Alterações legais na era digital

Em Dezembro de 2015 o Parlamento Europeu e Conselho chegaram a um entendimento relativamente à reforma da protecção de dados. Em 14 de Abril de 2016 o Conselho Europeu adoptou o projecto de Regulamento – o Regulamento Geral de Protecção de Dados (que revoga a Directiva 95/46/EC) – que entrará em vigor em 2018.

Todavia, poderá a carga administrativa prevista pelo regulamento, verdadeiramente, mitigar os efeitos de ataques informáticos e risco cyber decorrentes da violação de dados pessoais?

As obrigações dos subcontratantes de dados

Através do âmbito territorial do novo Regulamento, alguns dos responsáveis pelo tratamento de dados (*controllers*) e subcontratantes (*processors*) fora da UE cujas actividades de processamento respeitem a oferta de bens ou serviços (ainda que gratuitos), devem designar um representante na EU.

Os processadores devem:

- manter um registo físico das actividades desempenhadas por conta de cada controlador.

- designar um "*Data Protection Officer*" quando lhes seja exigido.

- notificar, imediatamente, o responsável pelo tratamento dos dados quando tenha conhecimento de uma violação de dados pessoais.

Qualquer violação de dados pessoais deve ser comunicada à entidade reguladora nas 72 horas seguintes ao seu conhecimento, quando possível.

Direitos dos titulares dos dados

De modo a provir pela escorreita e transparente utilização e acesso a dados pessoais, o novo regulamento pretende alargar os direitos dos titulares e desenvolver o seu estatuto legal. Por exemplo:

- A necessidade de cada utilizador dar, livremente, o seu consentimento para processamento dos seus dados pessoais, o qual terá de ser explícito quando se tratem de dados de natureza sensível, identificando, explicitamente, a finalidade específica a que se destina;O "direito a ser esquecido" ou de apagamento, quando um utilizador retira o consentimento para processamento dos seus dados pessoais ou requer a sua retificação ou apagamento;Os responsáveis pelo tratamento de dados também devem discriminar o destinatário ao qual os dados serão divulgados, bem como a sua finalidade e período de armazenamento;

Caso se verifique uma violação de dados pessoais que afete a sua protecção ou privacidade, os seus titulares devem ser, imediatamente, notificados pelo responsável pelo tratamento;

Também, os titulares dos dados podem requerer cópia dos dados pessoais em fase de tratamento, junto dos responsáveis pelo tratamento.

Vicissitudes da gestão de cyber riscos

Ainda que o novo Regulamento seja um passo importante na protecção de dados pessoais, também representa um ónus administrativo acrescido para os responsáveis pelo tratamento de dados e subcontratantes, bem como, para as autoridades reguladoras.

Ora, de acordo com uma estimativa apresentada pelo Center for Media, Data and Society, verificaram-se cerca de 200 violações de dados pessoais na Europa, envolvendo 227 milhões de registos desde 2005. Considerando que os responsáveis pelo tratamento e entidades reguladoras devem cumprir com os prazos para notificação de violações, é previsível que a maioria seja elaborada de forma incompleta.

Mais do que provavelmente, o responsável procurará demonstrar – para satisfação da entidade reguladora - que implementou os meios de protecção adequados e que esses meios estavam em utilização aquando da violação em causa. O Conselho sublinha que a encriptação de dados pode ser incluída no leque de medidas tecnológicas a adoptar.

Portanto, os efeitos deste ónus administrativo podem estender-se a todos os intervenientes e a falta de eficácia de algumas medidas poderá importar custos acrescidos, pois o regulamento prevê a aplicação de multas - no maior valor de 20 milhões de Euros ou, em caso de empresa, 4% da facturação mundial.

Face à aproximação do pós-Brexit, não está ainda assegurada a manutenção do Regulamento no Reino Unido ou, contrariamente, se irão vigorar novas regras relativas à protecção de dados.

Apesar da procura por produtos cyber não ter ainda disparado, o seu preço e falta de divulgação podem ser uma barreira significativa para mercados que considerem a necessidade destas coberturas, pois a frequência e sofisticação dos ataques informáticos continua a aumentar. De facto, o cyber crime terá custado ao Reino Unido cerca de £27 biliões em 2013. Estima-se em média de custos em £65.000,00 a £115.000,00 para as pequenas e médias empresas e £600.000,00 a £1.15 milhões para as grandes.

O seguro cyber com cobertura para terceiros é um dos mecanismos de compensação para perdas derivadas de violações de dados, contudo, o ónus de apurar o grau de exposição ao risco e defender-se contra a natureza evolutiva dos riscos cyber recai sobre a própria empresa ou empresário. Numa perspectiva mais alargada este novo Regulamento vem demonstrar o compromisso do legislador Europeu com a cyber segurança.