GUIA RÁPIDO

LEI GERAL DE PROTEÇÃO DE DADOS

(LGPD)

PREVCOM

Qual o seu projeto de vida?

Este Guia é um resumo da
lei nº 13.709, de 14 de agosto de 2018
e das alterações contidas na lei nº 13.853,
de 8 de julho de 2019

ARTE E EDIÇÃO:
Luiz Fernando Carneiro

PLANEJAMENTO:
Fabiana Ishikawa
Jefferson Ferreira dos Santos
Diego Galdino dos Santos

REVISÃO JURÍDICA:
Renata Malpica Caldeira Tanoue
Joseane da Silva Prado

São Paulo, 06 de novembro de 2019

SUMÁRIO

Glossário 4

Lei Geral de Proteção dos Dados (LGPD) 5

Aplicação 5

Principais objetivos 5

Princípios gerais para tratamento de dados 6

Não se aplica à LGPD 7

Fiscalização 7

Tratamento de dados pessoais 7

Aceite do titular (consentimento) 8

Direito dos titulares dos dados pessoais 8

Tratamento de dados pessoais sensíveis 9

Tratamento de dados pessoais de crianças e adolescentes 10

Término do tratamento de dados pessoais 11

Controlador e operador 11

Encarregado pelo tratamento de dados 12

Segurança e sigilo de dados 12

Boas práticas e governança 12

Responsabilidade e indenização de danos 13

Sanções 13

GLOSSÁRIO

Para acompanhar este guia, é importante compreender algumas definições estabelecidas no artigo 5º da a Lei Geral de Proteção de Dados:

ANONIMIZAÇÃO: processos e técnicas por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

CONSENTIMENTO: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

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

DADO ANONIMIZADO: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. O dado anonimizado não é considerado dado pessoal para fins de aplicação da LGPD.

DADOS PESSOAIS: é toda informação relacionada a pessoa natural identificada ou identificável, tal como nome, RG, CPF, e-mail, etc. Dados relativos a uma pessoa jurídica (tais como razão social, CNPJ, endereço comercial, etc.) não são considerados dados pessoais.

DADOS PESSOAIS SENSÍVEIS: é todo dado pessoal que pode gerar qualquer tipo de discriminação, tais como os dados 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, dado genético ou biométrico.

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

PSEUDONIMIZAÇÃO: processos e técnicas por meio dos quais um dado tem sua possibilidade de associação dificultada. O dado pseudoanonimizado é considerado dado pessoal para fins de aplicação da LGPD, tendo em vista a possibilidade de associação desse dado a uma pessoa natural. (§4º do artigo 13).

TITULAR: pessoa natural a quem se referem os dados pessoais, que são objeto de tratamento.

TRATAMENTO: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Aprovada no Brasil em agosto de 2018 e tem como base o Regulamento Geral de Proteção de Dados da União Europeia *(GDPR – General Data Protection Regulation)*.

APLICAÇÃO

Aplica-se a qualquer empresa pública ou privada, envolvida na coleta, tratamento e utilização de dados pessoais.

Vigência: agosto de 2020.

PRINCIPAIS OBJETIVOS

Além do desenvolvimento econômico e tecnológico, o principal objetivo da LGPD é respeitar os direitos fundamentais das pessoas, protegendo privacidade, intimidade e liberdade de expressão.

PRINCÍPIOS GERAIS PARA TRATAMENTO DE DADOS

Em seu artigo 6º, a LGPD define que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

FINALIDADE: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem tratamento posterior;

ADEQUAÇÃO: compatibilidade do tratamento com as finalidades informadas ao titular;

NECESSIDADE: limitação do tratamento ao necessário para a realização de suas finalidades;

LIVRE ACESSO: garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento;

QUALIDADE DOS DADOS: garantia aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

TRANSPARÊNCIA: garantia aos titulares de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os agentes de tratamento;

SEGURANÇA: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

PREVENÇÃO: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

NÃO DISCRIMINAÇÃO: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS: demonstração pelo agente da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e da eficácia dessas medidas.

NÃO SE APLICA À LGPD

O tratamento de dados pessoais realizado para fins particulares e não econômicos, jornalísticos, artísticos, acadêmicos ou para fins de segurança pública, defesa nacional e investigações penais não é abrangido pela LGPD.

FISCALIZAÇÃO

A ANPD (Autoridade Nacional de Proteção dos Dados) é o órgão responsável por fiscalizar e regulamentar os critérios da LGPD e tem, dentre outras, as seguintes competências:

- Zelar pela proteção dos dados pessoais;
- Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais;
- Decidir sobre a interpretação da LGPD, inclusive sobre casos omissos;
- Requisitar informações às empresas que realizam tratamento de dados;
- Implementar mecanismos para o registro de reclamações;
- Fiscalizar e aplicar sanções.

TRATAMENTO DE DADOS PESSOAIS

Somente poderá ser realizado nas seguintes hipóteses:

- Mediante o fornecimento de consentimento pelo titular;
- Para o cumprimento de obrigação legal ou regulatória pelo controlador;
- Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
- Para a realização de estudos por órgão de pesquisa;
- Quando necessário para a execução de contrato ou de procedimentos relacionados, a pedido do titular dos dados;
- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- Para a tutela da saúde;
- Quando necessário para atender aos interesses legítimos do controlador ou de terceiro; ou
- Para a proteção do crédito.

ACEITE DO TITULAR (CONSENTIMENTO)

- Fornecimento do aceite pelo titular, por escrito ou por outro meio que demonstre sua vontade;
- Cabe à empresa provar que o aceite foi obtido de forma legal;
- Proibido o tratamento de dados sem o aceite do titular;
- O aceite não poderá ser para finalidade genérica, sob pena de nulidade;
- O titular terá o acesso facilitado às informações sobre o tratamento de seus dados.

DIREITO DOS TITULARES DOS DADOS PESSOAIS

Em seu artigo 18, a LGPD traz os direitos dos titulares de dados pessoais. Os titulares poderão solicitar, a qualquer momento:

- Confirmação da existência de tratamento;
- Acesso aos seus dados;
- Correção de dados;
- Anonimização, bloqueio ou eliminação de dados tratados em desconformidade com a LGPD;
- Portabilidade dos dados;
- Eliminação dos dados;
- Informação sobre compartilhamento de dados;
- Informação sobre a possibilidade e consequências de não fornecimento de consentimento;
- Revogação do consentimento;
- Revisão decisões automatizadas.

TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Somente poderá ocorrer nas seguintes hipóteses:

- Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
- Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
  - Cumprimento de obrigação legal ou regulatória pelo controlador;
  - Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
  - Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
  - Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
  - Proteção da vida ou da incolumidade física do titular ou de terceiro;
  - Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
  - Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados.

- É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, assistência farmacêutica e de assistência à saúde, desde que observado o § 5º do artigo 11 da LGPD, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:
  - A portabilidade de dados quando solicitada pelo titular; ou
  - As transações financeiras e administrativas resultantes do uso e da prestação dos serviços descritos acima.

- É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

Deverá ser realizado em seu melhor interesse, nos termos da LGPD e da legislação pertinente.

- O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal;
- No tratamento dos dados, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos;
- Poderão ser coletados dados pessoais de crianças sem consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem consentimento;
- Os controladores não deverão condicionar a participação de crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade;
- O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis;
- As informações sobre o tratamento dos dados deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

TÉRMINO DO TRATAMENTO DE DADOS PESSOAIS

Deverá ocorrer nas seguintes hipóteses:

- Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- Fim do período de tratamento;
- Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º da LGPD, resguardado o interesse público; ou
- Determinação da autoridade nacional, quando houver violação ao disposto na Lei;
- Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
    - Cumprimento de obrigação legal ou regulatória pelo controlador;
    - Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
    - Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na Lei; ou
    - Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CONTROLADOR E OPERADOR

CONTROLADOR: empresa a quem compete as decisões referentes ao tratamento de dados pessoais.

OPERADOR: empresa que realiza o tratamento de dados pessoais em nome do controlador.

Ambos devem manter registro das operações de tratamento de dados que realizarem. A autoridade nacional (ANPD) poderá determinar ao controlador que elabore relatório de impacto à proteção de dados, contendo a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e mecanismos de mitigação de riscos adotados.

ENCARREGADO PELO TRATAMENTO DE DADOS

O controlador deverá indicar um profissional encarregado (pessoa física ou jurídica) pelo tratamento de dados pessoais, o qual deverá conhecer em detalhes todas as operações da empresa.

Ao encarregado caberá aceitar reclamações e comunicações dos titulares, receber comunicações da autoridade nacional, e orientar os funcionários e contratados sobre as práticas a serem adotadas em relação ao tratamento e proteção dos dados.

SEGURANÇA E SIGILO DE DADOS

A empresa deve adotar medidas de segurança aptas à proteção dos dados desde a coleta até a sua exclusão. É necessário comunicar à autoridade nacional e ao titular sobre eventuais incidentes de segurança que possam acarretar risco ou danos.

Medidas técnicas também devem ser implantadas para tornar os dados ininteligíveis em caso de incidente de segurança.

BOAS PRÁTICAS E GOVERNANÇA

Formulação de regras de boas práticas e de governança que estabeleçam:

- As condições de organização;
- O regime de funcionamento;
- Os procedimentos de reclamações e solicitações de usuários;
- As normas de segurança;
- Os padrões técnicos;
- As obrigações específicas para os envolvidos no tratamento;
- As ações educativas;
- Os mecanismos internos de supervisão e de mitigação de riscos;
- Demais aspectos relacionados ao tratamento de dados pessoais.

RESPONSABILIDADE E INDENIZAÇÃO DE DANOS

A empresa será obrigada à reparação de danos causados no exercício da atividade de tratamento de dados sempre que um incidente de segurança ocorrer e causar danos aos titulares dos dados envolvidos.

Os agentes não serão responsabilizados quando provarem não terem realizado o tratamento de dados, não terem violado a LGPD ou quando o dano for decorrente de culpa exclusiva do titular dos dados.

SANÇÕES

As sanções administrativas para o descumprimento da LGPD estão previstas no art. 52. São elas:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples, de até 2% do faturamento líquido da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada, no total, a R$ 50.000.000,00 por infração;
- Multa diária;
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- Bloqueio dos dados pessoais envolvidos na infração até a sua regularização;
- Eliminação dos dados pessoais envolvidos na infração.

Avenida Brigadeiro Luís Antônio, 2701 - São Paulo/SP
prevcom.com.br facebook.com/prevcom twitter.com/spprevcom

APOIO: