FAQ sobre o Regulamento Geral de Proteção de Dados (RGPD)

1. O que é o RGPD?

O **RGPD** (Regulamento Geral de Proteção de Dados) é uma lei da União Europeia (UE) relativa à proteção de dados e à privacidade, que entrou em vigor a 25 de maio de 2018. O seu principal objetivo é **harmonizar as leis de privacidade de dados em toda a Europa**, protegendo os dados pessoais de todos os cidadãos da UE e do Espaço Económico Europeu (EEE), e redefinindo a forma como as organizações abordam a privacidade dos dados.

2. Qual o objetivo principal do RGPD?

O RGPD visa:

- **Capacitar os indivíduos:** Dando-lhes mais controlo sobre os seus dados pessoais.
- **Simplificar o ambiente regulatório:** Para as empresas, ao unificar as leis de proteção de dados em toda a UE.
- **Aumentar a responsabilização:** Impondo maiores obrigações às organizações que tratam dados.
- **Proteger o direito fundamental à privacidade:** Num mundo cada vez mais digitalizado.

3. A quem se aplica o RGPD?

O RGPD aplica-se a:

- **Qualquer organização que trate dados pessoais de indivíduos na UE/EEE**, independentemente de onde a organização esteja localizada. Isto significa que uma empresa fora da UE que ofereça bens ou serviços a cidadãos da UE ou monitorize o seu comportamento deve cumprir o RGPD.
- **Todas as organizações dentro da UE/EEE** que tratem dados pessoais, sejam elas entidades públicas ou privadas, grandes ou pequenas.

4. O que são "dados pessoais" segundo o RGPD?

Dados pessoais são qualquer informação relativa a uma pessoa singular identificada ou identificável. Isto inclui:

- **Identificadores diretos:** Nome, morada, endereço de correio eletrónico (e-mail), número de identificação civil/fiscal, dados bancários.
- **Identificadores indiretos:** Dados de localização, endereço IP, *cookies* (quando associados a uma pessoa), dados de saúde, dados genéticos, dados biométricos, informações sobre origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, etc.

5. Quais são os principais direitos dos indivíduos (titulares dos dados) ao abrigo do RGPD?

O RGPD confere aos indivíduos (titulares dos dados) uma série de direitos importantes sobre os seus dados, incluindo:

- **Direito de Acesso:** Saber se os seus dados estão a ser tratados e ter acesso a eles.
- **Direito de Retificação:** Corrigir dados incorretos ou incompletos.
- **Direito ao Apagamento ("Direito a Ser Esquecido"):** Solicitar a eliminação dos seus dados em determinadas circunstâncias.
- **Direito à Limitação do Tratamento:** Limitar a forma como os seus dados são utilizados.
- **Direito de Portabilidade dos Dados:** Receber os seus dados num formato estruturado, de uso corrente e leitura automática, e transmiti-los a outro responsável pelo tratamento.
- **Direito de Oposição:** Opor-se ao tratamento dos seus dados para fins específicos.
- **Direito a Não Ficar Sujeito a Decisões Automatizadas:** Opor-se a decisões baseadas unicamente no tratamento automatizado, incluindo a definição de perfis, que produzam efeitos jurídicos ou que o afetem significativamente.

6. O que é o consentimento no RGPD?

O **consentimento** é uma das bases legais para o tratamento de dados pessoais. Para ser válido, o consentimento deve ser:

- **Livremente dado:** Sem coerção.
- **Específico:** Para uma finalidade clara.
- **Informado:** O indivíduo deve saber o que está a consentir.
- **Inequívoco:** Uma ação afirmativa clara (não pode ser implícito ou por omissão).
- **Facilmente revogável:** O indivíduo deve poder retirar o seu consentimento a qualquer momento.

7. O que acontece em caso de violação de dados pessoais?

Uma **violação de dados pessoais** é um incidente de segurança que resulta na destruição, perda, alteração, divulgação não autorizada ou acesso a dados pessoais. O RGPD exige que as organizações notifiquem a autoridade de controlo competente (em Portugal, a **Comissão Nacional de Proteção de Dados - CNPD**) no prazo de **72 horas** após terem tido conhecimento da violação, se houver um risco para os direitos e liberdades dos indivíduos. Em casos de alto risco, os próprios titulares dos dados também devem ser informados.

8. O que é um Encarregado de Proteção de Dados (EPD)?

Um **Encarregado de Proteção de Dados (EPD - Data Protection Officer, DPO)** é uma pessoa responsável por garantir a conformidade de uma organização com o RGPD. A nomeação de um EPD é obrigatória em determinadas situações, como para:

- Autoridades e organismos públicos.
- Empresas cujas atividades principais consistam em operações de tratamento que exijam um controlo regular e sistemático de grande escala de titulares de dados.
- Empresas cujas atividades principais consistam no tratamento em grande escala de categorias especiais de dados pessoais (dados sensíveis) ou de dados relacionados com condenações penais e infrações.

9. Quais as consequências do não cumprimento do RGPD?

O não cumprimento do RGPD pode resultar em **coimas significativas**, que podem atingir até:

- **20 milhões de euros** ou
- **4% do volume de negócios anual global** da empresa (o que for mais elevado).

Além das coimas, o não cumprimento pode levar a danos reputacionais, perda de confiança dos clientes e ações judiciais por parte dos indivíduos afetados.

10. O RGPD aplica-se a pequenas e médias empresas (PMEs)?

Sim, o RGPD aplica-se a todas as empresas e organizações que tratam dados pessoais, independentemente do seu tamanho. No entanto, existem algumas exceções para PMEs, como a dispensa da obrigação de manter registos de atividades de tratamento em certas condições, mas os princípios e direitos fundamentais do RGPD permanecem aplicáveis.