Sztajn e Marques da Silva: A relação entre compliance e a LGPD

O termo *compliance* tem origem no verbo inglês *to comply*, que significa agir de acordo com uma regra, uma instrução interna, um comando ou um pedido. No âmbito institucional e corporativo, *compliance* pode ser entendido como conjunto de ações que visam ao cumprimento das normas legais e regulamentares, das políticas e diretrizes do negócio e das atividades da instituição ou empresa, visando-se, sobretudo, a evitar, detectar e solucionar quaisquer desvios ou inconformidades que venham a

O *compliance* pode ser associado à Lei Geral de Proteção de Dados (LGPD), que é o marco legal de proteção e transferência de dados no Brasil, com o objetivo de proteger os cidadãos contra o uso disfuncional de seus dados ou informações relacionadas a pessoas naturais ou jurídicas. Garante poder para fiscalizar e controlar informações pessoais, que nem sempre precisam ser sigilosas, mas que, se utilizadas sem expressa anuência do titular, configurarão invasão de privacidade. Exige, por exemplo, consentimento explícito para coleta e uso dos dados, além de obrigar as empresas a oferecerem opções a fim de que o usuário consiga visualizar, corrigir e excluir os seus dados de qualquer plataforma em que estejam inseridos. Quanto ao mais, a LGPD determina que para a divulgação e disponibilização de dados do cidadão deve haver a sua consciente e inequívoca manifestação de anuência.

Com a entrada da LGPD em vigor, as instituições e empresas são obrigadas a atualizar seus códigos de conduta, de sorte que tanto os procedimentos internos como as normas de segurança da informação deverão ser revistos. Governo e empresas devem desenvolver cuidadosamente uma abordagem estratégica para gerenciar o compartilhamento e a divulgação de registros e informações pessoais dos seus colaboradores e clientes. Necessariamente, os programas de *compliance* deverão estar de acordo com a LGPD, além de seguirem preceitos de ordem interna que não necessariamente sejam regidos por essa norma.

Para responder a essas exigências, as empresas precisarão de um departamento de *compliance* ativo, independente e bem estruturado. Precisarão de profissionais qualificados para lidar com todos os procedimentos internos relacionados ao tratamento de dados e segurança das informações, não apenas de seus colaboradores, mas de todos aqueles com os quais as empresas se relacionem.

Os departamentos de *compliance* deverão garantir que os regulamentos e políticas internas de conformidade e retenção de documentos sejam cumpridos, entre os quais preservar a capacidade institucional de fazer o trabalho sem atritos de segurança, governança e atentados aos requisitos de conformidade. Com o emprego, por exemplo, de rotinas de criptografia, essas empresas podem ter mais controle e governança sobre os dados que administram. Assim sendo, seus colaboradores e parceiros podem libertar-se do temor da quebra de privacidade e concentrar-se no cerne do negócio.

Não bastasse, para se adequarem à LGPD, essas empresas precisam pensar em proteger os dados e documentos dos seus colaboradores e clientes durante todo o ciclo de vida desses documentos, o que significa proteger os documentos e dados sensíveis, de regra regulados pela LGPD, aplicando políticas inteligentes de acordo com o seu conteúdo. Por exemplo, ao definir níveis de proteção para seus usuários, com classificação e prazos de retenção/exclusão de dados, ou mesmo regras para compartilhamento externo, tornam a adesão aos requisitos de governança muito mais fácil para suas equipes. As políticas claras de retenção determinam os períodos de tempo para os quais as empresas manterão o conteúdo e definem ações de disposição para quando o período de retenção terminar.

Ademais, para atender aos requisitos da LGPD e, ao mesmo tempo, manterem-se competitivas, preservando o conteúdo útil das informações, as empresas devem auditar as alterações de conteúdo dos seus funcionários para evitar a espoliação. Manter o controle de exclusão, ou seja, decidir quem pode excluir permanentemente dados e documentos. Proteger dados de alto valor contra exclusão acidental ou maliciosa. Remover informações redundantes, desatualizadas ou triviais para simplificar como as equipes trabalham e encontram conteúdo relevante nas pesquisas eletrônicas.

Ao implementar esses tipos de ferramentas, as empresas atendem as necessidades de conformidade e reduzem drasticamente a sobrecarga dos requisitos de conformidade advindos da LGPD, permitindo-lhes também entregar de forma eficaz e rápida quaisquer pedidos de direitos de dados que lhes forem solicitados.

Ante a LGPD, as consequências do não *compliance* podem ser desastrosas para as empresas. A não conformidade, ao vir a público, causa dano à imagem das empresas, o bloqueio no tratamento de dados, sanções e multas de até R$ 50 milhões, além de perda de clientes e negócios.

Dessa perspectiva, a responsabilidade social das empresas, um dos fatores em regras de *compliance* , tende a impactar decisões de consumidores na tomada de decisão, notadamente quando os mercados são elásticos e, portanto, a possibilidade de optar por outro fornecedor é grande.

A LGPD facilita e, em boa medida, reforça a adoção de regras de *compliance*, o que, no médio e longo prazos, trará benefícios para todas as pessoas.

Date Created
08/09/2020