Link: https://cutt.ly/FZoLW1Z

Novas diretrizes da LGPD impactam no uso de dados privados por bancos e instituições financeiras

Quinta, 21 Julho 2022 15:02 Crédito de Imagens:Divulgação - Escrito ou enviado por Letícia Pêgo Adicionar comentario
SEGS.com.br - Categoria: Seguros Imprimir

Mais de 60% das empresas do setor ainda não seguem as novas normas e correm risco de multa de até R$ 50 milhões

Aprovada em outubro de 2021, a Resolução nº 155, do Banco Central do Brasil (Bacen) estabeleceu que as administradoras de consórcio e instituições de pagamento com autorização de funcionamento pelo órgão devem formular e adotar na prática uma política institucional de relacionamento com os clientes. Nesta nova série de normas, está a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD), legislação brasileira que trata especificamente da defesa de informações particulares e de respeito à privacidade individual. "As exigências incluem ter a autorização contratual do usuário para manter dados pessoais armazenados e para utilizá-los para qualquer finalidade, bem como uma política clara de exclusão dessa base a qualquer momento que o usuário solicitar", informa a engenheira de software Maria Cristina Diez, diretora da Most Technologies, especializada em segurança digital.

Na prática, porém, poucas empresas estão totalmente em conformidade com a LGPD (Lei nº 13.709/2018), em vigor desde 2020. No segmento de atividades financeiras, seguros e serviços relacionados, apenas 37,5% das organizações estão em nível correto de adequação, segundo a pesquisa "LGPD no mercado brasileiro", desenvolvida pela Alvarez & Marsal, HLFMap, Privacy Tools, Serur Advogados e ABNT. Vale lembrar que este é o setor que mais sofre golpes no país, em um total de R$ 5,8 bilhões em 2021, aumento de 55% comparado aos 3,8% registrados em 2020, conforme estudos do Mapa da Fraude.

A baixa adesão não demonstra, necessariamente, desleixo com o negócio e a segurança dos clientes, mas, sim, que, pelo menos 60% das empresas financeiras ainda não possuem ou não dominam as ferramentas necessárias para assegurar proteção e controle do cliente à base de dados. "Essa adequação, porém, deve estar na linha de frente destas instituições nos próximos meses, não apenas pela Resolução nº 155, mas, sobretudo, por uma questão de ética, segurança e transparência. Além disso, aquelas que não cumprirem a LGPD poderão ser multadas, valor que pode chegar a 2% do faturamento total (limitado a R$ 50 milhões), e sofrer bloqueio de dados", diz Maria Cristina Diez. Em contrapartida, a organização em conformidade com as novas diretrizes tem impacto positivo em sua credibilidade, fortalecendo a imagem de ser uma empresa séria, que preza pelo sigilo de informações privativas.

Para implantar as normas, o ideal é que os administradores de bancos e instituições financeiras invistam na contratação de uma empresa especializada, que se responsabilize por conduzir todas as atividades ligadas à proteção de dados, com monitoramento sistemático e regular dos titulares. Esse profissional se chama data protection officer (DPO) ou encarregado de proteção de dados, basicamente um especialista em monitoramento e proteção de dados, com conhecimento em tecnologia da informação (TI) e base em direito. Como pré-requisito, a pessoa física ou jurídica contratada deve estar bem informada do cotidiano das transações e dos processos internos da empresa, com autonomia assegurada pelos gestores.

"A responsabilidade do DPO envolve aplicar e desenvolver ações, por meio de softwares avançados, para assegurar que tantos os dados de terceiros quanto os da própria organização sejam protegidos. Isso inclui, por exemplo, não permitir que as informações de um cliente sejam usadas ou vazadas para envio de publicidade, caso ele não tenha autorizado isso previamente. Trata-se, portanto, de um trabalho de fiscalização constante, compromissado com a ética e a idoneidade", descreve Cristina Diez, da Most Technologies.

Outras das funções estratégicas do DPO são descritas no 2º parágrafo do artigo 41 da LGPD e incluem o recebimento de comunicações e reclamações com os titulares dos dados, a fim de dar esclarecimentos e tomar providências; e prestar orientações aos colaboradores e funcionários da instituição sobre as práticas em conformidade com a legislação nacional. "Para além das normas, espera-se que a pessoa física ou jurídica contratada implemente melhorias tecnológicas, realize análises de riscos, acompanhe a evolução e a adesão do tema nos processos interno, atualize-se sobre eventuais adaptações nos termos da lei, de forma que a organização contratante esteja sempre em compliance", finaliza Cristina.