

RGPD _____

**Regulamento Geral
de Proteção de Dados**



Índice

RGPD Simplificado.....	3
O que fazer?	5
Guia Prático de Implementação:.....	8

RGPD Simplificado

Essencialmente o RGPD traduz-se num conjunto de medidas que têm como objetivo aumentar a transparência na utilização dos dados pessoais.

Aumentam também os direitos dos utilizadores relativamente à forma como os seus dados são tratados e armazenados.

Esses direitos são estendidos a todos os cidadãos da UE independentemente da localização das empresas que armazenem ou tratem esses dados.

Esses direitos distribuem-se da seguinte forma:

- Consentimento
- Consulta
- Esquecimento
- Portabilidade
- Oposição
- Controlo de acessos
- Registo de tratamentos
- Comunicação obrigatória de roubo de dados

O primeiro passo a tomar é identificar o que são dados pessoais e onde estão presentes:

- Estes dados referem-se apenas a utilizadores particulares, não se aplicam a empresas

Exemplo:

e-mail,

nº telemóvel,

NIF

Tipicamente será este tipo de informação que uma PME tem sobre os seus clientes ou contactos particulares.

O passo seguinte é identificar qual o trabalho a executar para a empresa estar em condições de responder aos novos direitos que entram em vigor a 25 de Maio de 2018.

Apesar de ter assistido a vários seminários que começam logo com o tema das multas – o texto original da UE tem uma abordagem mais educativa do que repressiva.

Se olharmos para a dimensão máxima das multas – **20 M € ou 4% da faturação** rapidamente percebemos que o objetivo é permitir sancionar grande empresas como a Facebook, Google, Amazon e **similares que, com multas “normais” não** seriam minimamente afetadas.

Dito isto devem as PMEs olhar para esta legislação como uma oportunidade para validar dados pessoais que têm nos seus sistemas e fazer deles uma fonte de informação útil para a organização, mantendo sempre um dever de confidencialidade, respeito e zelo no tratamento dessa informação.

O que fazer?

1. Definição do plano de implementação do RGPD

A Gestão de Topo deve começar por definir um plano de ação estratégico para implementar o RGPD, que envolva todas as áreas de negócio da empresa. No plano de ação deve constar a identificação, avaliação e categorização de todos os dados pessoais que as organizações têm armazenados.

2. Envolvimento de toda a organização

Deve ser criado um programa interno de comunicação mobilizador, que envolva transversalmente toda a organização, informando e sensibilizando os colaboradores sobre a privacidade, as alterações ao RGPD e os riscos inerentes ao incumprimento.

3. Aconselhamento jurídico

O aconselhamento jurídico é uma peça fundamental para a implementação do RGPD sem sobressaltos. O consultor jurídico deve identificar os passos já implementados e os que estão em falta para que se cumpra o novo Regulamento Geral para a Proteção de Dados e não incorra em coimas. Este levantamento de necessidades é extremamente útil se necessitar de recorrer a um parceiro para implementar as alterações necessárias.

4. Nomeação de um Data Protection Officer

A figura do Data Protection Officer apresenta-se **como necessária aos “olhos” da lei** e deverá assumir as questões de conformidade de proteção de dados, reportando à Gestão da organização o trabalho desenvolvido e as ocorrências que possam deflagrar.

5. Metodologia Privacy By Design

Devem ser criados/adaptados processos e políticas para a proteção e tratamento dos dados, de acordo com uma metodologia de Privacy by Design, que facilite a monitorização e comunicação de eventos relacionados com os acessos a dados pessoais.

6. Encriptação e Pseudonização dos Dados

Reveja os procedimentos de segurança que garantam a salvaguarda dos dados sensíveis recorrendo a técnicas de encriptação e pseudonização.

7. Realização de Avaliações de Impacto de Proteção de Dados

A metodologia escolhida deve agilizar as avaliações, para que seja fácil avaliar o impacto da proteção de dados e eventuais falhas. As auditorias são fundamentais para garantir a conformidade.

8. Segurança da Informação

Devem ser implementados processos que permitam detetar, mitigar, reportar e investigar violação dos dados pessoais, mantendo sempre presente a questão da segurança.

9. Atualização da Política de Privacidade de Dados

A Política de Privacidade de Dados tem de ser revista e alterada de acordo com as novas obrigações definidas pelo novo Regulamento Geral para a Proteção de Dados.

10. Definição do Tratamento e Catalogação de Dados

Identificar, recolher e processar os dados, a sua base jurídica e a documentação da informação são essenciais para um correto tratamento dos dados. Mantenha uma lista atualizada de todos os Dados Pessoais à guarda da sua organização e a forma como o consentimento foi obtido. É essencial desenhar o ciclo de vida desde a recolha até à destruição dos Dados, que permita ter uma visão geral e segura de todo o processo.

11. Cumprimento dos direitos dos Titulares

Reveja todos os procedimentos para garantir a conformidade. Caso se justifique, a notificação de uma falha à Comissão Nacional para a Proteção de Dados e aos titulares dos dados, deve estar sempre presente nas obrigações das empresas.

12. Validação do cumprimento do RGPD por parte de fornecedores

Garanta que todos os fornecedores envolvidos no processamento de dados cumprem os requisitos do novo Regulamento Geral para a Proteção de Dados. Por exemplo, no caso da compra uma base de dados ou do outsourcing de tarefas deverá assegurar-se que a entidade subcontratada também cumpre o RGPD.

Guia Prático de Implementação:

1. Implementação de Sistemas de Segurança

- a. Firewall: proteção contra roubo de dados / perda de informação.
- b. Antivírus: proteção contra perda de dados.

2. Implementação controlo de acessos

- a. Redefinir acessos nos servidores/computadores.

3. Pedido de Consentimento

- a. Caso envie newsletters deve ser pedido o consentimento dos inscritos para a receção das mesmas.

4. Implementação PHC RGPD

- a. Este módulo faz o tratamento dos registos no software PHC.