Lei Geral de Proteção de Dados Pessoais para RIG

Abrig
Associação Brasileira de Relações Institucionais e Governamentais

Introdução:

A Lei Geral de Proteção de Dados Pessoais (LGPD) é a nova lei que foi aprovada pelo Congresso Nacional do Brasil em 14 de agosto de 2018 e entrou em vigor em 15 de agosto de 2020. Suas sanções entrarão em vigor em 01 de agosto de 2021.

A LGPD tem como objetivo regulamentar o tratamento de dados pessoais pelas empresas, uma vez que os dados pessoais ganharam grande importância na economia moderna, pois permitem fazer predições, analisar perfis de consumo, opinião, entre outras atividades.

Mais de 126 países no mundo possuem leis para a proteção de dados pessoais visando à regulamentação do tratamento de dados das empresas, evitando-se o mau uso destes, bem como a responsabilização das empresas por isso, bem como por incidentes e acidentes com dados pessoais.

Contexto Histórico

Após anos de discussões e da unificação de diversos projetos que tramitaram na Câmara, no Senado e no Ministério da Justiça, em 14 de agosto de 2018, a Lei Geral de Proteção de Dados do Brasil (LGPD), a Lei 13.709/2018 foi finalmente sancionada. A LGPD foi baseada na General Data Protection Regulation (GPDR), regulação europeia que quando surgiu em 2012 foi considerada pioneira e inspirou outros países, assim como o Brasil, a criarem suas próprias leis.

Além da Europa e dos Estados Unidos, diversos países da América Latina, como Chile, Argentina, Uruguai e Colômbia também possuem legislação de proteção de dados vigente.

A LGPD trouxe importantes discussões no Brasil sobre privacidade e proteção de dados. Na era da informação digital em que atualmente vivemos, as recorrentes notícias sobre espionagem, vazamento de dados e abuso na utilização de dados pessoais, aumentaram a conscientização sobre privacidade e proteção de dados e a lei vem justamente para empoderar o titular de dados e garantir a transparência e direito à liberdade e à privacidade. Com a LGPD nasce uma nova cultura e deve ser encarada pelas empresas como um aspecto diferenciador para a competitividade do negócio, capaz de transmitir uma imagem de confiança perante o mercado.

A LGPD cria uma estrutura legal para o uso de dados pessoais de indivíduos no Brasil, independentemente de onde o processador de dados esteja localizado. Ela segue o modelo do Regulamento Geral de Proteção de Dados da União Européia (GDPR) e, assim como a GDPR, a LGPD tem conseqüências de grande alcance para as atividades de processamento de dados dentro e fora do Brasil.

Qual é a essência do LGPD?

A LGPD fornece nove direitos aos titulares de dados, ao definir o que constitui dados pessoais e criar dez bases legais para o processamento lícito destes dados pessoais.

Com a LGPD também se criou a Autoridade Nacional de Proteção de Dados (ANPD), que é responsável pela aplicação desta Lei, sua supervisão, orientação e execução das suas sanções administrativas previstas.

As organizações deverão nomear um Encarregado de Dados (ou DPO). Além disso, a LGPD introduz a notificação obrigatória de vazamento ou violação de dados.

A quem se aplica a LGPD?

No artigo 3º da LGPD, determina à quem ele se aplica:

a) Para quem faz o processamento de dados no território do Brasil;

b) Para quem faz o processamento de dados de indivíduos que estão dentro do território do Brasil,

independentemente de onde o controlador ou operador de dados esteja localizado;
c) Para quem faz o tratamento dos dados coletados no Brasil;

Isto significa que não são apenas os cidadãos brasileiros cujas informações e dados pessoais são protegidos, mas qualquer indivíduo cujos dados foram coletados ou processados enquanto estiverem dentro do Brasil.

Alerta para o Profissional de RIG

Toda organização (empresa) que realiza tratamento de dados pessoais deve:
1) documentar o processamento de dados pessoais desde a coleta inicial até o término;
2) fornecer uma descrição do que é coletado, a finalidade da coleta e do processamento, o tempo de retenção dos dados e com quem os dados são eventualmente compartilhados;
3) nomear um Encarregado de Dados / DPO (ver abaixo a definição deste profissional).
Quem está isento do LGPD?

O LGPD não se aplica a:

a) Dados processados por uma pessoa para fins estritamente pessoais
b) Dados exclusivamente para fins jornalísticos, artísticos, literários ou acadêmicos
c) Dados exclusivamente para segurança nacional, defesa nacional, segurança pública, investigações criminais ou atividades punitivas

Quais são os nove direitos para os Titulares dos dados sob a LGPD?

O artigo 18 da LGPD estabelece que os indivíduos titulares de dados têm os direitos de:
1) Confirmar a existência do processamento de seus dados;
2) Acessar seus dados;
3) Corrigir dados incompletos, imprecisos ou desatualizados;
4) Anonimizar, bloquear ou apagar dados desnecessários ou excessivos ou dados que não estejam sendo processados em conformidade com a LGPD;
5) Portabilidade dos dados, ou seja, transferência dos dados para outro prestador de serviço ou processador, se solicitado pelo titular;
6) Ter seus dados apagados;
7) Informações sobre entidades públicas e privadas com as quais o controlador tenha compartilhado dados;
8) Informações sobre a possibilidade de negar o consentimento e as suas consequências;
9) Revogar o consentimento.

Quais são as 19 definições na LGPD?

O artigo 5 da LGPD tem 19 definições:
1) **Dados pessoais:** Informações relativas a uma pessoa física identificada ou identificável;
2) **Dados pessoais sensíveis:** Dados pessoais relativos à origem racial ou étnica, crença religiosa, opinião política, filiação a sindicatos ou organizações religiosas, filosóficas ou políticas, dados relativos à saúde ou à vida sexual, dados genéticos ou biométricos, quando relacionados a uma pessoa natural (Pessoa Física)
3) **Dados anonimizados:** Dados relacionados a um envolvido que não pode ser identificado, considerando o uso de meios técnicos razoáveis e disponíveis no momento do processamento.
4) **Base de dados:** Conjunto estruturado de dados pessoais, mantidos em um ou vários locais, em suporte eletrônico ou físico

5) **Titular dos dados:** Uma pessoa natural e singular a quem os dados pessoais que são objeto de processamento se referem

6) **Controlador:** Pessoa física ou jurídica, de direito público ou privado, que tem competência para tomar as decisões relativas ao processamento de dados pessoais, ao determiner o propósito e meios de tratamento.

7) **Processador:** Pessoa física ou jurídica, de direito público ou privado, que processa dados pessoais em nome do controlador.

8) **Encarregado de Dados:** Pessoal física, nomeado pelo responsável pelo tratamento (controlador ou processador), que atua como canal de comunicação entre este responsável pelo tratamento para com os titulares dos dados e a ANPD

9) **Agentes de tratamento de Dados:** O controlador e o operador

10) **Tratamento de Dados:** Qualquer operação realizada com dados pessoais, como coleta, produção, recebimento, classificação, uso, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle das informações, modificação, comunicação, transferência, disseminação ou extração.

11) **Anonimização**: uso de meios técnicos suficientes e disponíveis no momento do processamento, através dos quais se perde a possibilidade de associação direta ou indireta de dados com um indivíduo.

12) **Consentimento:** Manifestação livre, expressa, informada e inequívoca pela qual o Titular dos dados concorda com o tratamento dos seus dados pessoais para um determinado fim.

13) **Bloqueio:** Suspensão temporária de qualquer operação de processamento, por meio da retenção dos dados pessoais ou do banco de dados

14) **Eliminação:** Exclusão de dados ou de um conjunto de dados armazenados em um banco de dados, independentemente do procedimento utilizado

15) **Transferência internacional de dados:** Transferência de dados pessoais para um país estrangeiro ou para uma entidade internacional da qual o país é membro

16) **Uso compartilhado de dados:** Comunicação, divulgação, transferência internacional, interconexão de dados pessoais ou processamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas, de acordo com suas competências legais, ou entre estas e entidades privadas, reciprocamente, com autorização específica, para um ou mais tipos de processamento permitidos por estas entidades públicas, ou entre entidades privadas

17) **Relatório de impacto sobre a proteção de dados pessoais:** Documentação do controlador que contém a descrição dos procedimentos de processamento dos dados pessoais que poderiam gerar riscos às liberdades civis e direitos fundamentais, bem como medidas, salvaguardas e mecanismos para mitigar o risco

18) **Órgão de pesquisa:** Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos, legalmente organizado sob a lei brasileira, com sede e jurisdição no Brasil, que inclui em sua missão institucional ou em seus objetivos corporativos ou estatutários pesquisa básica ou aplicada de natureza histórica, científica, tecnológica ou estatística

19) **Autoridade Nacional de Proteção de Dados:** Órgão da administração pública indireta responsável por supervisionar, implementar e monitorar o cumprimento da LGPD.

CONTROLADOR ou OPERADOR?

Cabe enfatizar a diferença entre Controlador e Operador de dados, nos termos da Lei:

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Quais são as 10 bases legais para o processamento lícito de dados pessoais sob a LGPD?

As dez bases jurídicas para o processamento lícito são descritas no artigo 7º:

1) Com o consentimento do titular dos dados.

2) Para o cumprimento de uma obrigação legal ou regulamentação por parte do controlador.

3) Pela administração pública, para o processamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos, ou baseadas em contratos, acordos ou instrumentos similares, sujeitos ao Capítulo IV da LGPD.

4) Para realização de estudos por entidades de pesquisa, garantindo, sempre que possível, a anonimização dos dados pessoais.

5) Quando necessário para a execução de um contrato ou procedimentos preliminares relacionados a um contrato do qual o envolvido é parte, a pedido do envolvido.

6) Para o exercício regular dos direitos em procedimentos judiciais, administrativos ou arbitrais, o último de acordo com a Lei de Arbitragem Brasileira.

7) Para a proteção da vida ou segurança física do titular dos dados ou de terceiros.

8) Para proteger a saúde, em um procedimento realizado por profissionais de saúde ou por entidades de saúde.

9) Quando necessário para atender aos interesses legítimos do responsável pelo tratamento ou de terceiros, exceto quando prevalecerem os direitos e liberdades fundamentais do titular dos dados, que exigem proteção de dados pessoais.

10) Para a proteção do crédito.

O que é a Autoridade Nacional de Proteção de Dados (ANPD)?

A Autoridade Nacional de Proteção de Dados (ANPD) é Autoridade Responsável pela aplicação da LGPD e suas sanções, como também pela sua fiscalização, interpretação e regulamentação.

Seu principal objetivo é:

a) estabelecer novas normas,

b) estabelecer padrões técnicos,

c) supervisionar,

d) auditar e educar,

e) lidar com as notificações de violação de dados e aplicar sanções necessárias.

A ANPD está vinculada ao gabinete da Presidência e tem dois órgãos:

a) **Conselho de Administração:** 5 membros com experiência em privacidade de dados e proteção de dados;

b) **Conselho Nacional:** Um conselho consultivo de 23 membros com representação do governo, da sociedade civil, de instituições de pesquisa e do setor privado.

Por que o LGPD é importante para o Profissional de RIG?

A LGPD é importante para o professional de RIG, uma vez que os Controladores ou Operadores de dados podem ser responsáveis conjunta ou separadamente por violações e vazamentos de dados, bem como pela não conformidade com a LGPD, sob pena de multa.

A LGPD é uma lei de privacidade com "aplicação extraterritorial" que significa que as organizações que processam dados pessoais de brasileiros serão obrigadas a cumpri-la, independentemente de onde eles sejam.

O Brasil tem mais de 138 milhões de internautas, tornando-o o maior mercado da Internet na América Latina e o quarto maior do mundo.

O governo brasileiro projetou a LGPD para alcançar um acordo de adequação com a UE para assegurar o livre fluxo de dados entre os dois entes.

Antes da LGPD, a proteção de dados pessoais no Brasil era aplicada por mais de 40 normas legais no plano federal, incluindo o Marco Civil da Internet e o Código de Defesa do Consumidor, ambos ainda em vigor, aplicados concomitantemente.

Na abordagem legal anterior, se tinha uma estrutura jurídica complexa, onde os direitos eram aplicados em níveis setoriais. Isto significava que indústrias diferentes tinham regulamentações diferentes. Com a LGPD se deu uma uniformização da Lei e uma centralização dos meios de controle e aplicação, através da ANPD.

Além disso, a LGPD é de aplicação transversal e multissetorial, portanto substitui e/ou complementa a estrutura regulatória setorial, fornecendo um conjunto simplificado de direitos aos indivíduos (titulares dos dados), que se aplicam em todos os setores públicos e privados e para fontes de dados online e offline.

A LGPD exige que os profissionais de RIG adotem medidas técnicas e administrativas para proteger os dados pessoais contra acesso não autorizado, destruição acidental ou legal, perda, alteração, exposição e vazamento.

Os profissionais de RIG podem ser responsabilizadas pelas ações de prestadores de serviços terceirizados com quem os dados coletados são compartilhados, razão pela qual a gestão de risco destes fornecedores se torna mais importante.

Os requisitos de notificação de violação e vazamento de dados são outra parte em que o Profissional de RIG deve se atentar. A LGPD exige que as violações e vazamentos de dados sejam notificadas à ANPD.

A LGPD não dá um prazo fixo, declarando que "o controlador deve comunicar à autoridade nacional e ao envolvido a ocorrência de um incidente de segurança que possa criar risco ou danos relevantes aos envolvidos, dentro de um período de tempo razoável, conforme definido pela autoridade nacional".

Espera-se que a ANPD defina este prazo fixo em breve, que deve seguir o padrão europeu (GDPR) de 72 horas.

MULTA e Reputação!

Em caso de descumprimento da LGPD, a multa máxima prevista é de 2% da receita bruta de uma pessoa jurídica privada, grupo ou conglomerado; calculada sobre o exercício do ano fiscal anterior, excluindo impostos, dentro de um teto total máximo de 50 milhões de reais por infração cometida.

Além da multa, uma eventual sanção aplicada pela ANPD fatalmente será noticiada pela mídia. Isto atentaria contra a reputação da sua organização, ao demonstrar falta de comprometimento com a privacidade de dados.

A privacidade de dados é um direito fundamental do indivíduo (titular dos dados), que pode inclusive ser alavancado para garantia constitucional, se aprovada a PEC 17/2019. Esta emenda constitucional altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Dentro de um ramo em que a credibilidade é imprescindível, como o nosso, uma mácula reputacional pode ser muito mais onerosa e gerar prejuízos irrecuperáveis à sua marca e/ou imagem. Isto seria pior do que qualquer multa ou sanção. Fiquem atentos!

Abrig
Associação Brasileira de Relações Institucionais e Governamentais

(61) 3327-0731 contato@abrig.org.br abrig.org.br abrig.rig abrig.rig
SHN Qd 01, Bloco A, Ed. Le Quartier Sala 1223, Brasília-DF, CEP: 70701-010