



ABREU
ADVOGADOS

www.abreuadvogados.com



**Impacto e desafios
do Regulamento
Geral sobre Proteção
de Dados Pessoais**

Regulamento Geral de Proteção de Dados Pessoais

- **Revoga** a Diretiva de Proteção de Dados n.º 95/ 46/ CE, de 24 de outubro de 1995
 - **Uniformização**: legislação comum, directamente aplicável em toda a UE
 - Maior **alcance** – um novo âmbito de aplicação
 - Maior **mudança** nos últimos 20 anos
 - Mudança de **paradigma**
 - **Definição** mais ampla de dados pessoais
 - **Pote de ouro**
 - **Invasão**
 - Devolver o **controlo** ao titular
 - Maior **exposição**
 - Oportunidade de recuperar/ reforçar relação de **confiança**
 - Reorganizar/ **mapear** organização (orgânica)
 - Accountability: demonstrar **cumprimento** com o RGPD
 - Realização de um mapeamento dos fluxos de dados e de uma avaliação de risco dos tratamento realizados
- sistema de balcão único**

Regulamento Geral de Proteção de Dados Pessoais

Conceitos essenciais:

- Licitude, lealdade e transparência
- Necessidade
- Informação
- Responsabilidade ativa
- Ato positivo
- Novas tecnologias
- Risco (elevado; residual)
- Probabilidade, possibilidade, gravidade
- Documentação e registo
- Proteção de dados desde a conceção (*privacy by design*)
- Proteção de dados por defeito (*privacy by default*)
- Medidas técnicas e organizativas de segurança
- Sanções pecuniárias
- Adaptação/ revisão contínua
- Responsável pelo tratamento
- Subcontratante

Regulamento Geral de Proteção de Dados Pessoais

Os Novos Direitos dos Titulares dos Dados:

- **Direito ao Apagamento dos Dados (“direito a ser esquecido”)**

Direito que confere ao titular dos dados a possibilidade de requerer ao responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, tendo o responsável a obrigação de aceder a esse pedido.

- **Direito à limitação do tratamento**

Inserção de uma marcação nos dados pessoais conservados para impossibilitar futuras utilizações.

- **Direito de portabilidade de dados**

Direito que confere ao titular dos dados a possibilidade de requerer uma cópia dos próprios dados para transferi-los para outro responsável pelo tratamento.

Regulamento Geral de Proteção de Dados Pessoais

Os Novos Direitos dos Titulares dos Dados (Cont.) / Novas Obrigações Para os Responsáveis pelo Tratamento de Dados:

- **Obrigação de obtenção de Consentimento expresso e inequívoco**

“Manifestação de vontade, livre, específica, informada e explícita pelo qual o titular dos dados aceita que os dados pessoais que lhe dizem respeito sejam objeto de tratamento”, ou seja, o consentimento tácito é considerado inválido.

- ***“Privacy by Design” e “Privacy by Default”***

O responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a concepção e da proteção de dados por defeito: minimização do tratamento de dados pessoais; medidas técnicas e organizativas adequadas; pseudonimização de dados pessoais; encriptação; etc.

Regulamento Geral de Proteção de Dados Pessoais

Novas Obrigações Para os Responsáveis pelo Tratamento de Dados:

- Nomeação de um “*Data Protection Officer*” (Encarregado da Protecção de Dados)

Caso as actividades principais da empresa envolvam:

- a monitorização regular e sistemática de dados pessoais em grande escala;
- o tratamento em grande escala de categorias especiais de dados;

No caso de tratamento de dados pessoais efetuado por uma autoridade pública.

- “*Privacy Impact Assessment*” (Avaliação de Impacto de Protecção de Dados)

Se o tipo de tratamento de dados for susceptível de implicar um elevado risco para os direitos e liberdades dos titulares dos dados, deve ser efectuada uma avaliação de impacto das operações de tratamento a realizar.

Regulamento Geral de Proteção de Dados Pessoais

Novas Obrigações Para os Responsáveis pelo Tratamento de Dados (Cont.):

Comunicação de violação de dados pessoais

- Notificação de violações de dados pessoais à autoridade de controlo, sem demora justificada e, sempre que possível, até 72 horas após conhecimento da mesma;
- Comunicação de violações de dados pessoais ao titular dos dados, sem demora injustificada, quando a violação for susceptível de implicar elevado risco para os direitos e liberdades das pessoas singulares.

Regulamento Geral de Proteção de Dados Pessoais

Novas Obrigações para os Subcontratantes:

- Os subcontratantes terão obrigações e responsabilidade directas, o que significa que os subcontratantes podem ser directamente responsabilizados;
- O tratamento em regime subcontratação é regulado por contrato escrito que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objecto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do Responsável pelo tratamento.

Regulamento Geral de Proteção de Dados Pessoais

Fundamentos para a recolha (bases de licitude)

- Consentimento
- Execução de um contrato ou para diligências pré-contratuais
- Cumprimento de uma obrigação jurídica
- Defesa de interesses vitais do titular dos dados ou de outra pessoa singular
- Exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento
- Interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros

Regulamento Geral de Proteção de Dados Pessoais

Regime sancionatório agravado:

Dois níveis de coimas:

- até **10 milhões de euros** ou, no caso de uma empresa, até **2 % do seu volume de negócios** mundial anual (obrigações do responsável pelo tratamento e do subcontratante);
- até **20 milhões de euros** ou, no caso de uma empresa, até **4% do volume de negócios mundial** anual (princípios básicos do tratamento, direitos dos titulares dos dados, regras de transferência transfronteiriça).

Responsabilidade Penal a determinar por cada Estado-Membro.

A título exemplificativo, a autoridade nacional de controlo tem poderes de investigação (ordena que lhe sejam prestadas informações, realiza auditorias, etc.), **poderes de correção** (faz advertências, repreensões, ordena que o responsável pelo tratamento ou subcontratante satisfaça pedidos de exercício de direitos, impõe limitação temporária ou definitiva ao tratamento de dados/ proíbe, impõe coimas, etc.) e **poderes consultivos e de autorização** (aconselha, emite pareceres, emite certificações, etc.).

Regulamento Geral de Proteção de Dados Pessoais

- 1. Risco de incumprimento (coimas, sanções)**
- 2. Risco de investigação e litígios (perturbação, custos e recursos humanos)**
- 3. Risco de violação de dados e dano ao titular dos dados (indenizações)**
- 4. Risco ético (mesmo que seja legal, poderá não ser eticamente aceite)**
- 5. Risco de reputação (degradação de imagem/marca)**
- 6. Risco de negócio (incumprimento contratual, perda negócios)**
- 7. Risco Pessoal (responsabilidade criminal)**

Regulamento Geral de Proteção de Dados Pessoais

Implementação de um programa de conformidade:

- Não é algo que se possa fazer de uma só vez:
É necessário planejar – fazer – verificar – agir em conformidade (e voltar ao início...)
- Princípio da Responsabilidade (*Accountability*):
Capacidade de demonstrar o cumprimento.
- Aspectos legais são apenas uma parte da questão:
 1. Integração nos processos de negócios;
 2. Envolvimento de outros departamentos: TI, Conformidade, EPD/ DPO?;
 3. Envolvimento do órgão de gestão da sociedade.

Regulamento Geral de Proteção de Dados Pessoais

Resumo:

1. Alerta/ sensibilização/ processo contínuo
2. Inventário (autoconhecimento organizacional; identificação de *bugs*)
3. Informação aos titulares dos dados/ comunicar política de proteção de dados
4. Exercício dos direitos dos titulares (definir fluxos, prazos, interlocutores, confirmar procedimentos)
5. Identificar base de licitude
6. Privacidade desde o princípio (“Privacy by Design”)
7. Avaliação de impacto sobre a proteção de dados (“Privacy by Default”)
8. Violação de dados pessoais
9. Crianças
10. Encarregado de proteção de dados
11. Avaliar os sistemas de tecnologias da informação para verificar a capacidade de produzir informações detalhadas sobre as fontes, usos e divulgações de seus dados pessoais.
12. Capacidade de demonstrar cumprimento.



OBRIGADO

A disponibilização do conteúdo da presente apresentação não constitui aconselhamento jurídico, não dispensando a consulta de um especialista.

www.abreuadvogados.com

Lisboa (Nova morada)

Av. Infante D. Henrique, 26
1149-096 Lisboa

☎ (+351) 217 231 800

📠 (+351) 217 231 899

✉ lisboa@abreuadvogados.com

Porto

Rua S. João de Brito, 605 E - 4.º
4100-455 Porto

☎ (+351) 226 056 400

📠 (+351) 226 001 816

✉ porto@abreuadvogados.com

Madeira


Rua Dr. Brito da Câmara, 20
9000-039 Funchal

☎ (+351) 291 209 900

📠 (+351) 291 209 920

✉ madeira@abreuadvogados.com

Siga-nos

 www.linkedin.com/company/abreu-advogados

 www.twitter.com/abreuadvogados



A Abreu Advogados é a 1ª sociedade de advogados em Portugal com sistema de gestão certificado (ISO 9001).



A Abreu Advogados compensa a sua pegada de carbono e está certificada como e)mission neutral.



A Abreu Advogados é uma B Corp. As empresas B Corp, líderes do movimento global de pessoas que usam os “negócios como uma força para o bem”, cumprem as mais elevadas normas corporativas em matéria de responsabilidade, transparência e desempenho social e ambiental e fomentam o poder dos negócios para resolver desafios sociais e ambientais.