COMUNICADO

Prezados associados,

A data de vigência da Lei Geral de Proteção de Dados entrou em vigor em 18/09/2020 e, com isso, cresce a preocupação das empresas em geral de se adequarem as novas regras para o tratamento de dados pessoais.

Além disso, a partir de agosto do corrente ano, a Autoridade Nacional de Proteção de Dados (ANPD), órgão que regula, fiscaliza e exerce outras funções com base na Lei Geral de Proteção de Dados Pessoais (LGPD), iniciará as fiscalizações e poderá aplicar as primeiras multas com base na norma de dados pessoais.

Para tentar facilitar o reconhecimento de boas condutas e também das práticas que são inadequadas no dia a dia dos negócios, separamos aqui os 10 princípios que norteiam a LGPD e que devem ser respeitados.

PRINCIPAIS PONTOS DA LGPD

1) Regra para todo o território nacional
A lei passa a valer em todo Brasil, não importa se a organização ou o centro de dados estão dentro ou fora do país. O intuito é criar um cenário de segurança jurídica para todo o território nacional. Além disso, os dados poderão ser transferidos internacionalmente, contanto que o outro país também pratique a proteção de dados.

2) Definição do conceito de dados pessoais
De acordo com a LGPD, passa a ser considerada como um dado pessoal toda informação que permite identificar, direta ou indiretamente, um indivíduo que esteja vivo, tal como: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies, entre outros.

3) Consentimento do cidadão
Outro elemento essencial da LGPD é o consentir. Ou seja, o consentimento do cidadão é a base para que dados pessoais possam ser tratados. Porém, há algumas exceções. É possível tratar dados sem consentimento se isso for indispensável para cumprir critérios legais.

4) Finalidade e necessidade
A transparência com os donos dos dados será rigorosamente exigida, com o quesito de informar previamente ao cidadão a finalidade e a necessidade da solicitação de seus dados pessoais.

5) Fiscalização centralizada e agentes responsáveis
A Autoridade Nacional de Proteção de Dados Pessoais (ANPD) **– que está em formação –** fica encarregada da fiscalização e da penalização em caso de seu descumprimento da nova lei.

Além disso, fica estipulado que as organizações deverão ter agentes responsáveis pelo tratamento de dados com funções de controladores, operadores e encarregados, dependendo do porte e do volume de dados tratados.

Será exigido que gestores de base de dados pessoais das empresas realizem também a administração de riscos e falhas, com funções como redigir normas de governança; adotar medidas preventivas de segurança; replicar boas práticas e certificações existentes no mercado; elaborar planos de contingência; fazer auditorias; e resolver incidentes com agilidade. Tudo com o máximo de transparência e a responsabilidade de notificar a ANPD e os indivíduos afetados em caso de vazamento de dados.

6) Penalidades
A falta de segurança e negligência na proteção dos dados pessoais dos usuários acarretarão em multas pesadas. Organizações e subcontratadas para tratar dados vão responder em conjunto por eventuais danos causados, com multas de até 2% do faturamento anual da organização no Brasil – e no limite de R$ 50 milhões por infração. A ANDP fixará níveis de penalidade segundo a gravidade da falha com o envio de alertas e orientações prévias antes de aplicar as sanções.

7) Garantias ao cidadão
A lei traz várias garantias ao cidadão, como a possibilidade de solicitar que dados sejam deletados, revogar um consentimento e transferir dados para outro fornecedor de serviços. Dentre outros direitos do titular dos dados estão: confirmação da existência do tratamento, acesso aos dados, correção dos dados, anonimação, bloqueio e eliminação dos dados, portabilidade dos dados, informações sobre compartilhamento de dados pessoais, informação da possibilidade de não consentir o tratamento e as consequências da negativa.

10 PRINCÍPIOS DA LGPD PARA O TRATAMENTO DE DADOS PESSOAIS

1) Finalidade:
A partir da LGPD não será mais possível tratar dados pessoais com finalidades genéricas ou indeterminadas. O tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, explícitos e informados. Ou seja, as empresas devem explicar para que usarão cada um dos dados pessoais.
Essas finalidades também devem estar dentro dos limites da lei e devem vir expressamente acompanhadas de todas as informações relevantes para o titular.
Além disso, a empresa não está autorizada a modificar a finalidade durante o tratamento. Se sua startup solicita o e-mail do cliente para a finalidade específica de login na plataforma, você não pode automaticamente utilizar esse mesmo e-mail para enviar publicidade ou ofertas.

2) Adequação:
Os dados pessoais tratados devem ser compatíveis com a finalidade informada pela empresa. Ou seja, sua justificativa deve fazer sentido com o caráter da informação que você pede.
Por exemplo: se o seu negócio é um **e-commerce** de produtos eletrônicos, dificilmente será justificável pedir dados de saúde aos Usuários. Então, se não é compatível, o tratamento se torna inadequado.

3) Necessidade:
As startups e empresas em geral devem utilizar apenas os dados estritamente necessários para alcançar as suas finalidades. Procure fazer uma ponderação entre o que é realmente essencial para o seu negócio e o que é apenas conveniente.
Lembre-se que quanto mais dados você tratar, maior será a sua **responsabilidade**, inclusive em casos de vazamentos e incidentes de segurança.

4) Livre acesso:
A pessoa física titular dos dados tem o direito de consultar, de forma simples e gratuita, todos os dados que a empresa detenha a seu respeito.
Além disso, devem ser especificadas questões como: o que a empresa faz com as suas informações, de que forma o tratamento é realizado e por quanto tempo.

5) Qualidade dos dados:
Deve ser garantido aos titulares que as informações que a empresa tenha sobre eles sejam verdadeiras e atualizadas. É necessário ter atenção à exatidão, clareza e relevância dos dados, de acordo com a necessidade e com a finalidade de seu tratamento.

6) Transparência:
Todas as informações passadas pela empresa, em todos os seus meios de comunicação, devem ser claras, precisas e verdadeiras.
Além disso, a empresa não pode compartilhar dados pessoais com outras pessoas de forma oculta. Se você repassa dados pessoais para terceiros, inclusive para operadores que sejam essenciais para a execução do serviço, o titular precisa saber.

7) Segurança:
É responsabilidade das empresas buscar procedimentos, meios e tecnologias que garantam a proteção dos dados pessoais de acessos por terceiros, ainda que não sejam autorizados, como nos casos de invasões por hackers.
Além disso, devem ser tomadas medidas para solucionar situações acidentais, como destruição, perda, alteração, comunicação ou difusão dos dados pessoais de suas bases.

8) Prevenção:
O princípio da prevenção objetiva que as empresas adotem medidas prévias para evitar a ocorrência de danos em virtude do tratamento de dados pessoais. Ou seja, as empresas devem agir antes dos problemas e não somente depois.

9) Não Discriminação:

Os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares.
A própria LGPD já criou regras específicas para o tratamento de dados que frequentemente são utilizados para discriminação, os chamados **dados pessoais sensíveis**, como os que tratam sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a **sindicato** ou a organização de caráter religioso, filosófico ou político, dado referente à **saúde** ou à vida sexual e dado genético ou biométrico

10) Responsabilização e Prestação de Contas:
Além de se preocuparem em cumprir integralmente a Lei, **as empresas devem ter provas** e evidências de todas as medidas adotadas, para demonstrarem a sua boa-fé e a sua diligência.
Alguns bons exemplos estão na comprovação que fizeram treinamentos de **equipe**, a contratação de **consultorias especializadas**, a utilização de protocolos e sistemas que garantam a segurança dos dados e o acesso facilitado do titular a empresa sempre que preciso.
Assim, nosso objetivo é conscientizar nossos associados para que compreendam e internalizam a verdadeira intenção da LGPD para tornar mais fácil para as empresas desenharem seus **modelos de negócios** e executados os dados na prática.

São Caetano do Sul, 14 de julho de 2021

Conrado Orsatti
OAB/SP 194.178
JURÍDICO SEAC ABC