CRÓNICA VISÃO ELECTRÓNICA
Nº 424 / 2017-02-02
http://www.gestaodefraude.eu
Edgar Pimenta

>> A nova regulamentação de dados pessoais

É uma sigla que já começa a ser um pouco mais conhecida: RGPD - Regulamento Geral de Proteção de Dados (GDPR em inglês). E do que se trata? É um novo regulamento emitido pela Comissão Europeia (e por ser um regulamento tem aplicação direta nos vários países) e cujo principal objetivo é harmonizar a legislação relacionada com a proteção de dados pessoais em toda a Europa. Mas faz mais do que isso... A União Europeia quis criar aquele que será uma das referências futuras na proteção de dados. Consequentemente, o RGPD traz vários novos direitos para os indivíduos e com isso, novas obrigações para as empresas. E o Regulamento (que já está em vigor) inclui um período de 2 anos para preparação para ser *compliant*. Na prática, significa que em Maio de 2018, a esmagadora maioria das empresas terá que estar em conformidade com o RGPD.

E porquê? Uma das razões está relacionada com as multas que podem ir até 20 milhões de euros. Valores que serão propositadamente altos para que o esforço de estar em conformidade seja sempre inferior ao custo de não estar.

E quais os impactos que o regulamento traz, numa perspetiva de segurança da informação e de fraude?

Um dos principais é a necessidade de reportar qualquer *data breach* ou perda de informação em 72 horas. Embora o conceito de *data breach* possa estar associado a um elevado número de registos, a verdade é que o RGPD não define um número mínimo. Como tal, um registo de um indivíduo é um *data breach*. E quando o tipo de informação que venha a público é sensível ou suscetível de macular os indivíduos afetados, a empresa deve avisá-los de que tal aconteceu.

Como é óbvio, isto traz novos requisitos para as empresas. Mais do que proteger a informação, passa a ser necessário ter a capacidade de detetar este tipo de situações, ser capaz de atuar em tempo útil e de ter uma perceção bastante correta do que aconteceu. E isso inclui saber quando aconteceu, o que aconteceu e exatamente em que moldes (incluindo quem foi afetado). Logo, torna-se necessário as empresas implementarem um conjunto

de controlos de resposta a este tipo de incidentes com um nível de maturidade bem mais elevado do que era o habitual até agora.

Outro requisito é o conceito de *Privacy by Design*. O conceito é simples: A privacidade e a segurança que lhe está associada devem ser consideradas logo na fase de desenho, seja de aplicações ou sistemas tecnológicos, seja de processos. Ou seja, quando se pensar em soluções para um qualquer problema e que envolva o tratamento de dados pessoais (e a definição é bastante abrangente), deve-se desde logo pensar como será esse tratamento e como serão os dados protegidos e cumpridos todos os direitos que os indivíduos terão com o novo regulamento (e que incluem o direito a ser esquecido, à portabilidade dos dados, à eliminação dos dados, ao acesso e retificação dos seus dados)...

Este resumo de dois parágrafos pode ser redutor e parecer que o que é preciso fazer para estar em conformidade com o regulamento é simples. Mas estes dois parágrafos são a ponta do *iceberg*.

Talvez uma boa forma de começar seja colocar a si mesmo esta questão: na sua empresa, sabe que dados pessoais são tratados (seja de clientes ou colaboradores), qual a finalidade desse tratamento e onde reside essa informação?

Se a resposta for um confiante sim, está no bom caminho para fazer o muito que ainda lhe poderá faltar para cumprir com o RGPD. Se a resposta for tremida, pouco confiante ou simplesmente um honesto não.... está na hora de olhar para a privacidade com outros olhos e colocar o RGPD no topo das suas prioridades.