E-LEARNING RGPD

O RGPD PARA PROFISSIONAIS DO DIREITO: COMO ABORDAR A CONFORMIDADE?

Introdução:

O Regulamento Geral de Protecção de Dados (conhecido como "RGPD"), adoptado em 14 de Abril de 2016 e que entrou em vigor em 25 de Maio de 2018 foi visto e sentido como uma verdadeira revolução na protecção dos dados pessoais e, de uma forma mais geral, da privacidade.

Contudo, o RGPD substitui ou completa textos antigos cujos princípios já eram muito semelhantes: a Directiva 95/46/CE de 24 de Outubro de 1995 a nível europeu ou, por exemplo, a francesa *Loi Informatique et Libertés* de 6 de Janeiro de 1978.

O que torna o RGPD um texto particularmente inovador com impacto nas empresas em sentido lato é, por um lado, o seu desejo de uniformizar o quadro regulamentar para a protecção de dados em toda a União Europeia, e mesmo para além dela, e, por outro lado, o reforço das obrigações que pesam sobre as empresas, acompanhado de sanções muito severas.

Este âmbito de aplicação mais amplo reflecte-se no facto de o RGPD dizer respeito a todas as empresas e a todas as organizações públicas ou privadas que recolhem ou processam dados pessoais na Europa: escritórios de advogados, mas também profissionais do direito, tais como notários ou oficiais de justiça, são, por conseguinte, todos abrangidos pelo RGPD nas suas actividades que envolvem o processamento de grandes volumes de dados pessoais.

Tendo em conta as nossas obrigações profissionais e éticas, devemos estar particularmente vigilantes para assegurar que as nossas actividades cumpram estes novos requisitos.

I. O que há de novo no RGPD

I.1 Um âmbito de aplicação mais vasto

Os principais objectivos do RGPD, nomeadamente a harmonização das regulamentações nacionais e o reforço da protecção dos dados pessoais, dado o contexto globalizado em que são processados, resultaram num âmbito de aplicação significativamente alargado:

A noção de "dados pessoais" é extremamente ampla, pois diz respeito a "*qualquer informação relativa a uma pessoa em causa*" que corresponda a "*uma pessoa singular identificada* [...] *ou que possa ser identificada, directa ou indirectamente, por meios que sejam razoavelmente susceptíveis de serem utilizados pelo responsável pelo tratamento ou por qualquer outra pessoa singular ou colectiva [...*]". Assim, os dados pessoais já não são definidos apenas em termos da natureza de identificação das informações na posse do próprio controlador, mas também em termos da possibilidade de estas informações poderem ser cruzadas com quaisquer outras informações na posse de terceiros, conferindo-lhes um carácter identificador.

Além disso, a definição de dados anónimos ou pseudónimos no RGPD é extremamente restritiva. Em essência, logo que os dados sejam susceptíveis de ser individualizados, mesmo que não identifiquem directamente uma pessoa, são abrangidos pelo âmbito dos dados pessoais.

Por exemplo, ao fazer estatísticas pseudónimas sobre as preferências dos seus clientes ou ao guardar documentos relativos a um caso que não mostram o nome ou o nome próprio de uma pessoa ... os dados pessoais são tratados a priori e o RGPD deve ser respeitado.

O âmbito territorial de aplicação da RGPD é extenso: assim que uma operação de processamento é realizada no contexto das actividades de um estabelecimento situado no território da União Europeia, relativo a um residente europeu ou ligado a uma oferta de bens ou serviços a pessoas situadas no território da União Europeia, o RGPD aplica-se. Do mesmo modo, a transferência de dados fora da União Europeia ou o acesso a dados de fora deste território está sujeito a regras muito estreitas que tendem a ser reforçadas sob a influência da Comissão Europeia.

É compreensível, no contexto da utilização constante de ferramentas digitais e novas tecnologias e onde os dados pessoais se estão a tornar uma forte aposta económica: o RGPD aplica-se em todo o lado e a toda a hora!

II.2 Obrigações reforçadas

O RGPD exige que as empresas repensem a sua organização da gestão e protecção de dados pessoais, em particular através de:

A obrigação para todas as empresas, excepto em certos casos, **de manter um registo** com a lista das operações de processamento que realizam. Este registo deve mostrar uma certa quantidade de informação que requer saber exactamente quais os dados que estão a ser processados e como. Este trabalho pode parecer enfadonho, mas muitas vezes permite uma análise aprofundada que facilita o cumprimento do RGPD numa data posterior.

A obrigação de definir a **divisão de responsabilidades com os seus prestadores de serviços ou parceiros:** o RGPD prevê diferentes qualificações (responsável pelo tratamento, co-responsável pelo tratamento ou processador) que dependem de quem decide sobre os meios e finalidades do tratamento dos dados pessoais. A distribuição destas responsabilidades deve ser contratualizada dentro de um documento que respeite um certo número de disposições impostas pelo RGPD.

- Pode ser obrigatório ou recomendado nomear um "**Encarregado de Protecção de Dados"**, o chamado "EPD", que é a pedra angular do cumprimento da RGPD.

- Os princípios de minimização e proporcionalidade introduzidos pelo RGPD também exigem a definição **dos períodos de tempo em que os dados são mantidos** (independentemente do meio: papel ou digital). Estas "políticas de conservação de dados" devem ser fiáveis e baseadas em critérios claros, tais como os fins para os quais os dados são utilizados (não se deve conservar dados que não sejam necessários), obrigações legais ou prazos de prescrição aplicáveis.

O RGPD também dá grande ênfase à implementação das **medidas necessárias, quer técnicas quer organizacionais, para garantir um nível suficiente de segurança dos dados processados.** Isto inclui também a obrigação de notificar a autoridade supervisora nacional de perdas graves e violações de dados pessoais no prazo de 72 horas após a descoberta da violação, o que é generalizado a todas as organizações. Além disso, quando a violação for susceptível de afectar a privacidade dos titulares dos dados, estes terão também de ser notificados.

O RGPD alterou as expectativas das empresas e organizações que processam dados: onde anteriormente, como em França, bastava fazer simples declarações à Commission Nationale Informatique et Libertés, é agora necessário ter um conhecimento profundo das operações de processamento que estão a ser realizadas e documentar a forma como os requisitos regulamentares estão a ser cumpridos.

3. Aumento da protecção dos direitos das pessoas em causa

A natureza protectora do RGPD reflecte-se num reforço dos direitos dos titulares dos dados. Assim, para além dos direitos existentes, tais como o direito de acesso ou o direito de rectificação, existem novos direitos que as pessoas em causa podem exercer junto das empresas:

O **direito** alargado **à informação** (artigos 13.º e 14.º do RGPD): Para além dos elementos de informação já previstos no regulamento anterior, a informação fornecida aos indivíduos deve, em particular, abranger também "a duração do período de conservação" e "qualquer outra informação necessária para assegurar um tratamento justo dos dados", que é muito ampla.

Consentimento (artigos 4.º e 7.º do PIBR): Sempre que necessário, o consentimento terá de ser explícito e distinto. Ou seja, os indivíduos devem dar o seu consentimento para cada utilização dos seus dados para a qual são necessários. Além disso, o RGPD introduz requisitos específicos de consentimento para crianças menores de 16 anos para a prestação de certos serviços.

O direito a **apagar** ou "direito a ser esquecido" (Artigo 17.º do RGPD): As pessoas em causa podem solicitar o apagamento dos seus dados em múltiplos casos, em particular quando os dados deixarem de ser necessários para os fins para que foram recolhidos ou processados ou quando as pessoas desejarem retirar o seu consentimento ou opor-se ao processamento.

O direito à **portabilidade** (Artigo 20.º do RGPD): Os responsáveis pelo tratamento devem permitir a comunicação dos dados de uma pessoa em causa a outro responsável pelo tratamento num formato "estruturado, comummente utilizado e legível".

A gestão dos pedidos para o exercício dos direitos pelos titulares dos dados deve ser antecipada a fim de poder responder plenamente e dentro dos prazos impostos pelo RGPD. Isto envolve, por exemplo, o direito à informação, a revisão dos avisos de informação ou da política de privacidade no seu website ou em qualquer outro meio através do qual os dados são recolhidos. Do mesmo modo, para poder responder a um pedido de direito de acesso, recomenda-se antecipar um procedimento destinado a identificar quais os dados que devem ou podem ser transmitidos e como extrair volumes de dados dos seus sistemas de informação que possam ser significativos.

A fim de assegurar o cumprimento destas obrigações e de proporcionar às autoridades de protecção alavancas reais contra as empresas que controlam, o RGPD acrescentou **sanções administrativas,** cujo montante foi grandemente aumentado. Dependendo do tipo de violação, uma multa pode atingir 20.000.000 euros ou até 4% do volume de negócios anual a nível mundial, o que for mais elevado. O arsenal de sanções contém também a possibilidade de as autoridades de controlo tornarem públicas as suas decisões, o que tem um elevado impacto e, por conseguinte, dissuasor para as empresas sancionadas.

II. As principais acções de conformidade

Quais são os principais passos?

1. **Definir conformidade**: para abordar a conformidade de uma forma adequada e racional, recomenda-se:
    - Definir se é obrigatório ou relevante nomear um EPD e identificar os intervenientes estratégicos internos e/ou externos para assegurar o cumprimento;
    - Realização de campanhas internas de sensibilização para divulgar boas práticas e assegurar a eficácia da abordagem.

2. **Inventário das operações de processamento**: esta fase é essencial para adaptar as medidas de conformidade e assegurar que seja produzido um registo completo. Para tal, é muitas vezes útil começar por reunir e analisar qualquer documentação existente (registo, antigas declarações, etc.) antes de fazer um inventário das principais categorias de processamento por projecto e/ou finalidade (clientes, recursos humanos, fornecedores de serviços informáticos, etc.).

3. **Dar prioridade às acções a realizar**: é necessário **estabelecer um calendário tendo em conta:**
    - As actividades, dimensão e estrutura das equipas envolvidas;
    - Possíveis factores externos que possam ter impacto nas acções prioritárias a tomar (por exemplo, novo projecto em curso ou a ser lançado).

4. **Garantia de conformidade** : Todas estas acções podem ser implementadas como e quando necessário, de acordo com as prioridades específicas de cada actividade.