados tenha de apresentar garantias suplementares e sem que esteja sujeito a condições adicionais. Por outras palavras, as transferências para um país terceiro «adequado» serão semelhantes a uma transmissão de dados no interior do EEE.⁴⁹ Tal não obsta, contudo, à obrigatoriedade dos titulares de dados serem previamente informados dessa transferência na FIP.

A lista de países com decisões de adequação pode ser consultada nas páginas da Comissão Europeia⁵⁰.

M.2 Transferências para países sem «decisão de adequação»

Na ausência de uma decisão de adequação, o RGPD prevê um número de instrumentos jurídicos para assegurar garantias adequadas, na condição de os titulares de dados gozarem de direitos oponíveis e de medidas corretivas eficazes.⁵¹

Todavia, em contexto de investigação científica, a forma mais expedita e habitual de transferências internacionais para países sem decisão de adequação é por via de consentimento *explícito* do titular de dados, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e de garantias adequadas.⁵² Para ser explícito, o titular dos dados tem que manifestar *expressamente* o consentimento (sobre o requisito explícito do consentimento, ver secção G.1).

Caso um projeto de investigação preveja transferir dados pessoais para países fora do EEE sem decisão de adequação, a coordenação do projeto deve demonstrar a legalidade dessa transferência e requerer a sua aprovação prévia junto do Gabinete de Apoio à Investigação, podendo ser ainda necessário juntar o parecer da Comissão de Ética e/ou do Encarregado de Proteção de Dados.

⁴⁹ Consultar https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pt

⁵⁰ A lista está disponível em https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_pt.

⁵¹ RGPD, art. 46º.

⁵² RGPD, art. 49, nº1, alínea a).

N. ACESSO A ARQUIVOS COM DADOS PESSOAIS DE PESSOAS FALECIDAS

A Lei de Execução do RGPD determina que os dados pessoais de pessoas falecidas são protegidos quando se integrem nas categorias especiais de dados pessoais, ou quando se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações, exceto nas condições previstas do nº2 do art. 9º do RGPD.⁵³

No quadro dessas condições de exceção, é possível aceder a dados pessoais de pessoas falecidas se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, com base em uma ou mais leis portuguesas ou da União Europeia, desde que cumpridas as medidas técnicas e organizativas apontadas no nº1 do art. 89º do RGPD, referentes ao tratamento para investigação científica.⁵⁴

Em Portugal, o Regime Geral dos Arquivos e do Património Arquivístico⁵⁵ prevê o livre acesso a documentos em arquivos públicos que contenham dados pessoais de pessoas singulares nos seguintes prazos:

- 1) Após o decurso de 30 anos sobre a data da morte das pessoas a que respeitam os documentos; ou
- 2) Não sendo conhecida a data da morte, decorridos 40 anos sobre a data da emissão dos documentos, mas não antes de terem decorrido 10 anos sobre o momento do conhecimento da morte.

Após estes prazos é livre o acesso a documentos administrativos que contenham dados pessoais de pessoas falecidas. Já o direito de acesso antes dos prazos referidos, na ausência de alguma lei portuguesa ou europeia que o preveja, é exercido por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respetivos herdeiros.

No caso de arquivos particulares, compete aos proprietários proporem as regras e modalidades de acesso à documentação, homologadas pelo membro do governo que superintende na política arquivística.

O. AVALIAÇÃO DE IMPACTO NA PROTEÇÃO DE DADOS

O.1 Quando é necessário realizar uma avaliação de impacto?

Quando o tratamento for suscetível de implicar *um elevado risco* para os direitos e liberdades das pessoas singulares, pode ser necessário realizar, *antes de iniciar o tratamento*, uma *Avaliação de Impacto na Proteção de Dados Pessoais (AIPD)*.⁵⁶ A AIPD é particularmente importante quando se introduz uma nova tecnologia.⁵⁷ A AIPD visa identificar riscos para os titulares de dados, tendo em vista mitigá-los com garantias adequadas.

⁵³ Lei de Execução, art. 17º.

⁵⁴ Art. 9º, nº2, alínea j) do RGPD. Essa lei deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.

⁵⁵ Decreto-Lei nº16/93, de 23 de Janeiro.

⁵⁶ RGPD, art. 35º.

⁵⁷ RGPD, considerandos 89-91.

O RGPD não define "elevado risco", mas a AIPD é obrigatória nos seguintes casos:⁵⁸

a) Avaliação sistemática e completa de aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos ou afetem significativamente o titular de dados.

Por *definição de perfis* entende-se a avaliação de aspetos pessoais de uma pessoa singular, nomeadamente para prever ou classificar em categorias aspetos relacionados com o desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.⁵⁹ Uma decisão produz *efeitos jurídicos* quando aspetos da sua esfera jurídica são afetados, por exemplo, o direito de voto. O tratamento pode *afetar significativamente* um indivíduo se influenciar as suas circunstâncias, comportamentos ou escolhas. Por exemplo, o tratamento automatizado pode levar à recusa de um pedido de crédito num banco.

b) Operações de tratamento em grande escala de categorias especiais de dados, ou de dados pessoais relacionados com condenações penais e infrações.

O RGPD não define o que constitui "grande escala". Alguns indicadores podem ser o número de titulares de dados envolvidos, o volume de dados e a diversidade de dados diferentes a tratar, a duração da atividade de tratamento de dados ou a sua pertinência, ou a dimensão geográfica da atividade de tratamento.⁶⁰

c) Controlo sistemático de zonas acessíveis ao público em grande escala.

Por controlo sistemático entende-se o tratamento para observar, monitorizar ou controlar os titulares dos dados.

⁵⁸ RGPD, art. 35º, nº3.

⁵⁹ RGPD, art. 4º, nº4.


⁶⁰ Não existe uma definição do que constitui grande escala no RGPD. Os seguintes fatores podem ser considerados na apreciação:

- O número de titulares de dados afetados como número concreto ou em percentagem da população em causa, por exemplo uma percentagem alta dos alunos do Iscte;
- O volume de dados e/ou o alcance dos diferentes elementos de dados objeto de tratamento;
- A duração, ou permanência, da atividade de tratamento de dados;
- O âmbito geográfico da atividade de tratamento.

Contam-se como exemplos de tratamento de grande escala: i) O tratamento de dados de uma tecnologia para uso de indivíduos de uma população e que faz o rastreio de contactos, como o Stayaway Covid; ii) O tratamento de dados de doentes no exercício normal das atividades de um hospital; iii) O tratamento de dados de viagem das pessoas que utilizam o sistema de transportes públicos de uma cidade; iv) O tratamento de dados de clientes no exercício normal das atividades de uma companhia de seguros ou de um banco.

Exemplos que **não** constituem tratamento de grande escala, incluem: i) O tratamento de dados de doentes pacientes por um médico; ii) o tratamento de dados pessoais relacionados com condenações penais e infrações por um advogado.

Ver a secção 3 do documento do GT29: https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf

ISCTE - Instituto Universitário de Lisboa  Av. das Forças Armadas, 1649-026 Lisboa ☎ 351 217 903 000
www.iscte.pt www.facebook.com/ISCTEUL twitter.com/iscteiu www.linkedin.com/company/iscte-iul www.flickr.com/photos/iscteiu/ www.youtube.com/user/iultr

Uma AIPD é igualmente obrigatória quando o tratamento conste na [Lista](#) da CNPD de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados.⁶¹

No caso de nenhuma das condições anteriores se aplicar, a conjugação de dois ou mais dos seguintes critérios pode ser indicadora de elevado risco, e bem assim a necessidade de realizar a AIPD:

1. Avaliação ou classificação, incluindo definição de perfis e previsão.⁶²
2. Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente o titular de dados de modo similar.⁶³
3. Controlo sistemático: tratamento utilizado para observar, monitorizar ou controlar os titulares dos dados, incluindo dados recolhidos através de redes, ou um controlo sistemático de zonas acessíveis ao público.⁶⁴
4. Tratamento de dados sensíveis ou dados de natureza altamente pessoal, incluindo categorias especiais de dados pessoais e dados relacionados com condenações penais e infrações.
5. Tratamento de dados em grande escala⁶⁵.
6. Estabelecer correspondências ou combinar conjuntos de dados: por exemplo, com origem em duas ou mais operações de tratamento de dados realizadas com diferentes finalidades e/ou por

⁶¹ Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados, CNPD, 16 de Outubro de 2018, https://www.cnpd.pt/home/deciso/es/regulamentos/regulamento_1_2018.pdf

⁶² Em especial de «aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados» (considerandos 71 e 91 do RGPD). Os exemplos deste critério podem incluir: Uma plataforma de ensino à distância onde se recolhem, analisam e classificam dados das atividades e comportamentos dos alunos para o docente aplicar pedagogias diferenciadas e melhorar os objetivos de aprendizagem; Uma instituição financeira que faça um controlo seletivo dos seus clientes a partir de uma base de dados de referências de crédito bancário ou a partir de uma base de dados de combate ao branqueamento de capitais e ao financiamento do terrorismo ou de combate à fraude; Uma empresa de biotecnologia que ofereça testes genéticos diretamente aos seus clientes por forma a avaliar e prever riscos de doença ou para a saúde; ou Uma investigação que desenvolva perfis comportamentais ou de comercialização baseados na utilização ou navegação num sítio web.

⁶³ Tratamento destinado à tomada de decisões sobre os titulares dos dados e que produza «efeitos jurídicos relativamente à pessoa singular» ou que «afetem significativamente de forma similar» (art. 35.º, n.º 3, alínea a) do RGPD). Por exemplo, o tratamento pode implicar a exclusão ou a discriminação de indivíduos. O tratamento que produza poucos ou nenhuns efeitos relativamente aos indivíduos não satisfaz estes critérios específicos.

⁶⁴ Tratamento utilizado para observar, monitorizar ou controlar os titulares dos dados, incluindo dados recolhidos através de redes, ou um «controlo sistemático de zonas acessíveis ao público» (art. 35.º, n.º 3, alínea c) do RGPD). Por exemplo, captação de vídeo para o tratamento e investigação dos trajetos usados pelas pessoas em circulação num edifício acessível ao público, e.g numa universidade.

⁶⁵ Sobre grande escala consulte o rodapé **Erro! Marcador não definido..**

diferentes responsáveis pelo tratamento de dados de tal forma que excedam as expectativas razoáveis do titular dos dados.⁶⁶

7. Dados relativos a titulares de dados vulneráveis, sempre que haja acentuado desequilíbrio de poder entre os titulares dos dados e o responsável pelo tratamento dos dados, 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. É o caso, por exemplo, de crianças, empregados, segmentos vulneráveis da população que necessitem de proteção especial, e.g. pessoas com doenças mentais, requerentes de asilo, idosos, doentes, etc.

8. Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais, que podem envolver novas formas de recolha e utilização de dados, possivelmente com elevado risco para os direitos e liberdades dos indivíduos. Por exemplo, combinar a utilização da impressão digital e do reconhecimento facial para melhorar o controlo de acesso físico a um edifício. O uso de big data, técnicas de Inteligência Artificial ou aplicações de Internet das Coisas são candidatos a este critério.

9. Quando o tratamento impede ou prejudica os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato.⁶⁷

A descrição detalhada dos critérios acompanhada de exemplos pode ser consultada nas orientações do grupo do Artigo 29º para a avaliação de impacto na proteção de dados e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do RGPD.⁶⁸

O.2 A quem incumbe realizar a avaliação de impacto?

Cabe ao Iscte, enquanto Responsável pelo Tratamento, garantir a realização da AIPD, podendo ser efetuada pelo Iscte ou por subcontratação, cabendo ainda ao Iscte envolver o Encarregado de Proteção de Dados na sua realização e solicitar o seu parecer.

Em projetos de investigação científica incumbe ao coordenador do projeto assegurar a realização da AIPD. Em teses e dissertações, incumbe ao orientador assegurar e supervisionar a sua realização. Em qualquer dos casos é obrigatório solicitar o parecer do Encarregado de Proteção de Dados.

⁶⁶ Por exemplo, com origem em duas ou mais operações de tratamento de dados realizadas com diferentes finalidades e/ou por diferentes responsáveis pelo tratamento de dados de tal forma que excedam as expectativas razoáveis do titular dos dados. Por exemplo, o tratamento de dados pessoais do percurso curricular e de desempenho de alunos de uma instituição universitária e que, para esse efeito, recorre também a dados pessoais relativos aos mesmos alunos e disponíveis publicamente numa rede social.

⁶⁷ Por exemplo, operações de tratamento destinadas a autorizar, alterar ou recusar o acesso dos titulares dos dados a um serviço ou que estes celebrem um contrato. Por exemplo, quando um banco faz um controlo seletivo dos seus clientes a partir de uma base de dados de referências de crédito bancário com vista a decidir se lhes concede ou não um empréstimo.

⁶⁸ Grupo de trabalho do artigo 29.º para a proteção de dados: 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, https://www.cnpd.pt/home/rgpd/docs/wp248rev.01_pt.pdf.

O parecer do Encarregado de Proteção de Dados e as decisões tomadas pelos coordenadores após o parecer são documentadas na AIPD.

P. VIOLAÇÃO DE DADOS PESSOAIS

Na ocorrência de uma violação de dados pessoais, o investigador ou o estudante comprometem-se a comunicá-la de imediato aos SIIC – Serviço de Infraestrutura Informática e de Comunicações e ao Encarregado de Proteção de dados do Iscte, através dos endereços de correio eletrónico institucionais ou de formulário eletrónico próprio para o efeito.

Uma violação de dados pessoais é uma violação de segurança que provoque, de modo accidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. As violações de dados pessoais envolvem uma ou mais de três tipos de ocorrências:

Violação da confidencialidade – quando existe uma divulgação ou acesso accidental ou não autorizado a dados pessoais.

Violação da integridade – quando existe uma alteração accidental ou não autorizada dos dados pessoais.

Violação da disponibilidade – quando existe uma perda de acesso ou a destruição accidental ou não autorizada de dados pessoais.

Exemplos de violações de dados pessoais incluem o extravio ou o roubo de uma *pen* ou um computador portátil que contém dados pessoais, o envio accidental ou deliberado de dados pessoais para terceiros que não tenham autorização de acesso aos dados, a infeção de um computador com vírus que destrua, altere ou comprometa a disponibilidade de dados pessoais.

A comunicação atempada da ocorrência de violações de dados pessoais é fundamental para os serviços competentes executarem um plano de resposta, capaz de mitigar os riscos para o Iscte e/ou para os titulares de dados.

Q. COMISSÃO DE ÉTICA E ENCARREGADO DE PROTEÇÃO DE DADOS

No caso de dúvidas os investigadores podem procurar aconselhamento junto do Gabinete de Apoio à Investigação e da Equipa de Proteção de Dados.

Se o projeto envolve pelo menos um dos critérios referidos na secção O.1, o investigador deve submeter o projeto a aprovação pela Comissão de Ética do Iscte ou a consulta do Encarregado de Proteção de Dados.

Se o projeto suscita questões complexas de proteção de dados, é aconselhado realizar uma AIPD - Avaliação de Impacto sobre a Proteção de Dados. A AIPD requer o parecer do Encarregado de Proteção de Dados. Quando possível, pode ser útil o projeto designar um consultor em proteção de dados.

R. DOCUMENTOS E LIGAÇÕES ÚTEIS

- [Política de Proteção de Dados Pessoais do Iscte](#)

ISCTE - Instituto Universitário de Lisboa ☑ Av. das Forças Armadas, 1649-026 Lisboa ☎ 351 217 903 000
www.iscte.pt www.facebook.com/SCTEUIUL twitter.com/iscteuiul www.linkedin.com/company/iscte-iul www.flickr.com/photos/iscteuiul www.youtube.com/user/iultv



- Página de documentos sobre proteção de dados pessoais no Fenix (separador ‘Pessoal’)
- [Código de Ética na Investigação do Iscte](#)
- [Sítio web da Comissão de Ética do Iscte](#)
- RGPD <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32016R0679>
- Lei de Execução do RGPD <https://dre.pt/web/guest/pesquisa/-/search/123815982/details/maximized>
- A proteção de dados e a investigação, opinião do Supervisor Europeu de Proteção de Dados de 6 de janeiro de 2020 https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en
- Notas de orientação sobre ética e proteção de dados para a elaboração de projetos de investigação, realizadas por um painel de peritos a pedido da Comissão Europeia https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf
- Comissão Nacional de Proteção de Dados <https://www.cnpd.pt/>
- European Data Protection Board <https://edpb.europa.eu/>
- Opiniões e Orientações relativas à proteção de dados do grupo de trabalho do Artigo 29º https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360
- Orientações relativas ao princípio da transparência https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
- Orientações relativas ao consentimento https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
- Orientações relativas à avaliação de impacto na proteção de dados https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
- Opinião relativa a técnicas de anonimização https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
- Orientações sobre as decisões individuais automatizadas e a definição de perfis https://www.cnpd.pt/home/rgpd/docs/wp251rev01_pt.pdf
- Outras opiniões do grupo do Artigo 29: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

S. DEFINIÇÕES

| | |
|------------------------------|---|
| 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. |
| 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. |
| Proteção de Dados Pessoais | Um direito fundamental, protegido não apenas pela legislação nacional, mas pela legislação europeia. |
| Titular dos Dados | Qualquer pessoa singular identificada ou identificável que seja objeto de dados pessoais detidos pelo responsável pelo tratamento. |
| 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. |
| Dados de natureza altamente pessoal | Tratam-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). |
| Responsável pelo Tratamento | A pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais. |
| 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. |
| Consentimento do titular de dados | Uma manifestação de vontade, livre, específica, informada e 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. |
| Finalidade legítima | Os fins para os quais os dados pessoais podem ser utilizados. |
| 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. |
| Anonimização | Conversão irreversível de dados pessoais em dados anónimos de forma a que deixem de poder ser atribuídos a titulares de dados identificados ou identificáveis. Os dados não devem ser passíveis de re-identificação. |
| FIP – Ficha de Informação ao Participante | 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. Vide secção F.2 |
| Re-identificação | Processo de transformar dados que se creem anonimizados novamente em dados pessoais por meio de correspondência de dados ou técnicas semelhantes. |
| 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. |
| Decisões individuais automatizadas (DIA) | As decisões individuais <i>exclusivamente</i> 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. |
| Violação de dados pessoais | Uma violação da segurança que provoque, de modo accidental 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 |

Registo do histórico de alterações

| Versão nº | Descrição da alteração | Data de emissão |
|-----------|--|-------------------------|
| 01 | Versão inicial, proposta do Encarregado de Proteção de Dados | 16 de Outubro de 2020 |
| 02 | Revisão da proposta pelos serviços jurídicos e Encarregado de Proteção de Dados. | 26 de Março de 2021 |
| 03 | Revisão da proposta pelo Equipe de Proteção de Dados após reunião com Reitoria e GAI. Incluídas secções ou informações adicionais, relativas a transferências internacionais, tipologia dos prazos de conservação e dados pessoais de pessoas falecidas. | 18 de Fevereiro de 2022 |
| 04 | Aprovado por despacho da Reitoria e autorização para publicação. | 28 de Março de 2022 |