



ABREU  
ADVOGADOS

[www.abreuvadogados.com](http://www.abreuvadogados.com)

REGULAMENTO  
GERAL DE  
PROTECÇÃO DE  
DADOS  
PESSOAIS

- **Revoga** a Directiva de Protecção de Dados n.º 95/46/CE (de 24 de Out. 1995).
- **Define** um novo quadro legal em matéria de protecção de dados a vigorar de forma uniforme em toda a União Europeia, passamos a ter uma **única lei**, directamente aplicável em toda a UE.
- **Aplica-se** às empresas sediadas em todo o território da União Europeia e ainda às empresas estabelecidas fora do espaço da UE e sem presença na UE que ofereçam serviços ou façam negócios na UE.
- **Vigora a partir** de 25 de Maio de 2018.

**Período de adaptação: agora! (de 4 Maio de 2016 a 24 de Maio de 2018).**

## Mudança de Paradigma:

- **Redução de burocracia** através da abolição do princípio geral da notificação prévia, o que implica uma maior fiscalização.
- Existência de um **sistema de balcão único** para a protecção de dados na U.E.: uma única agência de protecção de dados com competência transnacional para se relacionar com as empresas.

Tendencialmente, os responsáveis pelo tratamento e subcontratantes terão apenas que comunicar com a autoridade de controlo principal, i.e., de acordo com o n.º 1 do artigo 56.º, a “*autoridade de controlo do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento ou do subcontratante*”.

## Novas Obrigações Para os Responsáveis pelo Tratamento de Dados:

- Nomeação de um “Data Protection Officer” (Encarregado de 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
- 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.

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

### **Obrigaçãõ de obtençãõ de Consentimento expresso e inequívoco**

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

### **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 obrigaçãõ de aceder a esse pedido.

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

### **Obrigaçãõ de Registo do Tratamento de Dados Pessoais** *Accountability*

Obrigaçãõ de conservaçãõ de registo detalhado de todas as actividades de tratamento sob a sua responsabilidade, o qual deve ser disponibilizado, a pedido, à autoridade de controlo.

## 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

## 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 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.



## 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.

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 (indemnizações)
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)

## Implementação de um programa de conformidade:

- Não é algo que se possa fazer de uma só vez:

É necessário planear – fazer – verificar – agir em conformidade (e voltar ao início...).

- Princípio da Responsabilidade (*Accountability*):

Capacidade de demonstrar o cumprimento.

- Aspetos 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.

## Algumas recomendações durante o período transitório e de adaptação ao novo Regulamento:

1. Implementar processos e políticas (incluindo auditorias regulares e formação de pessoal) para ser capaz de assegurar e demonstrar a conformidade com todas as obrigações do RGPD.
2. Determinar se são necessários recursos humanos adicionais para cumprir as obrigações decorrentes do Regulamento, especialmente no que diz respeito à nomeação de um responsável pela proteção de dados da empresa.
3. Realizar uma análise detalhada sobre os fluxos de dados e criar de um inventário de dados detalhado.
4. Criar um procedimento para a avaliação do impacto de privacidade de dados.

5. Realizar as notificações necessárias à CNPD e mantê-las atualizadas. Apesar do regulamento eliminar algumas das exigências de notificação/autorização, estes documentos poderão servir para registos internos de Compliance.

6. Rever documentação (políticas de privacidade, políticas internas da empresa, formulários de consentimento) e identificar quaisquer detalhes ausentes que possam ser exigidos pelo regulamento.

7. Desenvolver uma política de resposta a violação de dados e designar indivíduos responsáveis.

8. Analisar o seu cumprimento contratual e determinar se alterações aos acordos existentes são necessárias, em especial à luz dos novos requisitos para os acordos de tratamento de dados.

9. 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

Obrigada!



**Filipa Iglésias**

Advogada Associada

[filipa.iglesias@abreuadvogados.com](mailto:filipa.iglesias@abreuadvogados.com)

[www.abreuadvogados.com](http://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](http://www.linkedin.com/company/abreu-advogados)

 [www.twitter.com/abreuadvogados](http://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.