



# Proteção de dados: estão as empresas preparadas?

Por MARIA DE LURDES GONÇALVES



Associada sénior de Privacidade, Proteção de Dados & Cibersegurança da VdA

A PARTIR DE 25 DE MAIO, AS NOVAS REGRAS DE proteção de dados tornam-se obrigatórias para todas as organizações (públicas e privadas) que tratam dados pessoais de cidadãos europeus ou que se encontrem na União Europeia. **Estas regras assentam na devolução aos cidadãos do controlo sobre os seus dados pessoais e num novo modelo de regulação baseado na verificação prévia do cumprimento do RGPD pelas entidades que tratam dados (sejam responsáveis pelo tratamento ou subcontratantes).**

Se muitas organizações já têm um percurso de vários meses de adaptação ao Regulamento Geral sobre a Proteção de Dados (RGPD), muitas outras estão a começar agora o seu caminho, que será mais ou menos longo considerando o sector de atividade em que atuam, o atual perfil de compliance em matéria de proteção de dados ou a apetência para assumir maior ou menor risco face às obrigações impostas pelo RGPD.

De entre os vários desafios sentidos, destacam-se: (i) a implementação de medidas de compliance sem colocar em causa as prioridades estratégicas e comerciais da organização, (ii) a elaboração de textos de privacidade e pedidos de consentimento user friendly e operacionalizáveis no contexto dos serviços prestados, ou (iii) a inexistência de ferramentas/softwarewares no mercado totalmente adaptadas às regras do RGPD e que permitam uma gestão adequada de compliance nesta matéria.

Acresce que a falta de uma lei nacional que densifique, à data, alguns aspetos essenciais do RGPD ou a atual indefinição em torno da aplicação das coimas, em particular para os organismos públicos e para grandes grupos económicos, dificulta a realização de uma análise de risco ajustada pelas organizações. **Existe, por isso, grande expectativa em torno da atuação da CNPD após 25 de maio (i.e., se adotará uma postura mais interventiva ou mais reativa).**

Neste panorama, e não obstante a necessidade de cumprir todas as obrigações decorrentes do RGPD, existem aspetos que, por razões que vão para além das de natureza jurídica (como a visibilidade para os clientes e autorida-

des de controlo), assumem prioridade:

1. a preparação dos registos das atividades de tratamento e adoção de mecanismos de atualização dos mesmos;
2. a revisão das políticas de proteção de dados e gestão dos pedidos de consentimento;
3. a criação de um plano de gestão dos incidentes que impliquem violações de dados pessoais;
4. a regulação da relação com os subcontratantes (incluindo definição de planos de auditoria); e
5. a avaliação da necessidade de nomeação de um Data Protection Officer ou designação de equipa interna de acompanhamento dos temas de proteção de dados.

**Apesar da premência no cumprimento mínimo das regras para evitar a aplicação das pesadas coimas (uma vez que nenhuma organização quer “servir de exemplo”), a adaptação ao RGPD é muito mais do que “tickar” pontos numa checklist, implicando antes uma alteração profunda na forma como as organizações gerem os seus dados, com impactos reais no negócio, IT, recursos humanos e a nível financeiro.**

De facto, uma estratégia de privacidade bem-sucedida

**“Estas regras assentam na devolução aos cidadãos do controlo sobre os seus dados pessoais e num novo modelo de regulação baseado na verificação prévia do cumprimento do RGPD pelas entidades que tratam dados”**

passa, para além do cumprimento das regras legais, por construir uma cultura de proteção da privacidade, escolher as tecnologias adequadas ou compreender o valor dos dados. **As organizações mais adiantadas na adaptação ao novo paradigma da proteção de dados pessoais poderão capitalizar os ganhos reputacionais associados a uma estratégia de compliance mais sólida, já que tal será certamente um fator diferenciador face à concorrência. ●**