PRESIDÊNCIA DO CONSELHO DE MINISTROS
Secretaria-Geral

TRANSPARÊNCIA

RGPD

Manual de Implementação

ÂMBITO

O Regulamento Geral de Proteção de Dados (RGPD) é um Regulamento aplicável em toda a União Europeia (UE), tendo sido aprovado em 27 de abril de 2016 pelo Parlamento Europeu e pelo Conselho, e entrado em vigor a 25 de maio de 2018, em todos os Estado-Membros, sem necessidade de transposição para o seu ordenamento jurídico interno.

O RGPD - Regulamento (EU) n.º 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 retificado pela Retificação do Regulamento (UE) 2016/679 - estabelece novas regras relativas à proteção dos dados pessoais das pessoas singulares, vivas, no que respeita ao tratamento e à livre circulação dos respetivos dados.

Na ordem jurídica nacional a execução do Regulamento encontra-se assegurada pela Lei n.º 58/2019, de 8 de agosto.

O presente Manual é uma guia de orientação prática e procedimental destinado à implementação do RGPD, tendo em vista o estabelecimento de uma cultura organizacional de proteção de dados.

Índice

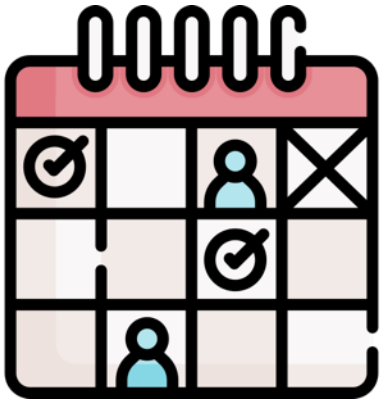
DISPOSIÇÕES INICIAIS

O RGPD tem como objetivo principal uniformizar o regime de proteção de dados pessoais no Espaço Económico Europeu (EEE), eliminando, dessa forma, as assimetrias existentes nos diferentes regimes em vigor nos países que integram o EEE e que se constituíam como uma dificuldade ao funcionamento do Mercado Único.

Com esse intuito, o RGPD apresenta um conjunto de **direitos dos titulares de dados pessoais** e de **obrigações no tratamento de dados** que conformam a ação dos Responsáveis pelo Tratamento e Subcontratantes.

Esta nova legislação europeia impõe que toda a apreciação, interpretação e aplicação do RGPD seja feita na perspetiva da proteção dos direitos do titular dos dados, pelo que o importante não é o local onde os dados pessoais são tratados, mas antes o local onde se encontra o titular dos dados pessoais.

A proteção abrange o tratamento de dados feito por uma entidade - pessoa singular ou coletiva - situada na UE, assim como todas as entidades que desenvolvam atividades de oferta de bens e serviços aos titulares dos dados situados neste território, ou que controlem o comportamento dos titulares dos dados, desde que esse comportamento ocorra na UE. O que releva é o facto de se tratar de dados pessoais de indivíduos que se situem na UE, não sendo necessário que sejam nacionais ou residentes de um Estado-Membro.



CONCEITOS

Dados pessoais

Qualquer informação relativa a pessoas singulares que as identifique ou as torne identificáveis, de forma direta ou indireta[1]. O RGPD prevê ainda categorias especiais de dados (conceito *infra*) com diferentes regras de tratamento.

Encarregado de Proteção de Dados

A pessoa nomeada que tem como função principal informar e aconselhar quanto ao cumprimento das obrigações relevantes em matéria de proteção de dados. Assegura, ainda, a realização de auditorias, sensibiliza para a deteção atempada de incidentes de segurança e serve de ponto de contato com os titulares dos dados e com a autoridade de controlo.

Tratamento de dados

Operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre um conjunto de dados pessoais, por meios automatizados ou não automatizados[2].

---

[1] Por exemplo:
- O nome;
- Os números de identificação;
- A morada;
- O telefone;
- O endereço de correio eletrónico;
- O estado civil;
- O identificador de cliente;
- O IP de um computador;
- A matrícula de um automóvel.

Exemplos de dados não considerados pessoais:
- N.º de registo de uma empresa;
- Endereço de correio eletrónico tipo info@institutopublico.pt;
- Dados anonimizados.

[2] Exemplos: 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; Tipos de operação de tratamento: processamento salarial e gestão de pessoal; destruição de documentos que contenham dados pessoais; colocação de fotografias pessoais em websites; recolha de elementos identificativos num serviço de receção.

Responsável pelo tratamento

A entidade que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais. É o responsável pelo cumprimento das regras legais de proteção de dados.

Subcontratante

A entidade, pública ou privada, que trata os dados pessoais por conta do responsável pelo tratamento. Inclui-se aqui, *por exemplo*, a entidade que processa os salários, ou que armazena os processos administrativos.

Destinatário

A pessoa ou entidade que, não sendo o responsável pelo tratamento, nem subcontratante, nem o titular dos dados, recebe dados pessoais. O destinatário pode, ou não, ser qualificado como um *terceiro*.

Terceiro

O conceito de terceiro é um conceito negativo, assim, não é considerado terceiro o responsável pelo tratamento, o subcontratante, quem, sob a autoridade direta destes, está autorizada a tratar dados[3], nem o titular dos dados.

Consentimento

O consentimento é a manifestação de vontade livre, específica, informada e inequívoca, prestada de forma clara e expressa, que o titular dos dados aceita o tratamento.

O responsável pelo tratamento deve poder demonstrar que o consentimento foi efetivamente prestado pelo titular (artigo 7.º, n.º 1, do RGPD).

[3] Por exemplo, uma empresa que, para prestar assistência informática, necessite de aceder a dados pessoais; um trabalhador em funções públicas que proceda à introdução de dados pessoais num ficheiro informático

O consentimento face a serviços de sociedade de informação[4] prestado por um menor só releva se o mesmo tiver completado 13 anos de idade, caso contrário o consentimento é prestado pelos representantes legais do menor, preferencialmente por meio de autenticação segura (artigo 16.º da Lei n.º 58/2019, de 8 de agosto).

Violação de dados pessoais

A violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizados a dados pessoais.

Definição de perfis

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

Pseudonimização

O tratamento de dados de forma que deixem de poder ser atribuídos a um titular de dados sem recorrer a informações suplementares, desde que essas informações sejam mantidas separadamente e sujeitas a medidas para assegurar que os dados não possam ser atribuídos a uma pessoa identificada ou identificável.

Anonimização

Processo pelo qual informações são alteradas de forma irreversível de modo que já não possam ser identificadas direta ou indiretamente, pelo responsável pelo tratamento por si só, ou em colaboração com qualquer outra entidade.

Categorias especiais de dados

As categorias especiais de dados são dados pessoais especialmente sensíveis para efeitos do RGPD.

---

[4] Qualquer serviço prestado normalmente sem remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços (artigo 1.º, al. *b)*, da Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, por remissão do artigo 4.º, ponto *25)*, do RGPD).

São categorias especiais de dados:

- Dados sobre origem racial ou étnica;
- Dados sobre opiniões políticas;
- Dados sobre convicções religiosas;
- Dados sobre convicções filosóficas;
- Dados sobre a filiação sindical;
- Dados genéticos;
- Dados biométricos;
- Dados relativos a saúde;
- Dados sobre a vida sexual;
- Dados sobre a orientação sexual.

O tratamento destes dados é, em princípio, proibido, carecendo de uma das exclusões da ilicitude do tratamento que consta do artigo 9.º, n.º 2, do RGPD.

Titulares de dados vulneráveis

Critério aferido quando exista um acentuado desequilíbrio e poder entre os titulares dos dados e o responsável pelo tratamento, significando que os titulares podem não consentir, ou opor-se, facilmente ao tratamento dos seus dados (*por exemplo, crianças, trabalhadores, pessoas que necessitem de proteção especial - como pessoas com doenças mentais, requerentes de asilo, idosos, doentes, etc.*).

Dados sensíveis ou de natureza altamente pessoal

Além das categorias especiais de dados do artigo 9.º do RGPD, e dados relativos a condenações penais e infrações (constante do artigo 10.º do RGPD), podem ser dados sensíveis ou de natureza altamente pessoal os dados que o sejam na aceção comum do termo, e estão, nomeadamente, associados a atividades privadas ou familiares, que afetem o exercício de um direito fundamental, ou porque a sua violação implicaria a grave afetação da vida quotidiana do titular.

Dados tratados em grande escala

O RGPD não define o que constitui um tratamento em grande escala, contudo o Grupo de Trabalho do Artigo 29.º para a Proteção de Dados recomenda, nomeadamente, os seguintes fatores para determinar esse tratamento:

- o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente;
- o volume de dados e/ou a diversidade de dados diferentes a tratar;
- a duração da atividade de tratamento de dados ou a sua pertinência.

ENCARREGADO DE PROTEÇÃO DE DADOS

A designação de EPD[5] é obrigatória nos organismos e autoridades públicas.

Os dirigentes das entidades públicas podem propor a designação do encarregado de proteção de dados ao responsável pela respetiva área governativa, a quem cabe decidir quanto ao número de encarregados de proteção de dados a designar.

Nos termos do RGPD, o EPD exerce a sua atividade com independência, não podendo ser prejudicado pelo exercício das suas funções.

São funções do EPD, nomeadamente:

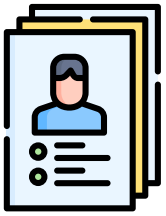
- Informar e aconselhar o responsável pelo tratamento, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações em matéria de proteção de dados;
- Verificar se as recomendações efetuadas, no sentido do respeito pelo cumprimento das obrigações constantes do RGPD e da lei, estão a ser cumpridas, podendo realizar auditorias, periódicas ou não;
- Cooperar com a autoridade de controlo, servindo de ponto de contacto;
- Servir de ponto de contacto dos titulares dos dados relativamente a todas questões relacionadas com o tratamento dos seus dados pessoais;
- Sensibilizar o responsável do tratamento de dados para que, em todas as fases do tratamento, desde a recolha à destruição, sejam observados os princípios do registo e tratamento de dados.
- Emitir parecer quanto à necessidade de realização de uma Avaliação de Impacto sobre Proteção de Dados.
- Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança

Elementos adicionais sobre o EPD - consultar Grupo de Trabalho do Artigo 29.º para a Proteção de Dados

[5] Sobre o estatuto do EPD nas entidades públicas, *vide* "O Encarregado de Proteção de Dados nas Pessoas Coletivas Públicas – Notas breves para a compreensão do seu estatuto", FERNANDA MAÇÃS e FILIPA CALVÃO, pág. 44 e ss., *Forum de Proteção de Dados – Comissão Nacional de Proteção de Dados*, n.º 7, Dezembro de 2020, disponível em https://www.cnpd.pt/media/5kajlbve/forum7_web.pdf

FASES DE IMPLEMENTAÇÃO

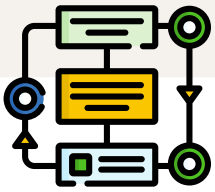
De modo a simplificar a implementação do RGPD pelas entidades visadas, foram definidas cinco fases de implementação do Regulamento:



Designar
um encarregado de proteção de dados

Mapear
os dados pessoais objeto de tratamento

Priorizar
as ações a desenvolver



Organizar
os processos internos

Documentar
a conformidade com o RGPD

FASE 1 - DESIGNAR UM ENCARREGADO DE PROTEÇÃO DE DADOS

O Regulamento introduz a figura do encarregado de proteção de dados, que terá como função supervisionar os processos de segurança instituídos com vista a garantir a proteção de dados pessoais no dia-a-dia da entidade.

Integram o elenco de funções do EPD, sem prejuízo de outras que se considerem necessárias para assegurar o cumprimento do RGPD, as seguintes funções:

- Informar e aconselhar o responsável pelo tratamento, bem como todos os trabalhadores que tratem os dados, a respeito das suas obrigações no que respeita ao tratamento de dados pessoais;
- Controlar a conformidade das operações de tratamento com o RGPD;
- Cooperar com a Comissão Nacional de Proteção de Dados (CNPD);
- Receber os pedidos de contacto dos titulares dos dados sobre todas as matérias relacionadas com o tratamento dos seus dados e o exercício dos seus direitos;
- Assegurar a realização de auditorias, periódicas ou não programadas;
- Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança;
- Assegurar as relações com os titulares dos dados nas matérias abrangidas pela lei.

As entidades públicas, independentemente da sua dimensão e do tipo de dados pessoais que tratam, estão obrigadas a nomear um EPD (cf. o artigo 37.º, n.º 1, do RGPD), que pode ser comum a várias entidades. A designação formal do EPD cabe:

i. na administração direta, ao ministro responsável por cada área governativa, sem prejuízo de este delegar tal competência noutro órgão;
ii. na administração indireta, ao órgão executivo, de administração ou gestão, com faculdade de delegação.

PROCEDIMENTOS A REALIZAR

- Designar um encarregado de proteção de dados (EPD), com vista a apoiar a entidade pública na adoção de medidas que assegurem o cumprimento sistemático das obrigações impostas pelo RGPD;

- Publicitar os contactos profissionais do EPD no sítio eletrónico da entidade pública;

- Comunicar à autoridade nacional de controlo - a CNPD - a identificação do encarregado e os seus contactos profissionais: morada, telefone e correio eletrónico.

***Checklist* para a Fase 1**

Fase 1. Designar um Encarregado de Proteção de Dados (EPD)	
1	Foi nomeado um EPD com as funções de apoiar a implementação e a conformidade com o RGPD?
2	Os contatos do EPD foram publicitados no *website* institucional da entidade?
3	A designação e os contatos do EPD foram comunicados à CNPD?
4	Encontram-se asseguradas as condições necessárias para que o EDP desenvolva as tarefas que lhe incumbem de forma independente e eficaz?

FASE 2 - MAPEAR OS DADOS PESSOAIS OBJETO DE TRATAMENTO

A presente etapa consiste na execução do levantamento, completo e prévio, de todos os dados pessoais tratados pela entidade.

PROCEDIMENTOS A REALIZAR

Esta tarefa de levantamento de dados deve permitir responder às seguintes questões:

Quem	O quê	Porquê	Onde	Até quando	Como
• Identificação do responsável pelo tratamento de dados pessoais; • Identificação do responsável pelos serviços que processam os dados; • Identificação do subcontratante (caso exista).	• Identificação das categorias de dados pessoais objeto de tratamento; • Identificação dos dados pessoais que apresentam maiores riscos devido à sua sensibilidade específica (por exemplo, dados relativos à saúde).	• Indicação da(s) finalidade(s) para a(s) qual(is) os dados pessoais são recolhidos e tratados (por exemplo: gestão de recursos humanos).	• Determinação de todos os locais onde os dados pessoais se encontram arquivados; • Identificação dos eventuais fluxos de dados, indicando a sua origem e o destino.	• Determinação do prazo de conservação dos dados.	• Especificação das medidas de segurança implementadas (a nível técnico e organizativo) para minimizar os riscos de violações de dados.

***Checklist* para a Fase 2.**

Fase 2. Verificação dos objetivos a atingir	
1	Foram identificados todos os serviços e entidades que processam dados pessoais?
2	Foram identificados os tipos de dados pessoais objeto de tratamento, incluindo os dados sensíveis (quando seja o caso)?
3	Foi estabelecida a listagem dos principais processos de tratamento e da(s) finalidade(s) a que se destinam?
4	Foram identificados todos os locais onde os dados pessoais se encontram arquivados?
5	Foi estabelecido o período durante o qual esses dados devem ser mantidos?

FASE 3 - PRIORIZAR AS AÇÕES A DESENVOLVER

A terceira fase consiste na avaliação da conformidade dos processos de recolha e tratamento dos dados com os princípios e regras do RGPD, dando prioridade às situações que comportam um maior risco de violação do Regulamento.

PROCEDIMENTOS A REALIZAR

- Identificar o fundamento de licitude que permite o tratamento dos dados[6]:
    - Caso o fundamento seja o consentimento do titular, verificar se o mesmo foi prestado em conformidade com as exigências do RGPD, ou seja, se existe uma declaração de vontade livre, informada, explícita e inequívoca. Não são admitidos consentimentos tácitos nem opções pré-validadas;
    - O titular dos dados tem o direito de retirar o consentimento a qualquer momento, pelo que, mesmo quando este tenha sido validamente prestado, deverá ser sempre aferida a existência de outros fundamentos de licitude.
- Desde o início, especificar a finalidade a que se destina o tratamento dos dados recolhidos;
- Garantir que apenas são recolhidos e tratados os dados pessoais estritamente necessários para a prossecução da finalidade identificada;
- Rever os contratos com subcontratantes (quando existam), certificando-se de que as respetivas cláusulas oferecem garantias de respeito pelo RGPD e propondo, se necessário, as modificações relevantes ao contrato.

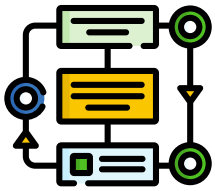
[6] Por exemplo, o consentimento do titular, a necessidade do tratamento para o cumprimento de um contrato ou de uma obrigação legal. Os fundamentos da licitude do tratamento encontram-se no artigo 6.º do RGPD. Quando se trate de categorias especiais de dados deve ter-se em conta, ainda, o artigo 9.º do RGPD.

***Checklist* para a Fase 3.**

Fase 3. Verificação dos objetivos a atingir	
1	Foi(ram) identificado(s) o(s) fundamento(s) de licitude que legitimam cada operação de tratamento?
2	Foi verificada a conformidade das declarações de consentimento pré-existentes com o RGPD?
3	Foi verificado que nenhum dado é tratado de forma incompatível com a finalidade para que foi recolhido?
4	Foi verificado que a recolha e tratamento de dados se limita ao estritamente necessário?
5	Foi verificada a conformidade dos contratos de tratamento de dados pré-existentes com o RGPD?

FASE 4 – ORGANIZAR OS PROCESSOS INTERNOS

PROCEDIMENTOS A REALIZAR



- Organizar os processos internos que envolvem o tratamento de dados pessoais de forma a assegurar o cumprimento efetivo do RGPD em todas as fases do tratamento.

No cumprimento deste procedimento devem ser garantidas:

- A proteção de dados desde a conceção e por defeito, através da implementação de medidas técnicas[7] e organizativas[8] que garantam o respeito pelos princípios consagrados no artigo 5.º do RGPD e a segurança e confidencialidade dos dados recolhidos e conservados pela entidade em todas as fases do tratamento;
- A eficácia na resposta a possíveis violações de dados, elaborando planos de contingência a acionar em caso de quebra de segurança, incluindo medidas de mitigação/eliminação dos riscos, procedimentos de notificação à CNPD e procedimentos de notificação aos titulares dos dados afetados (quando necessário);
- A correta gestão dos pedidos e queixas dos titulares dos dados, devendo ser disponibilizados mecanismos que facilitem o exercício dos direitos dos titulares de dados pessoais (acesso, retificação, portabilidade, retirada do consentimento, etc.);
- A sensibilização dos trabalhadores para a importância da temática e a criação de uma cultura organizacional de respeito pela proteção de dados.

[7] Por exemplo, fortalecendo o *software* contra intromissões informáticas.
[8] Por exemplo, estabelecendo normas de acesso diferenciado.

***Checklist* para a Fase 4.**

Fase 4. Organizar os processos internos	
1	Os princípios de tratamento de dados pessoais são tidos em conta na conceção de todas as ferramentas, procedimentos e sistemas de recolha, tratamento e conservação dos dados.
2	Os principais riscos de segurança foram identificados e devidamente acautelados.
3	Foram elaborados planos de contingência que permitem saber o que fazer e quem contatar em caso de incidente de segurança.
4	Estão instaladas plataformas/canais de comunicação que permitem aos titulares dos dados exercer os seus direitos.
5	Foi elaborado um plano de formação e sensibilização dos trabalhadores.

FASE 5 - DOCUMENTAR A CONFORMIDADE COM O RGPD

PROCEDIMENTOS A REALIZAR

- Criar um registo, periodicamente revisto, que permita ao responsável pelo tratamento de dados pessoais demonstrar que todas as atividades desenvolvidas sob a sua responsabilidade respeitam, em cada momento, o RGPD.

Este registo deve incluir:

1. **Relativamente à documentação sobre o tratamento de dados pessoais:**
    - O registo de tratamento ou as categorias de atividade de tratamento;
    - Avaliações de impacto (para dados pessoais cujo tratamento possa comportar um risco elevado para os direitos, liberdades e garantias dos cidadãos);
    - O registo das transferências de dados para fora da UE (quando existam).

2. **Relativamente aos dados pessoais:**
    - Os dados em causa;
    - A indicação dos fundamentos de licitude do tratamento dos dados (incluindo, quando for o caso, as declarações de consentimento dos respetivos titulares);
    - A descrição dos procedimentos estabelecidos para que os titulares dos dados pessoais possam exercer os seus direitos;
    - A descrição dos procedimentos internos de resposta às situações de violação das obrigações do RGPD.

3. **Relativamente aos subcontratantes:**
    - Cópias dos contratos que regem a transmissão e tratamento dos dados tratados pelo subcontratante[9].

[9] Esta obrigação não se aplica a entidades com menos de 250 trabalhadores, a menos que o tratamento:
a) possa implicar um risco para os direitos, liberdades e garantias do titular dos dados;
b) não seja ocasional;
c) abranja dados sensíveis ou dados pessoais relativos a condenações penais e infrações.

***Checklist* para a Fase 5.**

Fase 5. Documentar a conformidade com o RGPD	
1	A entidade documenta de forma sistemática as atividades de tratamento desenvolvidas.
2	As informações incluídas no registo permitem demonstrar o cumprimento das obrigações estabelecidas no RGPD.
3	O registo é regularmente atualizado.
4	A segurança e integridade do registo está assegurada.

REGISTO DE ATIVIDADES DE TRATAMENTO

O artigo 30.º do RGPD impõe a obrigação de registo das atividades de tratamento para os responsáveis pelo tratamento e para os subcontratantes, sendo o conteúdo dos registos distinto consoante para cada uma destas funções, razão pela qual se devem manter dois registos diferenciados.

Esta obrigação também se estende às organizações ou empresas com menos de 250 trabalhadores, sendo absolutamente excecionais as circunstâncias em que se aplica a derrogação prevista no artigo 30.º, n.º 5, do RGPD.

Os registos são efetuados por escrito, incluindo em formato eletrónico, e são facultados à CNPD a seu pedido.

A CNPD disponibiliza um modelo de registo que pode ser utilizado para o cumprimento desta obrigação e que pode ser obtido aqui.

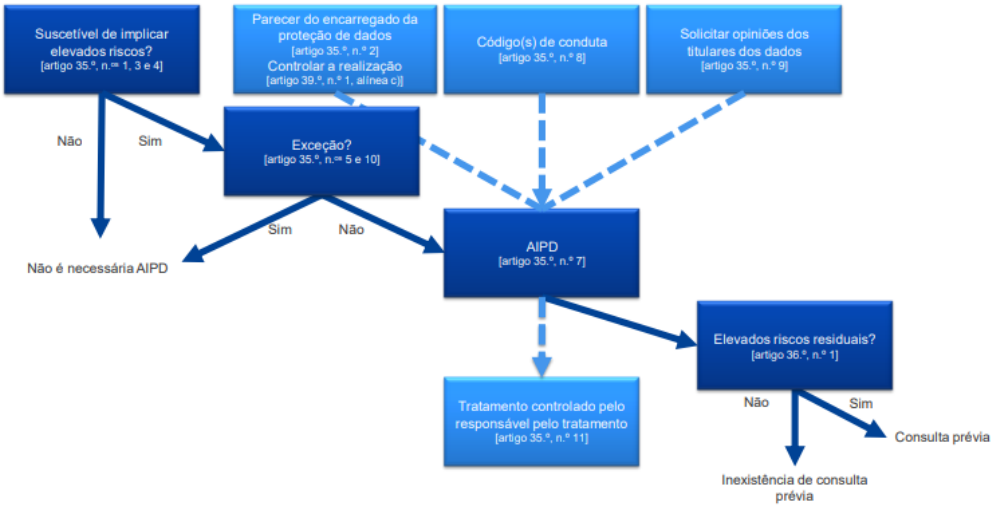
Elementos adicionais consultar CNPD

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

O artigo 35.º do RGPD introduz o conceito de Avaliação de Impacto sobre a Proteção de Dados (AIPD) que consiste num processo concebido para descrever o tratamento, avaliar a necessidade e a proporcionalidade desse tratamento, e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos.

As AIPD são, assim, um processo que visa estabelecer e demonstrar conformidade, sendo instrumentos importantes em matéria de responsabilização, permitindo aos responsáveis pelo tratamento não apenas cumprir os requisitos do RGPD, mas também demonstrar que foram tomadas as medidas adequadas para assegurar a conformidade com o regulamento.

Figura 1. Princípios básicos da AIPD no RGPD



Fonte: Grupo de Trabalho do Artigo 29.º para a Proteção de Dados

De acordo com o artigo 35.º, n.º 1, do RGPD só existe a obrigação de realizar uma AIPD quando o tratamento for «suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares», explicitando o n.º 3, do mesmo artigo, os seguintes exemplos:

- Avaliação sistemática e completa dos 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 relativamente à pessoa singular ou que a afetem significativamente de forma similar;
- Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º;
- Controlo sistemático de zonas acessíveis ao público em grande escala».

A CNPD, no âmbito dos seus poderes regulamentares, aprovou o Regulamento n.º 1/2018[10], em que elenca ainda os seguintes casos em que uma AIPD é obrigatória:

- Tratamento de informação decorrente da utilização de dispositivos eletrónicos que transmitam, por redes de comunicação, dados pessoais relativos à saúde;
- Interconexão de dados pessoais ou tratamento que relacione dados pessoais previstos no artigo 9.º, n.º 1, ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal;
- Tratamento de dados pessoais previstos no artigo 9.º, n.º 1, ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal com base em recolha indireta dos mesmos, quando não seja possível ou exequível assegurar o direito de informação nos termos do artigo 14.º, n.º 5, alínea *b)*, do RGPD;
- Tratamento de dados pessoais que implique ou consista na criação de perfis em grande escala;
- Tratamento de dados pessoais que permita rastrear a localização ou os comportamentos dos respetivos titulares (por exemplo, trabalhadores, clientes ou apenas transeuntes), que tenha como efeito a avaliação ou classificação destes, exceto quando o tratamento seja indispensável para a prestação de serviços requeridos especificamente pelos mesmos;
- Tratamento dos dados previstos no artigo 9.º, n.º 1, ou no artigo 10.º do RGPD ou ainda dos dados de natureza altamente pessoal para finalidade de arquivo de interesse público, investigação científica e histórica ou fins estatísticos, com exceção dos tratamentos previstos e regulados por lei que apresente garantias adequadas dos direitos dos titulares;
- Tratamento de dados biométricos para identificação inequívoca dos seus titulares, quando estes sejam pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados;
- Tratamento de dados genéticos de pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados;
- Tratamento de dados pessoais previstos no artigo 9.º, n.º 1, ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal, com utilização de novas tecnologias ou nova utilização de tecnologias já existentes.

Como menciona GRAÇA CANTO MONIZ[11], o Grupo de Trabalho do Artigo 29.º para a Proteção de Dados definiu nove critérios para aferir se o tratamento é «*suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares*»:

1. Avaliação ou classificação de aspetos relacionados com o desempenho profissional, situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados;

1. Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar;

2. Controlo sistemático;

3. Dados sensíveis ou dados de natureza altamente pessoal;

[10] Regulamento n.º 798/2018, publicado no Diário da República n.º 231/2018, 2.ª Série, de 30 de novembro.
[11] *Manual de Introdução à Proteção de Dados Pessoais*, Coimbra: Almedina, 2023.

4. Dados tratados em grande escala;

5. Correspondências ou combinar conjuntos de dados[12];

6. Dados relativos a titulares de dados vulneráveis;

7. Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais[13];

8. Quando o próprio tratamento impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato[14].

Os resultados da AIPD deverão ser tidos em conta na determinação das medidas que deverão ser tomadas para comprovar que o tratamento de dados pessoais é feito em conformidade com o RGPD.

Quando a avaliação de impacto indicar que o tratamento de dados que se pretende efetuar, apesar das medidas mitigadoras a adotar, resulta ainda num elevado risco para os direitos e liberdades dos indivíduos, o responsável pelo tratamento submete o tratamento de dados em causa a consulta prévia da CNPD (cf. artigo 36.º do RGPD). O que deverá ocorrer, ainda, quando se esteja no domínio da prevenção, deteção e investigação criminal ou repressão de infrações penais, nos termos do artigo 30.º, n.º 1, da Lei n.º 59/2019, de 8 de agosto.

Os anexos 1 e 2 apresentam listas de exemplos de tratamento relativamente aos quais se deve exigir, ou não, a realização de uma AIPD.

Elementos adicionais consultar Grupo de Trabalho do Artigo 29.º para a Proteção de Dados

[12] 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.
[13] Como por exemplo a impressão digital ou o reconhecimento facial.
[14] Por exemplo, quando um banco seleciona os seus clientes a partir de uma base de dados de referências de crédito para decidir se lhes atribui ou não um empréstimo.

ANEXO 1 - EXEMPLOS DE EXIGÊNCIA DE AIPD

Exemplos de tratamento	Critérios pertinentes possíveis
Um hospital que faz o tratamento dos dados genéticos e de saúde dos seus doentes (sistema de informação do hospital).	- Dados sensíveis ou dados de natureza altamente pessoal. - Dados relativos a titulares de dados vulneráveis. - Dados tratados em grande escala.
Utilização de um sistema de câmaras para controlar o comportamento dos condutores nas autoestradas. O responsável pelo tratamento pretende utilizar um sistema inteligente de análise através de vídeo para selecionar carros específicos e reconhecer automaticamente as matrículas.	- Controlo sistemático. - Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais.
Uma empresa que controle sistematicamente as atividades dos seus empregados, incluindo o controlo dos computadores, da atividade *internet*, etc. dos seus empregados.	- Controlo sistemático. - Dados relativos a titulares de dados vulneráveis.
Recolha de dados públicos das redes sociais para elaborar perfis.	- Avaliação ou classificação. - Dados tratados em grande escala. - Estabelecer correspondências ou combinar conjuntos de dados. - Dados sensíveis ou dados de natureza altamente pessoal.
Uma instituição que crie uma base de dados a nível nacional de notação de crédito ou fraude.	- Avaliação ou classificação. - Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar. - Impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato. - Dados sensíveis ou dados de natureza altamente pessoal.
Conservação para fins de arquivo de dados pessoais sensíveis pseudonimizados relativos a titulares de dados vulneráveis que tenham participado em projetos de investigação ou ensaios clínicos.	- Dados sensíveis. - Dados relativos a titulares de dados vulneráveis. - Impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato.

Fonte: Grupo de Trabalho do Artigo 29.º para a Proteção de Dados

ANEXO 2 - EXEMPLOS DE NÃO EXIGÊNCIA DE AIPD

Exemplos de tratamento	Critérios pertinentes possíveis
Tratamento de «*dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado*» (considerando 91).	- Dados sensíveis ou dados de natureza altamente pessoal. - Dados relativos a titulares de dados vulneráveis.
Revista em linha que utilize uma lista de endereços de correio eletrónico para enviar fascículos diários genéricos da revista para os seus subscritores.	- Dados tratados em grande escala.
Um sítio *web* de comércio em linha que mostre anúncios de peças de automóveis antigos envolvendo a utilização limitada de perfis com base nos itens visualizados ou comprados no seu próprio sítio *web*.	- Avaliação ou classificação.

Fonte: Grupo de Trabalho do Artigo 29.º para a Proteção de Dados

LIGAÇÕES ÚTEIS

Comissão Nacional de Proteção de Dados (CNPD)

Autoridade Europeia para a Proteção de Dados

Orientações Práticas para a Administração Pública sobre o RGPD

Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD)

Orientações sobre os encarregados da proteção de dados (EPD)

RGPD - Proposta de plano de ação em 5 fases (PCM)

Secretaria-Geral da Presidência do Conselho de Ministros (RGPD)

10 Medidas para Preparar a Aplicação do RGPD (Documento disponibilizado pela Comissão Nacional de Proteção de Dados)

PRESIDÊNCIA DO CONSELHO DE MINISTROS
Secretaria-Geral