Regulamento Geral de Proteção de Dados Pessoais (RGPD)

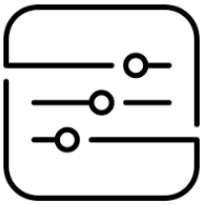
Proposta de plano de ação em 5 fases:

Designar

um encarregado de proteção de dados

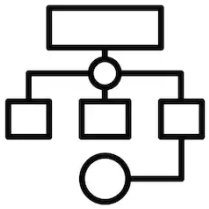
Mapear

os dados pessoais objeto de tratamento



Priorizar

as ações a desenvolver



Organizar

os processos internos

Documentar

a conformidade com o RGPD

Designar um encarregado de proteção de dados

O que fazer?

- 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 Comissão Nacional de Proteção de Dados) a identificação do encarregado e os seus contactos profissionais: morada, telefone e correio eletrónico.

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 autoridade nacional de controlo (a 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.

As entidades públicas, independentemente da sua dimensão e do tipo de dados pessoais que tratam, estão obrigadas a nomear um EPD (cf. o n.º 1 do artigo 37.º 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.

Checklist para esta etapa:

	Foi nomeado um EPD com as funções de apoiar a implementação e a conformidade com o RGPD
	Foram publicitados os seus contactos no sítio institucional
	Foi comunicada a designação e os contactos do EPD à Autoridade Nacional de Controlo
	Estão asseguradas as condições necessárias para o EPD poder desenvolver de forma independente e eficaz as tarefas que lhe incumbem

Mapear os dados pessoais objeto de tratamento

O que fazer?

Levar a cabo um levantamento, completo e prévio, de todos os dados pessoais tratados pela entidade.

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

QUEM?

- Identificação do responsável pelo tratamento de dados pessoais;
- Identificação do responsável pelos serviços que processam os dados;
- Identificação do subcontratante (caso exista).

O QUÊ?

- 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).

PORQUÊ?

- Indicação da(s) finalidade(s) para a(s) qual(is) os dados pessoais são recolhidos e tratados (*por exemplo: gestão de recursos humanos*).

ONDE?

- 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.

ATÉ QUANDO?

- Determinação do prazo de conservação dos dados.

COMO?

- Especificação das medidas de segurança implementadas (a nível técnico e organizativo) para minimizar os riscos de violações de dados.

Checklist para esta etapa:

	Foram identificados todos os serviços e entidades que processam dados pessoais
	Foram identificados os tipos de dados pessoais objeto de tratamento, incluindo os dados sensíveis (quando seja o caso)
	Foi estabelecida a listagem dos principais processos de tratamento e da(s) finalidade(s) a que se destinam
	Foram identificados eventuais fluxos de dados, indicando a sua origem e o destino
	Foram identificados todos os locais onde os dados pessoais se encontram arquivados
	Foi estabelecido por quanto tempo esses mesmos dados devem ser mantidos

Priorizar as ações a desenvolver

O que fazer?

Avaliar a 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.

- **Identificar** o fundamento de licitude que permite o tratamento dos dados (*por exemplo, o consentimento do titular, a necessidade do tratamento para o cumprimento de um contrato ou de uma obrigação legal*);

    - 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;
    - Importante: de acordo com o RGPD, 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.

- **Especificar** desde o início 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.

Checklist para esta etapa:

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

Organizar os processos internos

O que fazer?

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. Em concreto, visa-se:

- A **proteção de dados desde a conceção e por defeito**, através da implementação de medidas técnicas (por exemplo, fortalecendo o *software* contra intromissões informáticas) e organizativas (por exemplo, estabelecendo normas de acesso diferenciado) 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 autoridade nacional de controlo (a 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.

Checklist para esta etapa:

	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
	Os principais riscos de segurança foram identificados e devidamente acautelados
	Foram elaborados planos de contingência que permitem saber o que fazer e quem contatar em caso de incidente de segurança
	A informação sobre o tratamento de dados é disponibilizada de forma clara e concisa
	Estão instaladas plataformas/canais de comunicação que permitem aos titulares dos dados exercer os seus direitos
	Foi elaborado um plano de formação e sensibilização dos trabalhadores

Documentar a conformidade com o RGPD

O que fazer?

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 União Europeia (quando existam).

2) **Relativamente aos dados pessoais:**

- Os dados em causa;
- A indicação do fundamento 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.

Nota: 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 esta etapa:

	A entidade documenta de forma sistemática as atividades de tratamento desenvolvidas
	As informações incluídas no registo permitem demonstrar o cumprimento das obrigações estabelecidas no RGPD
	O registo é regularmente atualizado
	A segurança e integridade do registo está assegurada