Por Hizadora D´Ambros e Tainã Dias (*)

Após a promulgação da Lei Geral de Proteção de Dados (LGPD), a privacidade e a proteção dos dados pessoais ganharam espaço no dia a dia dos brasileiros. Diante desse cenário, convivemos e reconhecemos a importância do momento de escolher, por exemplo, quais permissões conceder a um aplicativo, quais cookies permitir o acesso a um site ou quais checkboxs marcar ao final de um formulário.

Essas palavras ganharam espaço também no mundo corporativo, trazendo para o território nacional discussões e práticas aplicadas em outros países, como aqueles sob a abrangência da General Data Protection Regulation (GDPR), regulamento aplicado à União Europeia. Acompanhamos com a LGPD a crescente implantação de avisos e políticas de privacidade, criação de novos canais de comunicação com os titulares, além do crescimento de algumas áreas, dedicadas a cultivar e manter uma cultura de privacidade nas organizações.

A missão de fomentar essa cultura pode parecer estar ao encargo da área de privacidade ou ser absorvida por áreas como segurança da informação, jurídico e compliance, entre outras. Contudo, as atividades que tratam dados pessoais não são desempenhadas apenas por essas áreas, mas por uma diversidade de áreas a depender da natureza do negócio. A coleta, o uso e o descarte adequados dos dados pessoais estão nas mãos de cada colaborador da organização que lida com tais informações.

Por isso, a construção de uma nova consciência voltada para a proteção dos dados de titulares e das operações da organização somente será possível com a colaboração de todas as partes. A integração entre as áreas de negócio e a área de privacidade deve ser constante, ou seja, desde a concepção das operações, serviços e produtos que envolvem dados pessoais, deve-se colocar em prática os Princípios de Privacy by Design, propostos por Ann Cavoukian.

Dessa forma, as práticas elencadas a seguir, agregando parte dessas recomendações, podem ser implementadas pela organização, contribuindo para a vivência da cultura de privacidade.

Buscar apoio com os times de segurança da informação e privacidade para avaliar fornecedores e sistemas antes da contratação, além de identificar possíveis vulnerabilidades que possam levar à exposição indevida de dados, bem como estabelecer cláusulas contratuais de proteção de dados com fornecedores e parceiros são ações essenciais para ajudar a prevenir e antecipar possíveis incidentes.

Identificar todos os dados necessários para a atividade em execução e os usos pretendidos para esses dados. Consultar o time de privacidade para alinhar as finalidades e propósitos legítimos, além de estruturar como essas finalidades serão informadas aos titulares por meio de avisos e políticas de privacidade, por exemplo, são medidas importantes para mitigar riscos.

Estruturar a coleta, o armazenamento e o compartilhamento dos dados sempre considerando aqueles estritamente necessários para a atividade, armazená-los somente pelo tempo necessário para atingir os objetivos almejados, além de compartilhá-los unicamente com as pessoas, fornecedores e parceiros envolvidos na atividade.

Atuar com responsabilidade, transparência e segurança no uso dos dados pessoais é essencial. Portanto, o fluxo de dados, ou seja, o caminho percorrido desde sua coleta até seu descarte, deve ser registrado, documentado e avaliado pelo time de privacidade. E, as medidas técnicas e organizacionais de segurança devem ser incorporadas às atividades.

A princípio são atividades corriqueiras, naturais na vida de qualquer organização, e, de fato, são. Contudo, o maior desafio está na incorporação do olhar de proteção de dados nas atividades realizadas pelas áreas, fomentando, dessa forma, a identificação de oportunidades de melhorias nos processos atuais e de cultivo dessa nova consciência, pois, como declarado por Tim Cook, “Proteger os dados de outra pessoa é proteger a todos nós”.

(*) **Hizadora D´Ambros** é consultora pleno e **Tainã Dias** é gerente de Data Privacy. Ambas atuam na Protiviti, empresa especializada em soluções para gestão de riscos, compliance, ESG, auditoria interna, investigação, proteção e privacidade de dados.

Fonte: IMAGE, em 16.10.2023