CISION

IT Channel

ID: 69975803

01-06-2017

Tiragem: 2150
País: Portugal
Period.: Mensal
Âmbito: Tecnologias de Infor.

Pág: 45
Cores: Cor
Área: 23,46 x 27,29 cm²
Corte: 1 de 1

Juliana Marcondes | Associado PLMJ TMT

Quem é o Data Protection Officer?

O Regulamento Geral sobre a Proteção de Dados (Regulamento UE 2016/679) será aplicável em todos os Estados Membros a partir de 25 de maio de 2018. Estamos, portanto, a menos de um ano de importantes alterações aos procedimentos que terão de ser observados pelas empresas no âmbito das atividades que envolvem o tratamento de dados pessoais.

De entre as principais inovações do Regulamento está a introdução da figura do Data Protection Officer ou Encarregado da Proteção de Dados (DPO). O DPO é uma pessoa nomeada pelas empresas - que sejam responsáveis ou que atuem como subcontratadas para o tratamento de dados pessoais - e a sua função será supervisionar e aconselhar a empresa a respeito das obrigações contidas no Regulamento.

Juliana Marcondes, PLMJ TMT

A nomeação de um DPO é um dos exemplos da alteração do paradigma no que diz respeito ao cumprimento das regras legais sobre proteção de dados pessoais: a lei atual confere à Autoridade de Proteção de Dados (em Portugal, a Comissão Nacional de Proteção de Dados, CNPD) a avaliação dos procedimentos de cada empresa para tratamento dos dados pessoais, mediante a submissão de formulários de notificação ou de pedidos de autorização. Com o Regulamento, as empresas deverão adequar-se à lei independentemente destes processos. Deixarão de ter o dever de comunicar à CNPD para terem que ter, internamente, organizados os procedimentos para assegurarem o cumprimento do Regulamento. E este cumprimento deverá ser demonstrado através de documentação adequada, que deverá refletir os procedimentos aplicados no contexto do tratamento de dados pessoais. A organização desses processos poderá ser facilitada com a nomeação de um DPO.

O Grupo de Trabalho do Artigo 29 – um órgão independente europeu com funções consultivas, WP29 - tem emitido orientações que ajudam a interpretar o texto do Regulamento. Há *guidelines* sobre o DPO publicadas em dezembro de 2016 e atualizadas em abril de 2017. As *guidelines* são uma importante fonte de auxílio para as empresas e, neste caso, de esclarecimento sobre a figura do DPO.

Uma das principais questões colocadas sobre o tema é: todas as empresas ou entidades devem ter um DPO? A resposta é não. O Regulamento prevê que a nomeação de um DPO é obrigatória apenas em três casos: i) quando o tratamento dos dados seja efetuado por uma autoridade ou entidade pública (com exceção dos tribunais), ii) quando as principais atividades de tratamento do responsável ou do subcontratante consistam na monitorização regular e sistemática dos titulares dos dados em grande escala (como por exemplo, os grandes operadores de dados na internet, motores de busca, redes sociais) ou iii) quando as principais atividades do responsável ou do subcontratante consistam no tratamento em grande escala de dados pessoais sensíveis e dados relativos a condenações penais e contraordenações (são exemplos desta categoria os hospitais, as instituições financeiras e as seguradoras).

O que configura um tratamento de dados "em grande escala"? As orientações do WP 29 recomenda que sejam analisados: o número de titulares de dados considerados (individualmente ou em relação à população relevante); o volume de dados e categorias que estão a ser processados; a duração – ou frequência – do tratamento de dados; a extensão geográfica do tratamento de dados. Quanto maiores forem esses índices, maior a probabilidades de se ter um tratamento de dados em grande escala. São exemplos dessas situações: tratamento de dados de tráfego e localização pelos provedores de internet; a recolha de dados pessoais para as atividades regulares de um hospital, de um banco ou de uma companhia de seguros; tratamento em tempo real de dados de geolocalização de consumidores para fins estatísticos, entre outros que permitam identificar a existência de uma "grande escala".

Temos, portanto, apenas três situações em que o Regulamento indica como obrigatória a nomeação de um DPO. No entanto, se a empresa não se enquadrar nessas situações, não significa que não possa nomear um DPO. Se assim pretender poderá fazê-lo. A existência de um DPO será sempre um indicador positivo que demonstra boas práticas com o cumprimento das regras de proteção de dados.

Outra dúvida sobre o tema consiste em saber quem deve ser o DPO. Um colaborador dos quadros da empresa? Ou poderá ser contratado um serviço externo? As duas situações são possíveis. Mesmo no caso de um DPO contratado mediante um serviço externo, deverá existir um efetivo responsável – uma pessoa singular – que possa exercer as funções de DPO e ser a pessoa encarregada a responder enquanto DPO.

As funções do DPO são, regra geral, zelar pelo cumprimento da legislação de proteção de dados no âmbito das atividades do responsável ou subcontratado pelo tratamento dos dados. O DPO terá o exaustivo trabalho de recolher informações para identificar as atividades de tratamento de dados pessoais, analisar e verificar a conformidade desses processos com as regras do Regulamento e manter-se em constante papel de informador, conselheiro e emissor de recomendações para o cumprimento das regras. Tantas funções levam a uma inevitável questão: poderá ser o DPO pessoalmente responsável pelo incumprimento das regras? Não. Apenas a entidade responsável ou subcontratada pelo tratamento dos dados responderá pelo não cumprimento das regras.

Se a adequação às regras de proteção de dados não era uma realidade no âmbito das empresas, certamente passará a ser. O DPO terá o importante papel de contribuir para a tarefa de sensibilizar as corporações para a importância e relevância do compliance em tratamento de dados pessoais. É uma figura que chega tarde, mas ainda a tempo no novo tempo para a proteção de dados na União Europeia.

Seja bem-vindo, caro DPO.