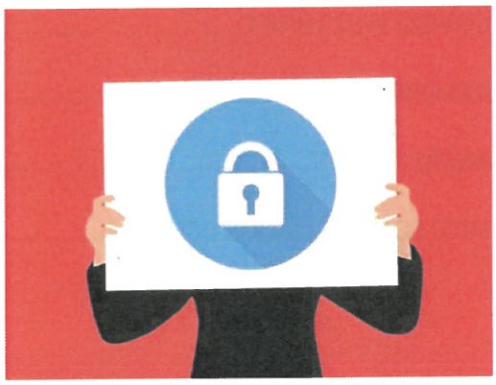
Politécnico de Coimbra

BOAS PRÁTICAS NO TRATAMENTO DE DADOS PESSOAIS



Índice

1. ENQUADRAMENTO

O Regulamento Geral sobre a Proteção de Dados (RGPD) – Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, aplicável desde 25 de maio de 2018, estabelece um conjunto de novos princípios a que deve obedecer o acesso e tratamento de dados pessoais, assim como direitos acrescidos para os titulares dos dados, consagrando a proteção das pessoas singulares relativamente ao tratamento de dados pessoais como um direito fundamental.

O Instituto Politécnico de Coimbra (IPC), enquanto Instituição de Ensino Superior (IES), tem necessidade de recolher dados pessoais para a prossecução das suas atribuições e para o cumprimento das suas obrigações legais, sendo o responsável pelo tratamento desses dados.

O tratamento dos dados pessoais deve ser feito em conformidade com o RGPD, bem como com a Lei nº 58/2019, de 8 de agosto, que assegura a sua execução na ordem jurídica nacional.

Reforçando o seu empenho na proteção e confidencialidade dos dados pessoais, e ainda no respeito pelo exercício do direito à privacidade dos titulares desses dados quando se relacionam com a instituição, o IPC aprovou, em 24 de março de 2022, a sua política de privacidade e de proteção de dados pessoais, a qual é aplicável a todas as operações desenvolvidas no âmbito das atividades por si prosseguidas.

Também o Código de Ética e Conduta do IPC, aprovado em 6 de outubro de 2022, salvaguarda a proteção de dados pessoais, garantindo que os membros da comunidade IPC que tomem conhecimento ou acedam a dados pessoais relativos a pessoas singulares ficam obrigados a respeitar as disposições legais relativas à proteção desses dados, não os podendo utilizar senão para os efeitos legalmente impostos ou inerentes às funções que desempenham.

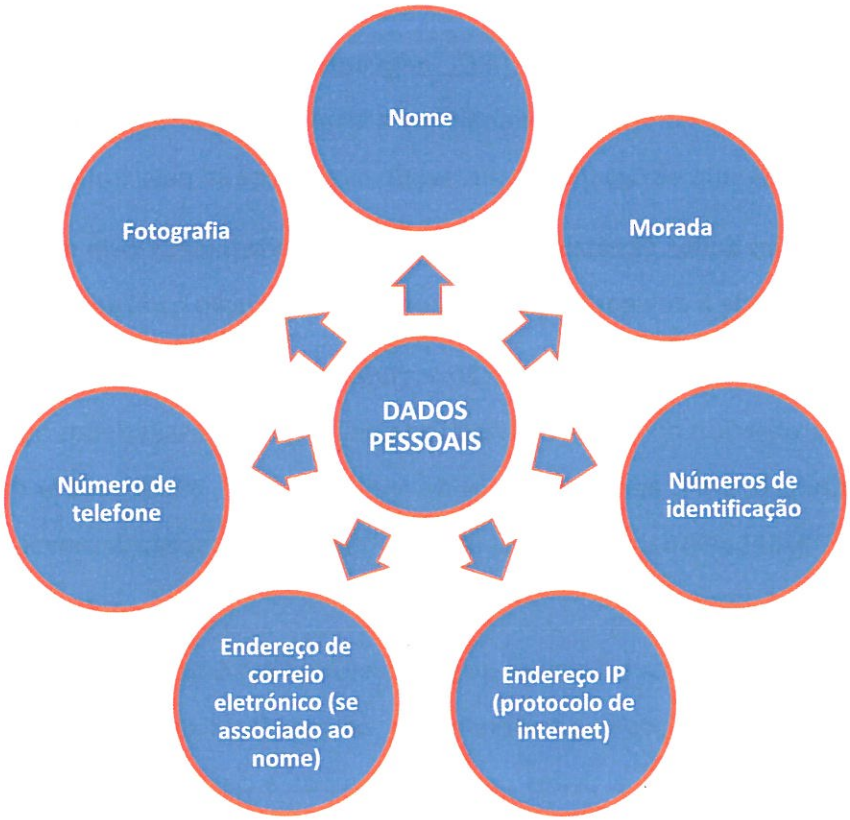
Neste contexto, o presente Manual de Boas Práticas tem como objetivo principal fornecer orientações práticas e claras que devem ser observadas pelos colaboradores[1] do IPC, contribuindo para que seja assegurado o respeito pela privacidade e segurança dos dados pessoais de acordo com a legislação em vigor em todas as suas atividades institucionais.

[1] Dirigentes, trabalhadores do corpo docente e não docente, investigadores, bolseiros e estagiários.

2. CONCEITOS

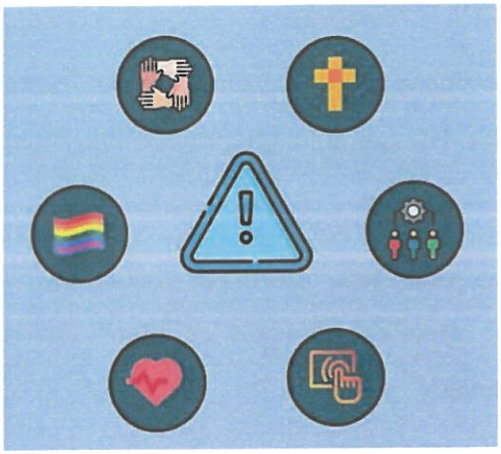
Dados pessoais: Informação relativa a uma pessoa singular identificada ou identificável que é o titular dos dados. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa.

Exemplos de dados pessoais:



Dados pessoais sensíveis: Dados que, pela sua natureza, são especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais e que, por esse facto, estão sujeitos a condições de tratamento específicas.

São considerados dados "sensíveis":



- Dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas
- Filiação sindical
- Dados genéticos, dados biométricos tratados simplesmente para identificar uma pessoa de forma inequívoca
- Dados relacionados com a saúde
- Dados relativos à vida sexual ou orientação sexual da pessoa.

Tratamento: 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,
- A eliminação.

Anonimização: Técnica de processamento de dados que remove ou modifica as informações que possam identificar uma pessoa. Por exemplo, um dado pessoal como data de nascimento pode ser substituído por uma categoria mais geral, como faixa etária.

Pseudonimização: Processo de remoção, modificação ou substituição das características individuais por outras representações codificadas. Por exemplo, um nome e sobrenome podem ser substituídos por um código.

Consentimento: 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.

3. SANÇÕES[2]

As contraordenações praticadas por infrações ao RGPD são punidas com coimas que podem ascender a 20.000.000€.

São ainda consideradas crime, puníveis com pena de prisão, as seguintes ações no tratamento de dados pessoais:

- Utilização de dados de forma incompatível com a finalidade da recolha;
- Acesso indevido;
- Desvio de dados (copiar, subtrair, ceder ou transferir dados sem previsão legal ou consentimento);
- Viciação ou destruição de dados (apagar, destruir, danificar, ocultar, suprimir ou modificar dados pessoais sem previsão legal ou consentimento);
- Inserção de dados falsos com intenção de obter vantagem indevida para si ou para terceiro;

- Violação do dever de sigilo;
- Desobediência após notificação da Comissão Nacional de Proteção de Dados (CNPD) para cumprimento das obrigações previstas no RGPD.

[2] Capítulo VII da Lei n.º 58/2019, de 8 de agosto.

4. BOAS PRÁTICAS

Para cumprir as exigências do RGPD é essencial que os colaboradores do IPC adotem um conjunto de boas práticas no desempenho das suas funções, de modo a assegurar a confidencialidade e a segurança no tratamento de dados pessoais, evitando acessos, utilizações ou divulgações não autorizadas, bem como a consulta, alteração, cópia ou eliminação de dados pessoais de forma indevida ou ilícita.

A) GESTÃO DE DADOS PESSOAIS

No âmbito da gestão de dados pessoais, os colaboradores do IPC devem:

- Recolher os dados pessoais que sejam estritamente necessários para a execução das suas tarefas;
- Tratar os dados pessoais apenas nas situações legal e regulamentarmente previstas, no âmbito das suas funções e exclusivamente para a(s) finalidade(s) para que foram recolhidos;
- Ter especial cuidado no tratamento de documentos com informações críticas, como é o caso de dados médicos ou de menores;
- Guardar sigilo sobre os dados pessoais a que tiverem acesso no exercício das suas funções;
- Limitar a partilha de dados pessoais com terceiros apenas às finalidades autorizadas;
- Fazer o registo das operações de tratamento de dados, de acordo com o procedimento do SIGQ do IPC, e definir procedimentos para o ciclo de vida dos dados, incluindo a recolha, armazenamento, utilização, partilha e eliminação segura dos dados pessoais;
- Realizar avaliações de impacto sobre a proteção de dados (AIPD), de acordo com o procedimento do SIGQ do IPC, para identificar e mitigar riscos associados ao tratamento de dados pessoais em novos projetos;
- Sempre que necessário, aplicar técnicas de anonimização ou pseudonimização para proteger a identidade dos titulares dos dados, garantindo que as mesmas permanecem robustas e eficazes face às novas ameaças e tecnologias;

- Manter registos detalhados dos métodos e procedimentos de anonimização e pseudonimização, incluindo as justificações para a sua escolha e as avaliações de risco realizadas;
- Sempre que os dados forem anonimizados, certificar-se que os dados não podem ser revertidos ou combinados com outras informações para identificar o seu titular;
- Obter o consentimento explícito dos titulares dos dados para o seu tratamento, garantindo que os mesmos estão devidamente informados sobre a finalidade, a utilização dos dados e as técnicas de anonimização ou pseudonimização aplicadas;

- Eliminar os dados pessoais após o respetivo tratamento ou após os prazos de conservação legalmente definidos, consoante os casos;
- Dar conhecimento imediato ao superior hierárquico da existência de acesso a dados pessoais não necessários ao desempenho das suas funções.

B) SEGURANÇA FÍSICA DOS PROCESSOS

A fim de garantir a segurança física dos processos, os colaboradores do IPC devem:

- Guardar num local seguro[3] todos os processos, dossiers, capas e documentos que contenham dados pessoais;
- Retirar da mesa de trabalho qualquer documento/processo que contenha dados pessoais depois de utilizado;
- Limitar ao estritamente necessário as impressões e/ou cópias de documentos que contenham dados pessoais;
- Retirar imediatamente todas as impressões que contenham informações pessoais, utilizadas ou processadas por equipamentos de suporte, como impressoras, fotocopiadoras e digitalizadoras, após o seu processamento;

- Destruir de forma definitiva, os documentos que contenham dados pessoais que não seja necessário arquivar, incluindo as fotocópias

[3] Cada serviço deverá identificar fisicamente o "local seguro" junto dos colaboradores para garantia desta segurança.

utilizadas apenas como instrumento de trabalho, garantindo que não serão recuperados por terceiros;

- Transportar documentos que contenham dados pessoais de forma devidamente protegida, utilizando um envelope apropriado para o efeito e identificado como confidencial, de modo a impedir o acesso não autorizado ao seu conteúdo.

Ainda neste âmbito, os colaboradores do IPC não devem:

- Criar cópias ou arquivos que contenham dados pessoais sem autorização para o efeito;
- Utilizar o verso de fotocópias com dados pessoais como folha de rascunho ou com outra finalidade;
- Retirar das instalações qualquer documento/processo que contenha dados pessoais sem estar devidamente autorizado.

C) SEGURANÇA DA INFORMAÇÃO DIGITAL

A fim de garantir a segurança da informação digital, os colaboradores do IPC devem:

- Bloquear o computador sempre que se ausentarem do seu posto de trabalho, utilizando a combinação das teclas (Windows+L) e desligá-lo no final do dia de trabalho;
- Proteger os ficheiros de trabalho que contenham dados pessoais com *passwords* para abertura e edição;
- Criar *passwords* robustas, com pelo menos 12 caracteres, contemplando as seguintes regras: combinação de letras maiúsculas e minúsculas, algarismos e caracteres especiais;
- Manter as *passwords* confidenciais e alterá-las com regularidade;
- Utilizar sempre a rede informática para criação das pastas de trabalho, evitando a utilização de pastas locais;
- Utilizar ferramentas recomendadas pela instituição para encriptar dados sensíveis tanto em repouso (armazenados) quanto em trânsito (enviados pela rede);

- Garantir que o transporte de dados é feito de modo seguro (por exemplo com *pens* encriptadas).

Ainda neste âmbito, os colaboradores do IPC não devem:

- Partilhar nem deixar em locais visíveis ou de fácil acesso, o *login*, as *passwords* e os códigos de acesso;
- Instalar *software* não autorizado em qualquer computador ou outro dispositivo da instituição;
- Utilizar discos externos e/ou *pens* para o trabalho regular.

D) UTILIZAÇÃO DE CORREIO ELETRÓNICO

Na utilização de correio eletrónico, os colaboradores do IPC devem:

- Garantir que os destinatários estão corretos e são os destinatários que devem receber e ter acesso à informação enviada;

- Assegurar que os ficheiros enviados em anexo contêm apenas os dados pessoais que se pretendam comunicar;
- Efetuar o envio de correio eletrónico de âmbito geral (ex.: *newsletters*, convocatórias, informações de carácter geral), para múltiplos endereços de correio eletrónico, utilizando o campo *Bcc*, por forma a não expor todos os destinatários;
- Encriptar com código ao qual só o destinatário tenha acesso, ou proteger com *password*, os dados pessoais enviados através de mensagens por correio eletrónico;
- Eliminar as mensagens recebidas caso não seja o destinatário das mesmas e informar o remetente.

Na utilização de correio eletrónico, os colaboradores do IPC não devem:

- Partilhar o acesso ao correio eletrónico;
- Enviar credenciais de acesso em correio eletrónico;
- Utilizar o endereço de correio eletrónico pessoal para transmitir informação da instituição;

- Utilizar dispositivos pessoais partilhados para aceder ao endereço de correio eletrónico institucional.

Ainda neste âmbito, os colaboradores do IPC também não devem:

- Abrir mensagens de correio eletrónico com origem desconhecida;
- Enviar *passwords* ou outros dados pessoais, em resposta a *e-mail* pedindo esses dados (prática conhecida por *"phishing");*

- Abrir anexos que tenham extensões executáveis (como: *.exe*, *.bat*, *.com*, *.dll*);
- Clicar em ligações e/ou atalhos (*links* e *URL's*) com origem desconhecida;
- Dar seguimento a "correntes", devendo eliminar todo o correio eletrónico que se enquadre nessa categoria;
- Utilizar o conteúdo de mensagens se não forem o destinatário legítimo da mesma, notificando o seu remetente para esse facto.

Ao receber mensagens de correio eletrónico, os colaboradores do IPC devem sempre estar alerta e desconfiar:

- Se o endereço de e-mail ou telefone do remetente não for conhecido por si;
- De mensagens que apresentem erros gramaticais e ortográficos.

E) ATENDIMENTO TELEFÓNICO

Nos contactos telefónicos com o exterior, os colaboradores do IPC não devem:

- Fornecer qualquer informação com dados pessoais. Caso sejam solicitados, os dados pessoais só devem ser transmitidos nas situações legalmente permitidas, após pedido formalizado por escrito;

- Transmitir informações sobre os colegas, limitando-se apenas à respetiva disponibilidade. No caso de indisponibilidade, deve ser solicitado que se deixe recado e não deverá ser prestada nenhuma informação sobre a localização do trabalhador ou a sua ausência do edifício sem autorização do mesmo.

No ambiente interno da Instituição os colaboradores do IPC apenas devem transmitir dados pessoais por telefone:

- No estrito cumprimento das suas funções, certificando-se que a informação é fornecida a interlocutor com autorização para a receber;
- Assegurando a confidencialidade das conversas telefónicas.

F) CAPTAÇÃO DE IMAGENS E SOM

Neste âmbito os colaboradores do IPC não devem:

- Recolher imagens ou som, por meio de fotografia, vídeo ou gravação de som, em qualquer contexto, designadamente aulas, avaliações, visitas de estudo, afixação de pautas, listas de alunos, horários, eventos institucionais ou reuniões de trabalho, salvo se estiverem verificados os seguintes requisitos cumulativos:
  - Ser imprescindível ao desenvolvimento de atividades enquadradas na missão e fins do IPC;
  - Ter autorização dos órgãos competentes do IPC; e
  - Ter autorização dos titulares dos dados ou, tratando-se de menores, dos respetivos representantes legais;

- Fazer capturas ou tirar fotografias de ecrã que contenham dados pessoais;
- Publicar imagens ou som de terceiros em sítios da Internet ou nas redes sociais, sem que tal esteja devida e previamente autorizado pelos titulares dos dados em causa.

5. ENCARREGADO DA PROTEÇÃO DE DADOS DO IPC

Para o esclarecimento de qualquer dúvida deverá contactar o Encarregado da Proteção de Dados do IPC (epd@ipc.pt).

Deverá ainda informar o Encarregado da Proteção de Dados do IPC sobre qualquer violação de dados pessoais, efetiva ou potencial, de que tome conhecimento.

Ficha Técnica

Título
Manual de Boas Práticas no Tratamento de Dados Pessoais

Emissor
Gabinete de Assessoria Jurídica do IPC
Departamento de Tecnologias de Informação e Comunicação
Gabinete da Qualidade

Versão 00
Editado em 15 de novembro de 2024

Aprovado
7/1/2025

www.ipc.pt
https://sigq.ipc.pt
qualidade@ipc.pt