Data: 2018/03/05 ADVOCATUS - PRINCIPAL
Título: O ADN do Regulamento Geral sobre a Proteção de Dados - Artigo/Crónica por Inês Antas de Barros
Tema: Vieira de Almeida & Associados
Periodicidade: Mensal Âmbito: Especializada
Temática: Gestão/Economia/Negócios Imagem: 1/2
Pág.: 12
GRP:
Inv.: 5959.97 €
Tiragem:
Área: 86714 mm2

O ADN do Regulamento Geral sobre a Proteção de Dados

Por **INÊS ANTAS DE BARROS**

Advogada associada coordenadora da VdA

A POUCOS MESES DA DATA DE APLICAÇÃO DO Regulamento Geral sobre a Proteção de Dados ("RGPD"), que sucederá a partir de 25 de maio, muitas são as organizações (públicas e privadas) que se encontram a preparar a implementação deste diploma.

Apesar de o tema não ser novo, a **mudança de paradigma que o RGPD impõe, coloca, na ordem do dia, o tema da proteção de dados pessoais e segurança.**

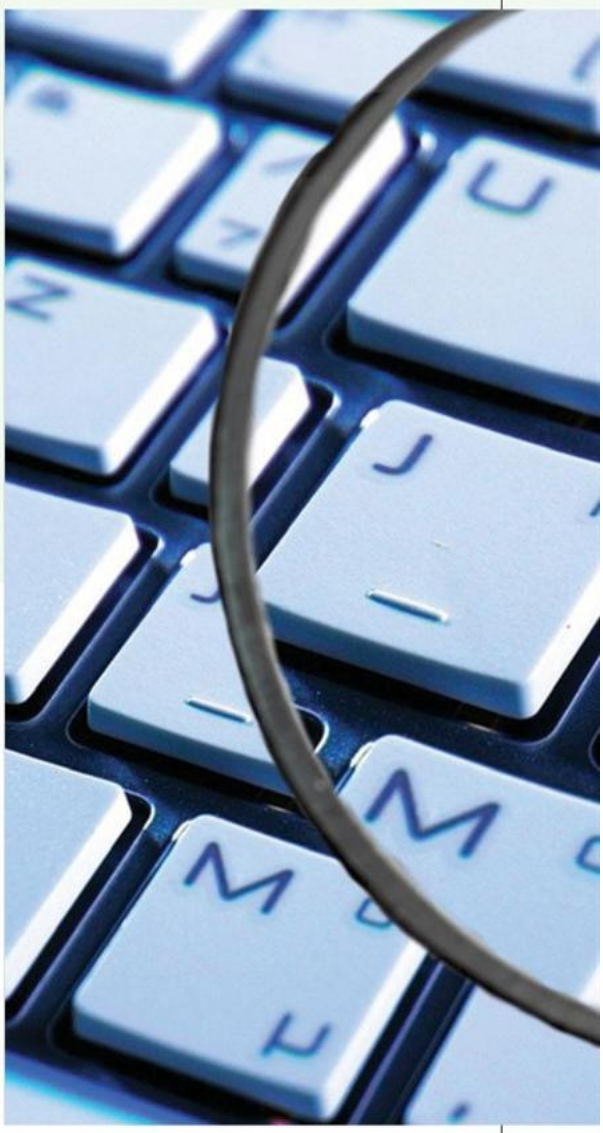
Há um conjunto de importantes lições que as organizações devem considerar.

A primeira lição é que é essencial **o engagement da Administração. É fundamental que este tópico esteja na agenda dos gestores de topo, caso contrário não será possível implementar um projeto eficaz ou minimente compliant, já que existem aspetos estratégicos que têm necessariamente que ser decididos pela gestão de topo.**

A segunda lição é que o RGPD exige a adoção de uma abordagem 360º aos vários streams (legal, tecnológico e processual), para que se consiga, com sucesso e eficiência, implementar as alterações necessárias.

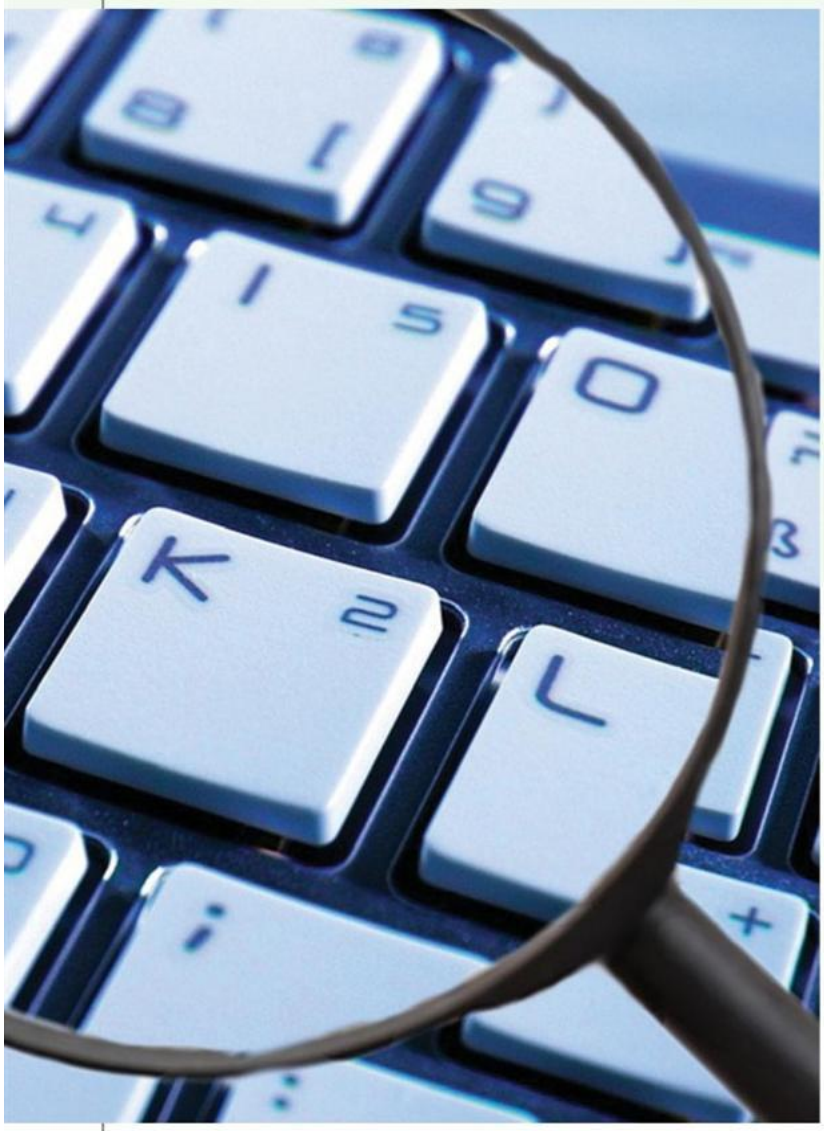
Note-se, como terceira lição, que não existe uma fórmula mágica. O nível de adaptação e mudança está dependente, por um lado, do grau de maturidade da organização e, por outro lado, das exigências próprias do setor de atividade da organização em causa. Em qualquer situação, é inegável, mesmo relativamente às organizações com elevado grau de maturidade e com reduzida regulação setorial, que as alterações são necessárias e impactantes - desde logo, ao nível do negócio. Por exemplo, organizações que se dediquem a atividades business to consumer terão que, na maioria dos casos, recolher novos consentimentos, prestar mais informação e ter mais interação com os titulares dos dados.

Outra lição importante é que terá que existir uma eficaz governance dos dados pessoais. **Os dados pessoais, o petróleo da era digital, constituem um ativo muito importante para as organizações, sendo essencial que tal ativo seja compliant.** Assim, as organizações estarão em condições de legitimamente utilizar os dados pessoais (desde logo, para desenho de estratégias de gestão de recursos humanos, marketing, big data, perfilagem, entre outras), caso seja assegurado o cumprimento de um conjunto de obrigações que são reforçadas com o RGPD.



É de destacar ainda a necessidade de implementar e/ou rever processos de compliance e de recolha de evidências. Estes processos são essenciais, desde logo, para garantir o cumprimento dos novos princípios de privacy by design e privacy by default; para assegurar a notificação às autoridades de controlo e a comunicação aos titulares dos dados da ocorrência de violações de dados pessoais; para responder aos

Data: 2018/03/05 ADVOCATUS - PRINCIPAL
Título: O ADN do Regulamento Geral sobre a Proteção de Dados - Artigo/Crónica por Inês Antas de Barros
Tema: Vieira de Almeida & Associados
Periodicidade: Mensal Âmbito: Especializada
Temática: Gestão/Economia/Negócios Imagem: 2/2
Pág.: 13
GRP:
Inv.: 5959.97 €
Tiragem:
Área: 86714 mm2



PIXABAY

pedidos dos titulares e, em geral, demonstrar que a organização cumpre todas as obrigações do RGPD.

Para as organizações que se encontram, agora, a implementar o RGPD, há que identificar prioridades. No mínimo, e até 25 maio, é essencial que as organizações:

1. Identifiquem os critérios de legitimidade para o tratamento de dados. Para o efeito, é essencial fazer um levantamento das finalidades do tratamento de dados pessoais, das categorias de dados pessoais e das categorias de titulares, para que possam ser identificados os critérios de legitimidade aplicáveis a cada situação.
2. Implementem os requisitos "mínimos", tanto internos como externos. Desde logo, assegurar a prestação de informação e recolha de consentimentos, quando e se aplicável, dos colaboradores e clientes; rever acordos com terceiras entidades de forma a considerar as novas obrigações aplicáveis à relação de subcontratação; ter o registo de atividades de tratamento completo e atualizado; avaliar a necessidade de nomeação de um Encarregado de Proteção de Dados ("Data Protection Officer") e definir responsabilidades internas.
3. Definam processos de compliance e de recolha de evidências. Assentando o RGPD no princípio da autorresponsabilização, as organizações devem ter documentados, preparados e testados processos internos de compliance e de recolha de evidências. Uma organização que não aposte na definição e reforço de processos internos, dificilmente conseguirá, em caso de fiscalização, demonstrar que cumpriu as obrigações previstas no RGPD.
4. Identifiquem os principais riscos e definam um plano de ação para o pós-25 de maio. É essencial que, relativamente aos requisitos que as organizações não consigam assegurar o seu cumprimento cabal, tenham identificado os riscos decorrentes de tal situação, preparando uma estratégia de damage control e delineando um plano de ação de implementação de tais requisitos.

Uma das lições das novas regras é que o RGPD exige a adoção de uma abordagem 360º aos vários streams (legal, tecnológico e processual), para que se consiga, com sucesso e eficiência, implementar as alterações necessárias.

"É essencial o engagement da Administração. É fundamental que este tópico esteja na agenda dos gestores de topo, caso contrário não será possível implementar um projeto eficaz ou minimente compliant, já que existem aspetos estratégicos que têm necessariamente que ser decididos pela gestão de topo"

Existem algumas dificuldades à conclusão da implementação do RGPD numa organização. Desde logo, a ausência de um quadro legal nacional que regule e densifique, como previsto no Regulamento, alguns aspetos essenciais.

Acresce que se desconhece, à data, qual será o nível de intervenção das autoridades de controlo – i.e. se as autoridades de controlo (nacional e outras, atendendo ao âmbito transnacional do RGPD) vão ser muito interventivas e fiscalizadoras ou se, pelo contrário, serão primordialmente reativas. **A estratégia de compliance e exposição ao risco de uma organização será naturalmente adaptada ao nível de intervenção das autoridades.** ●