Orientações Práticas para a Administração Pública sobre o Regulamento Geral de Proteção de Dados (RGPD)

(Regulamento UE 2016/679, de 27 de abril)

Índice

1- **Introdução**

2- **Conceitos-chave:**

- **Dados pessoais**
- **Tratamento de dados**
- **Responsável pelo tratamento**
- **Subcontratante**

3- **Aplicação do RGPD:**

- **Princípios relativos ao tratamento de dados pessoais**
- **Fundamentos de licitude do tratamento**
- **Direitos dos titulares de dados**
- **Obrigações do responsável pelo tratamento**

4- **Síntese de medidas a adotar**

1. Introdução:

O Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral de Proteção de Dados – RGPD) aplica-se em Portugal e nos demais Estados-Membros da União Europeia a partir de 25 de maio de 2018.

O RGPD contém muitos conceitos, princípios e mecanismos semelhantes aos da Lei da Proteção de Dados Pessoais – Lei n.º 67/98, de 26 de outubro. Todavia, modifica o paradigma: a obrigação geral de notificação prévia à Comissão Nacional de Proteção de Dados (CNPD) foi suprimida, tendo sido substituída por uma maior responsabilização daqueles que procedem ao tratamento de dados pessoais.

Consagra-se, assim, um princípio de responsabilidade (pro)ativa: cabe ao responsável pelo tratamento de dados pessoais demonstrar que, em todas as suas fases, esse tratamento obedece ao Regulamento.

Este documento pretende ser um guia rápido de aplicação do RGPD no âmbito da Administração Pública, elencando as principais obrigações que lhe incumbem em matéria de proteção de dados pessoais e propondo medidas a implementar.

2. Conceitos-Chave

DADOS PESSOAIS

Qualquer informação relativa a pessoas singulares que as identifique ou as torne identificáveis.

Exemplos:

- O nome;
- Os números de identificação;
- A morada;
- O telefone;
- O endereço de correio eletrónico;
- O estado civil;
- O identificador de cliente da Via Verde;
- 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.

O RGPD prevê ainda as seguintes categorias de **dados sensíveis, que não podem ser objeto de tratamento a não ser em casos excecionais**:

- A origem racial ou étnica;
- As opiniões políticas;
- As convicções religiosas ou filosóficas;

- A filiação sindical;
- Os dados genéticos;
- Os dados biométricos que permitam identificar uma pessoa de forma inequívoca (por exemplo, impressões digitais ou imagens faciais);
- Os dados relativos à saúde ou dados relativos à vida sexual (por exemplo, dados relativos a consultas médicas ou baixas médicas);
- Os dados relativos à orientação sexual.

TRATAMENTO DE DADOS

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

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.

Exemplos 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

É a entidade que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais.

SUBCONTRATANTE

É a entidade que trata os dados pessoais por conta do responsável pelo tratamento.

Exemplos:

- uma empresa que procede ao processamento de salários;
- uma empresa que armazena o arquivo de processos administrativos de uma entidade pública.

TERCEIRO

Não é responsável pelo tratamento, nem subcontratante, mas, sob a autoridade direta destes, está autorizado a tratar os dados pessoais ou a aceder aos mesmos.

Exemplos:

- 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.

ENCARREGADO DE PROTEÇÃO DE DADOS

Trabalhador em funções públicas ou consultor externo que tem como função principal informar e aconselhar quanto ao cumprimento das obrigações relevantes em matéria de proteção de dados.

3. APLICAÇÃO DO RGPD

Princípios relativos ao tratamento de dados pessoais

- **Princípio da licitude**

O tratamento dos dados pessoais deve assentar numa das causas de licitude do tratamento previstas no artigo 6.º do RGPD (cfr. página 8).

- **Princípio da finalidade**

Os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas, e não podem ser tratados posteriormente de uma forma incompatível com essas finalidades.

- **Princípio da minimização**

Só devem ser tratados dados que sejam adequados, pertinentes e necessários à finalidade estabelecida.

- **Princípio da exatidão**

Os dados devem ser exatos, e atualizados sempre que necessário. Os dados inexatos devem ser apagados ou retificados sem demora.

- **Princípio da limitação da conservação**

Os dados devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período estritamente necessário para as finalidades para as quais são tratados.

- **Princípio da integralidade e confidencialidade**

Os dados devem ser tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental.

Fundamentos de licitude do tratamento

Como regra, o RGPD mantém os fundamentos da licitude de tratamento de dados pessoais previstos na Diretiva 95/46/CE, de 24 de outubro de 1995, que são os seguintes:

- **Consentimento;**
- **Relação contratual;**
- **Cumprimento de obrigação legal pelo responsável;**
- **Interesses vitais do titular ou de terceiro;**
- **Interesse público e exercício de poderes públicos;**
- **Interesses legítimos do responsável e de terceiros.**

ATENÇÃO: ***a entidade pública deve documentar e identificar expressamente o fundamento da licitude do tratamento, e a finalidade a que se destina.***

Consentimento: o responsável pelo tratamento deve obter do titular dos dados uma declaração de vontade livre, informada, explícita e inequívoca.

ATENÇÃO*: *o consentimento exige um ato expresso e positivo. O pedido de consentimento deve ser apresentado de modo inteligível e de fácil acesso, e numa linguagem clara e simples. Não são admitidos consentimentos tácitos nem opções pré-validadas. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento.

Relação contratual: os dados são necessários para a execução de um contrato no qual o titular é parte.

Exemplo: para pagar o vencimento aos trabalhadores, os serviços têm de dispor de dados pessoais seus como o NIF e um número de conta bancária. Não é necessário o consentimento para o tratamento desses dados.

Obrigação legal: os dados são necessários para o cumprimento de uma obrigação legal a que o responsável pelo tratamento está sujeito.

Exemplo: uma norma que determine que devem ser identificados todos os trabalhadores da Administração direta e indireta do Estado que tenham formação jurídica. Não é necessário o consentimento para o tratamento desses dados.

Interesse público: os dados são necessários ao exercício da autoridade pública ou de funções de interesse público.

Exemplo: uma investigação pública ou averiguações que envolvam dados pessoais.

DIREITOS DOS TITULARES DOS DADOS

A Administração Pública deve (i) **fornecer aos titulares de dados todas as informações a que estes têm direito, de forma clara e concisa**, e (ii) **facilitar o exercício dos direitos consagrados no RGPD** por aqueles que deles beneficiam.

- **TRANSPARÊNCIA E INFORMAÇÃO**

As entidades públicas que procedam à recolha de dados pessoais devem prestar as seguintes informações ao titular dos dados:

- Quem é o responsável pelo tratamento e respetivos contactos;
- Quem é o encarregado da proteção de dados e respetivos contactos;
- Quais as finalidades do tratamento em causa;
- O prazo de conservação dos dados ou, se tal não for possível, os critérios para definir tal prazo;
- Se o tratamento se basear no consentimento, a existência do direito de retirar tal consentimento;
- Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;
- Que o titular dos dados tem o direito de apresentar queixa junto da Comissão Nacional de Proteção de Dados.

Quando os dados pessoais não são recolhidos junto do titular, devem ainda ser prestadas as seguintes informações adicionais:

  - Os destinatários ou categorias de destinatários dos dados pessoais, se houver;
  - A origem dos dados;
  - As categorias dos dados.

***ATENÇÃO*: a prestação de informação pelo responsável ao titular dos dados deve ser registada, de molde a garantir a prova dessa prestação por parte do responsável.**

Não é exigível ao responsável pelo tratamento a prestação da informação ao titular dos dados quando:

- O titular dos dados já disponha dessa informação;
- Os dados solicitados digam respeito a um terceiro;
- O cumprimento dessa obrigação implique um esforço desproporcionado para o responsável pelo tratamento;
- A obtenção dos dados, bem como a sua transmissão, se encontre expressamente prevista no Direito da União Europeia ou em legislação nacional;
- Os dados revistam natureza confidencial ou secreta, em decorrência do cumprimento de uma obrigação legal.

- **DIREITO DE ACESSO**

O direito de acesso consiste na faculdade de o titular dos dados obter do responsável pelo tratamento as seguintes informações:

- Quais os fins do tratamento;
- Quais os dados pessoais em causa;
- Quais os destinatários dos dados;
- Qual o prazo de conservação dos dados;
- Se os dados não tiverem sido recolhidos junto do titular, qual a origem desses dados;
- Qual a forma de exigir a retificação ou o apagamento dos dados.

Para facilitar o exercício do direito de acesso, o responsável pelo tratamento deve disponibilizar publicamente os contactos do Encarregado de Proteção de Dados.

ATENÇÃO*: *É reconhecido o direito de o titular dos dados obter uma cópia dos dados pessoais objeto do tratamento. Poderá ser oferecido ao interessado o acesso remoto a um sistema seguro que permita o acesso direto aos seus dados.

- **DIREITO DE RETIFICAÇÃO**

O titular dos dados pode exigir a retificação/alteração dos dados que lhe digam respeito e que não correspondam à verdade. Tem, também, o direito de exigir que os seus dados sejam completados, caso se encontrem incompletos.

***ATENÇÃO*: *a retificação/alteração deve fazer-se no mais curto período de tempo possível*.**

- **DIREITO AO APAGAMENTO (direito a ser esquecido)**

O titular dos dados tem o direito de exigir o apagamento de dados, nomeadamente, nas seguintes situações:

- Quando os dados pessoais deixem de ser necessários para a finalidade que motivou a sua recolha;
- Quando o titular retire o consentimento em que se baseia o tratamento dos dados, nos casos em que a lei o permite;
- Quando os dados tenham sido tratados ilicitamente.

ATENÇÃO**: **O exercício do direito ao apagamento não pode afetar, designadamente:

- ***O cumprimento de obrigações legais;***
- ***Razões de interesse público na área da saúde pública;***
- ***O tratamento para fins de arquivo público, investigação científica e histórica e fins estatísticos;***
- ***O exercício de direitos em processos judiciais.***

- **DIREITO DE PORTABILIDADE/TRANSMISSÃO DE DADOS PESSOAIS**

Sempre que o tratamento seja informatizado e feito com base no consentimento, o titular dos dados tem:

- o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática;
- o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável inicial o possa impedir;
- o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.

Exemplo #1: uma pessoa dirige-se a um hospital e solicita os exames médicos que realizou nesse hospital. O hospital deve fornecer-lhe tais exames, podendo nalguns casos exigir um pagamento que cubra o custo do material.

Exemplo #2: uma pessoa dirige-se a um hospital e solicita que os exames médicos que realizou nesse hospital sejam transmitidos a uma outra unidade hospitalar ou a um médico em particular. O hospital deve transmitir esses dados.

***ATENÇÃO*: O direito de portabilidade não se aplica:**

- ***aos dados de terceiros que tenham sido facultados pelo titular ao responsável;***
- ***no caso de o interessado solicitar a portabilidade de dados que tenham sido facultados ao responsável por terceiro.***

- **LIMITAÇÃO DO TRATAMENTO**

O titular dos dados pode exigir junto do responsável pelo tratamento que o tratamento seja limitado a determinados dados.

- **DIREITO DE OPOSIÇÃO**

O titular dos dados pode opor-se a qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar dados pessoais para avaliar e determinar características do titular dos dados, designadamente para prever aspetos relacionados com a sua situação económica, tendências comportamentais, saúde e interesses (definições de perfis/*profiling*).

Quando seja exercido o direito de oposição, o responsável pelo tratamento deve cessar o tratamento, salvo se razões imperiosas e legítimas justificarem a prossecução desse tratamento.

- **DIREITO DE QUEIXA**

O titular dos dados tem o direito de apresentar queixa junto da Comissão Nacional de Proteção de Dados (CNPD), enquanto autoridade de controlo nacional.

- **DIREITO DE INDEMNIZAÇÃO**

Os titulares dos dados têm direito a ser indemnizados pelos danos que lhes sejam causados pela violação ou incumprimento do RGPD.

OBRIGAÇÕES DO RESPONSÁVEL PELO TRATAMENTO

Levantamento de Dados

Todos os responsáveis pelo tratamento devem proceder ao diagnóstico e à inventariação das operações de tratamento de dados, incluindo a inventariação dos sistemas informáticos que tratam dados pessoais. Exemplo:

1) Que dados possuo?
2) Que condição de licitude me permite tratá-los?
3) Para que finalidade são recolhidos?
4) As operações de tratamento respeitam os princípios consagrados no artigo 5.º do RGPD?
5) Quem é que recolhe e trata os dados?

6) De que forma estou a documentar a conformidade com as regras do RGPD?

7) Os contratos assinados com subcontratantes (quando existam) oferecem garantias de respeito pelo RGPD?

8) Onde é que os dados são conservados, e como é que são protegidos?

9) Em caso de quebra de segurança, quais os procedimentos definidos?

10) Que mecanismos estão implementados para garantir a prestação de informações aos titulares dos dados e facilitar o efetivo exercício dos seus direitos?

Registo

O responsável do tratamento e o subcontratante devem proceder ao registo das operações de tratamento de dados, do qual conste:

- Nome e contactos do responsável;
- Finalidades do tratamento;
- Descrição das categorias de titulares dos dados e das categorias dos dados;
- Categorias dos destinatários;
- Transferência de dados para países terceiros ou organizações internacionais;
- Se possível, prazos de conservação;
- Se possível, uma descrição das medidas técnicas e organizativas no domínio da segurança.

A obrigação de registo ***não existe para entidades com menos de 250 trabalhadores****, a menos que o tratamento:*

- *Possa implicar um risco para os direitos, liberdades e garantias do titular dos dados;*
- *Não seja ocasional;*
- *Abranja as categorias especiais de dados (dados sensíveis) ou dados pessoais relativos a condenações penais e infrações.*

Segurança dos dados

Nas entidades públicas, os responsáveis devem promover medidas técnicas e organizativas que garantam a segurança dos dados pessoais, designadamente:

- Devem ser implementados os requisitos técnicos mínimos das redes e sistemas de informação que constam do anexo à Resolução do Conselho de Ministros n.º 41/2018, de 28 de março, **até 1.10.2019**;
- Deve ser instituído um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas, de modo a garantir a segurança do tratamento;
- Devem ser reavaliadas as permissões de acesso a dados pessoais, sendo apenas dadas a quem necessita efetivamente de ter acesso aos mesmos para o desempenho das suas funções;
- Deve ser assegurada formação a quem procede ao tratamento de dados pessoais;

- Devem ser implementadas medidas de segurança dos dados pessoais quando estes se encontrem em suporte físico*, v.g.*, dossiers ou pastas, que devem ser guardados em armários fechados à chave.

Encarregado de proteção de dados

A designação de EPD 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 encarregado de proteção de dados exerce a sua atividade com independência, não podendo ser prejudicado pelo exercício das suas funções.

São funções do Encarregado de Proteção de Dados:

- 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 obrigações constantes do RGPD e da lei estão a ser cumpridas;
- 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;
- Assegurar que, em todas as fases do tratamento, desde a recolha à destruição, são observados os princípios do registo e tratamento de dados

***ATENÇÃO**: o mesmo encarregado de proteção de dados pode ser designado para várias entidades públicas. A identidade e os contactos do encarregado da proteção de dados devem ser comunicados à CNPD e colocados no sítio eletrónico da entidade pública.*

Avaliação de impacto

Quando estejam em causa tratamentos que representem um elevado nível de risco para os direitos, liberdades e garantias do cidadão, deve ser feita uma avaliação de impacto e devem ser definidas medidas específicas de atenuação, a adotar antes do início do tratamento e durante o período em que este se encontre em curso.

São considerados tratamentos de elevado risco os que implicam:

- Recolha e tratamento de dados sensíveis;
- Tratamento de elevado volume de dados;
- Definição de perfis;
- Cruzamento de dados obtidos junto do titular com dados recolhidos de outras fontes;
- Utilização de técnicas de análise em massa de dados;
- Dados recolhidos através de técnicas invasivas da privacidade, como por exemplo videovigilância, geolocalização, etc.

Se, na sequência de uma avaliação de impacto, resultar a identificação de um risco elevado, e caso não estejam definidas medidas específicas de atenuação desse risco, deve o responsável pelo tratamento promover a consulta prévia junto da CNPD.

ATENÇÃO: a CNPD elabora e torna pública uma lista dos tipos de operações sujeitas a avaliação de impacto.

Obrigação de notificação de violações de dados pessoais

As violações de dados pessoais traduzem-se em quebras de segurança que provocam a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais. Por exemplo: um trabalhador perde o portátil que contém dados pessoais.

***ATENÇÃO:* em caso de violação de dados pessoais, o responsável pelo tratamento deve notificar a CNPD no prazo de 72 horas após ter tido conhecimento dela.**

A notificação deve:

- Descrever a natureza da violação dos dados pessoais;
- Comunicar o nome e os contactos do EPD;
- Descrever as consequências prováveis da violação de dados pessoais;
- Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais.

O responsável pelo tratamento deve registar as violações de dados pessoais, bem como os factos com elas relacionados, os respetivos efeitos e a medida de reparação adotada.

ATENÇÃO: quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos, liberdades e garantias de pessoas singulares, **o responsável pelo tratamento deve comunicar a violação de dados pessoais ao titular dos dados** sem demora injustificada, em linguagem clara e simples.

A obrigação de comunicação ao titular dos dados não existe se se verificar um dos seguintes casos:

- O responsável pelo tratamento tiver aplicado aos dados pessoais afetados medidas de proteção adequadas, especialmente medidas que tornem os dados pessoais incompreensíveis (e.g., cifragem);
- O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o risco não se concretizará; ou
- A comunicação implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante.

4. Síntese de medidas a adotar

- **Designação de um Encarregado de Proteção de Dados.**
- **Criação de um sistema de diagnóstico e inventariação das operações de tratamento (centralidade, necessidade e pertinência dos dados), com identificação da base jurídica que legitima os tratamentos.**
- **Adoção de um sistema de segurança dos dados que garanta a proteção dos dados em todas as fases do tratamento.**
- **Implementação de um registo das atividades de tratamento.**
- **Revisão dos contratos com os subcontratantes.**
- **Criação de um registo de violações de dados pessoais.**
- **Criação de um canal de comunicação dedicado ao exercício dos direitos dos titulares dos dados (por exemplo, um sítio eletrónico).**
- **Criação de um registo de pedidos dos titulares.**
- **Garantir a formação dos funcionários que trabalham com dados pessoais.**