NOVO REGULAMENTO GERAL DE PROTECÇÃO DE DADOS (RGPD)

CONSELHO REGIONAL DE LISBOA DA O.A.
DELEGAÇÃO DE OEIRAS

LEONOR CHASTRE
PROPRIEDADE INTELECTUAL E PROTECÇÃO DE DADOS

13 de Março de 2018

Por ser um regulamento e não uma diretiva, o RGPD passa a vigorar automaticamente nos estados-membros da UE, dois anos depois da respetiva aprovação. O que significa que, em maio de 2018, o novo regulamento europeu de proteção de dados estará, obrigatoriamente, em vigor.

Com a aplicação do RGPD, há uma mudança de conceito e procedimentos que se avizinha:

- Data Privacy Impact Assessment (DPIA);
- Privacy by Design;
- Privacy by Default;
- Direito à portabilidade;
- Direito ao Esquecimento;
- Consentimento;
- Formação

A Administração Pública vai avançar com a criação dos postos de Encarregados de Proteção de Dados para os vários organismos, departamentos e setores que a constituem durante este ano de 2018. Esta nova função profissional pretende preparar os organismos do Estado para a transposição do Regulamento Geral de Proteção de Dados (RGPD).

A par dos Encarregados de Proteção de Dados na Administração Pública e nas empresas, o RGPD prevê a realização de auditorias no que toca à proteção de dados, e promete reforçar as funções de fiscalização das entidades de regulação (como a Comissão Nacional da Proteção de Dados ou CNPD). Entre as medidas previstas pelo RGPD figuram a **portabilidade dos dados** a pedido de cada cidadão ou empresa, as notificações de fugas de informação num prazo de 72 horas, e a criação de um sistema que permitirá aos cidadãos tratar de diferentes questões relacionadas com a privacidade dentro dos vários estados-membros da UE.

Consentimento

Nos termos do Artigo 7, é obrigação das organizações demonstrar que as pessoas deram o seu consentimento ao tratamento dos seus dados pessoais. O consentimento deve ser dado “de livre vontade”.

O Artigo 7 estabelece ainda: "Quando for efectuada a verificação de que o consentimento foi dado de livre vontade, deve ser levado em conta o facto de, entre outros, o cumprimento de um contrato, incluindo o fornecimento de um serviço ser condicionado ao consentimento para o tratamento de dados que não é necessário para o cumprimento do contrato". Este factor é de grande importância e será interessante ver o seu efeito. Curiosamente, também existe no HIPAA um tipo similar de restrição ao consentimento, onde a autorização para muitas finalidades não pode ser requerida como condição para receber tratamento.

Funções do *Data Protection Officer*

O artigo 37 estabelece as funções do *Data Protection Officer* o qual reporta ao *Chief Privacy Officer* (CPO), nos EU. As suas funções são as habituais, sem nenhuma alteração particular.

Mas o papel do CPO terá uma importância acrescida face às novas exigências do GDPR.

O artigo 35 estabelece um requisito para o CPO das empresas do sector público (com excepção dos tribunais) e para o Big Data.

Formação

O GDPR necessita de formação. Nos termos do Artigo 37, o GDPR determina, entre outras, a necessidade de levar a cabo a necessária formação a nível de protecção de dados do pessoal que mantenha acesso regular ou permanente a dados pessoais."

Formação é assim um requisito do GDPR. A qualidade da formação levada a cabo numa empresa é a chave através da qual as entidades reguladoras dos EU podem avaliar o nível de cumprimento dos requisitos da protecção de dados. A mensagem sobre privacidade e segurança não significa apenas palavras para os reguladores dos EU – é uma preocupação genuína. Isto poderá ter impacto na decisão do *timing* da implementação bem como no montante das coimas.

Direito ao Esquecimento

O Artigo 17 estabelece especificamente o direito ao esquecimento. Os dados devem ser apagados “sem demora” quando deixarem de ser necessários ou se a respectiva autorização expirar, entre outras coisas. A Directiva de Protecção de Dados da UE refere o direito ao esquecimento. O artigo 17 prevê ampla e explicitamente esse direito.

Notificação de violações

O artigo 31 estabelece que no prazo de 72 horas (3 dias) da tomada de conhecimento da violação, o responsável pelo tratamento deverá notificar a autoridade de supervisão. Este é um prazo muito curto e não muito prático.

Nos termos do Artigo 32 a notificação deve ser feita ao titular dos dados sempre que a violação "resulte num risco elevado para os direitos e liberdades dos individuais". A notificação deve ser efectuada "sem demora".

Uma “violação de dados pessoais” define-se como “uma violação das normas de segurança conduzindo à destruição, perda, alteração, divulgação não autorizada ou acesso acidental ou ilícito a dados pessoais transmitidos, armazenados ou sujeitos a qualquer outro tratamento.”

É interessante verificar que a notificação individual de violação é classificada como "risco elevado". Muitas notificações de violação de leis dos EU têm um sentido mais vasto. E as Regras de Violação de Dados da HIPAA são aplicáveis muito para lá das situações de alto risco. Será interessante verificar como as autoridades da UE definem "alto risco". Os Tribunais nos EU são muito relutantes em reconhecer risco ou dano; as coisas poderão ser muito diferentes na UE porque dano é entendido como uma violação de direitos enquanto nos EU dano é um conceito diferente. Em outras palavras, na UE uma violação de direitos constitui só por si um dano – é uma violação da dignidade. Nos EU, os direitos de uma pessoa podem ser violados sem dano, o que na perspectiva dos tribunais envolve ofensas físicas, reputacionais ou financeiras.

Sanções e Entrada em vigor

Nos termos do Artigo 79, o incumprimento de determinadas disposições resultará numa coima "até 2% do do volume total de negócios respeitante ao ano financeiro anterior". O incumprimento de outras disposições implicará uma coima até ao montante correspondente a 4% do volume total de negócios respeitante ao ano financeiro anterior." A coima de 4% aplica-se aos "princípios básicos do tratamento, incluindo condições para o consentimento", bem como os "direitos dos titulares dos dados" e "transferências de dados pessoais para um receptor num país terceiro ou organização internacional".

O RGPD constitui apenas uma parte da reformulação de quase todo o cenário de cibersegurança que se prevê para os próximos tempos.

Em maio de 2018, também deverá ficar concluída a transposição da diretiva europeia de Segurança das Redes e dos Sistemas de Informação (SRSI).

LEONOR CHASTRE

OBRIGADA

Sócia responsável do Departamento de Propriedade Intelectual, Media e Tecnologias de Informação da Cuatrecasas

- Advogada com título de Especialista em Direito da Propriedade Intelectual atribuído pela Ordem dos Advogados.
- Principais áreas de atividade: Propriedade Intelectual e Tecnologias de Informação, Contencioso Penal e Civil, Arbitragem e Societário.

Participa regularmente como oradora em vários seminários de Propriedade Intelectual, nacionais e internacionais.

Leonor.chastre@cuatrecasas.com