Com a Lei Geral de Proteção de Dados entrando em vigor em agosto, empresas precisarão manter profissionais ou equipes de DPO preparadas para contemplar a gestão de dados pessoais segundo aspectos tecnológicos, jurídicos e de compliance

Entre os maiores desafios da gestão de risco empresarial moderno está a proteção à privacidade dos colaboradores, fornecedores e, principalmente, clientes. Com a nova Lei Geral de Proteção de dados (Lei nº 13.709/2018 - LGPD), que entrará em vigor em agosto, a tendência é que ocorra uma verdadeira corrida para adequação de processos às novas exigências legais a fim de evitar penalizações pela Agência Nacional de Proteção de Dados (ANPD) e garantir a segurança das informações.

“Como consumidores, os brasileiros terão direito de saber as informações que serão utilizadas pelas empresas e de que maneira. As empresas, por sua vez, têm agora esta obrigação prevista em lei, sendo que irregularidades podem resultar em danos irreparáveis à imagem corporativa e multas pesadas – de até cinquenta milhões de reais -, com paralização total ou parcial do banco de dados, entre outras consequências”, afirma Marcelo Nascimento, do Escritório DPO da everis Brasil.

A maioria das companhias já está investindo na adequação, tendo agora de atingir a maturidade de implementação e sustentar as boas práticas, tendo o novo desafio de eleger um DPO – Data Protection Officer. Este profissional será encarregado da proteção de dados e deve reunir conhecimentos referentes às questões tecnológicas, de direito e compliance. Mas devido à complexidade das características exigidas, o ideal é que seja apoiado por diversos profissionais do escritório, ou seja, que exista uma área de DPO.

“Porém, o desafio não acaba por aí. Manter diversos profissionais tão especializados é, muitas vezes, caro, gerando uma provável terceirização da função, o que é extremamente aconselhável, desde que o DPO atue próximo do quadro diretivo da empresa para apontar as mais diversas medidas de sustentação do ambiente de respeito à privacidade”, reforça Nascimento. Entre estas medidas estão procedimentos para atender às requisições dos titulares de dados e da ANPD; elaborações de Data Privacy Impact Assessment – DPIA; aculturamento da empresa, entre outras, incluindo uma rotina de gerenciamento de riscos de privacidade e auditoria.

Outro fator a ser considerado é que uma auditoria e, por consequência, um auditor, deverá considerar temas como proteção, gerenciamento de risco e controles de proteção à privacidade, sem prejuízo de todas as demais necessidades. “O atual cenário de privacidade e proteção de dados pessoais permite que auditores sejam participantes ativos, ajudando as empresas a perceber e lidar com questões de risco à privacidade. A proteção à privacidade pode ser considerada o processo de estabelecer o balanço apropriado entre a privacidade e os múltiplos interesses de negócio”, explica Nascimento.

Segundo ele, com a LGPD, a auditoria terá a obrigação também de trabalhar para minimizar o impacto, maximizar uma entrega justa, criar expectativas legítimas no mercado e, principalmente, que sejam factíveis. Diz, ainda, que será necessário um conjunto de princípios que governam o processamento dos dados pessoais de um indivíduo e um modelo das funções de privacidade envolvidas, que vem evoluindo nas últimas décadas.

É necessário, em qualquer framework de proteção à privacidade, considerar os seguintes agentes legais:

- Titular dos dados, indivíduo cujos dados pessoais são tratados;

- Controlador de dados - organização ou entidade que trata os dados pessoais do titular de dados;

- Responsável pela privacidade - a supervisão da empresa quanto ao tratamento de dados pessoais, manifesto na figura do DPO;

- Agência Nacional de Proteção de Dados - autoridade governamental responsável por garantir o melhor cumprimento da lei;

- Processador de dados - prestador de serviço contratado pelo controlador para o processamento de dados.

“As empresas devem abordar de forma adequada a gestão de informações, com governança e supervisão constantes e adequadas pelos “C’s level”, diretores e gerentes. É absolutamente necessário que haja incentivo à classe executiva para que acompanhe as ações da companhia para gerenciar, controlar e proteger os dados pessoais que coleta sobre clientes e funcionários, juntamente do comitê de auditoria. Além disso, devem ser constantemente avaliadas as práticas de conformidade e manipulação de dados pessoais e pontos fracos, comparando-os com políticas, leis e regulamentos internos e melhores práticas de mercado”, reforça Nascimento.

É fundamental que a companhia implemente um programa de privacidade que inclui, dentre seus controles: governança e responsabilidade da privacidade; uma política ou aviso de privacidade (a depender do cenário, ambos); políticas e procedimentos escritos sobre privacidade com publicidade; controles e processos; papéis e responsabilidades. Precisa também investir em treinamento e educação de funcionários e prestadores de serviços; monitoramento e auditoria; práticas de segurança da informação. É necessário ainda ter planos de resposta a incidentes em privacidade; leis e regulamentos de privacidade aplicáveis à empresa em um framework organizado; assim como planos para responder a problemas detectados e ação corretiva.

Entretanto, em última análise, a proteção à privacidade dos dados pelas empresas vai além do projeto de adequação à LGPD, por mais privilegiado e necessário que este seja. O gerenciamento de riscos de privacidade e auditoria é apenas uma das diversas facetas que a manutenção do ambiente de proteção à privacidade deve possuir para uma maturidade adequada, sendo extremamente importante e relevante. “Por isto, o ideal é que toda a empresa trabalhe pela gestão da privacidade e mitigação dos riscos, mas o DPO, seja ele uma pessoa ou toda uma equipe, deveria ser escolhido e acionado agora, a fim de assegurar o respeito aos direitos dos consumidores estabelecidos pela LGPD, pelo marco regulatório da Internet e outras leis”, conclui Nascimento.

Sobre a everis

A everis é uma empresa do grupo NTT DATA que oferece soluções comerciais e estratégicas, desenvolvimento e manutenção de aplicações tecnológicas e serviços de terceirização. A empresa, que conduz suas atividades nos setores de bancos, seguros, indústria, serviços públicos, telecomunicações, administração pública e saúde, obteve um faturamento de 1.4 bilhão de euros no último exercício. Atualmente, conta com mais de 24.500 profissionais distribuídos em seus escritórios e centros de alto desempenho em 18 países.

A NTT DATA é uma prestadora de serviços de TI e parceira de inovação global líder de mercado, sediada em Tóquio, com operações comerciais em mais de 50 países. Nosso foco está no compromisso de longo prazo, combinando alcance global com intimidade local para fornecer serviços profissionais de primeira, que variam de consultoria e desenvolvimento de sistemas a terceirização. Para mais informações, visite www.nttdata.com

Fonte: Market21 Comunicação & Marketing, em 23.03.2020