O objetivo do Regulamento Geral de Proteção de Dados (RGPD) é garantir o respeito pelo Direito fundamental de cada indivíduo de exercer controlo sobre as suas informações pessoais, inserindo mudanças substanciais na abordagem à gestão de dados pessoais e impondo sanções significativas para casos de não conformidade.

Princípios fundamentais:

i. Livre circulação
ii. Legalidade, lealdade e transparência
iii. Limitação das finalidades
iv. Minimização dos dados
v. Exatidão
vi. Limitação da conservação
vii. Integridade e Confidencialidade
viii. Responsabilidade demonstrada

O tipo de dados pessoais e respetiva quantidade a tratar dependem do motivo jurídico pelo qual este tratamento está a ser efetuado e qual a sua finalidade, devendo ser respeitadas as seguintes regras fundamentais:

i. Consentimento do titular dos dados
ii. Relação Contratual
iii. Obrigação Jurídica
iv. Interesses Vitais
v. Interesse Público
vi. Interesses legítimos

Direitos & Deveres dos titulares dos dados pessoais:

Direitos:

1. Transparência
2. Informação
3. Acesso
4. Retificação
5. Esquecimento
6. Limitação no tratamento
7. Notificação
8. Portabilidade
9. Oposição
10. Não ser sujeito a decisões automatizadas

Deveres:

1. Estabelecer uma Política adequada

2. Demonstrar conformidade com RGPD

3. Realizar a Proteção de Dados desde a Conceção *(Privacy by Design)* e por Defeito *(Privacy by default)*

4. Registar as atividades de tratamento

5. Cooperar com a autoridade de controlo

6. Garantir a segurança dos dados e do seu tratamento

7. Notificar violações aos dados pessoais

8. Avaliar o impacto de evoluções nos processos, aplicações e sistemas de informação

9. Designar o Encarregado da Proteção de Dados *(DPO – Data Protection Officer)*

10. Garantir que a subcontratação é regulada

11. Comunicar a violação de dados aos seus titulares

12. Garantir a responsabilidade conjunta pelo tratamento

Uma Instituição estará em conformidade, se conseguir demonstrar que mantém evidências adequadas que cumpre com os requisitos do RGPD. Mesmo que na sua Instituição considere que já forma implementados todos os requisitos do RGPD, consegue garantir que tem evidências adequadas que os seus contratos, *website*, aplicações informáticas, tratamento de dados, processos de negócio, etc., continuam a garantir a conformidade?

De todos os direitos, os que merecem maior atenção, especialmente devido ao seu impacto nos Processos e Sistemas de Informação, são :

i. Direito de ser esquecido – Em que o titular de dados pessoais tem direito a solicitar que os dados sejam eliminados.

ii. Direito de portabilidade – Em que o titular dos dados pessoais tem o direito a receber os seus dados pessoais do responsável pelo tratamento, em formatos interoperáveis que permitam a portabilidade dos dados entre sistemas, para que os possa reutilizar na sua esfera privada, do modo que entender.

iii. Direito de não sujeição a nenhuma decisão tomada apenas com base no tratamento automatizado – Neste caso, o titular dos dados pessoais tem o direito de se opor ao *profiling* - qualquer forma automatizada de processamento de informação pessoal com o objetivo de utilizar essa informação na avaliação de aspetos relacionados com uma pessoa específica. Neste conceito inclui-se também o rastreamento com a intenção de prever um comportamento de um sujeito e as suas preferências.

Para garantir a segurança dos dados (confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços de tratamento), as Instituições devem utilizar técnicas, como:

1. *Privacy by Design* – Desenhar e criar novos Processos, Aplicações e Sistemas já com a Privacidade considerada a partir da fase de desenho.

2. *Privacy by Default* – A Privacidade é obrigatória.

3. Pseudonimização – Tratamento de dados que impeça a capacidade de relacionamento direto com o seu titular, sem recorrer a informações adicionais.

4. Anonimização - Tratamento de dados que elimine completamente a capacidade de relacionamento direto com o seu titular.

5. Encriptação – Os dados são transformados por um algoritmo que retira a capacidade de leitura direta, mas que podem voltar a ser lidos através da desencriptação realizada pelos mesmo algoritmo.

Paulo André
Partner
+ 351 918 954 968
pandre@bakertilly.pt

Rafael Nunes
Manager
+ 351 937 733 667
rafael.nunes@bakertilly.pt