LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

FIEMG

Realização:
Federação das Indústrias do Estado de Minas Gerais

Elaboração:
Paulo Soares Ribeiro de Oliveira
Ana Paula Bicalho Brandão

Atualizada em setembro/2020

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Lei nº 13.709/2018

1

A LGPD

A Lei nº 13.709, de 14/8/2018, denominada Lei Geral de Proteção de Dados – LGPD, sancionada em agosto de 2018 tem como objetivo a regulamentação do tratamento de dados pessoais, por meios físicos ou digitais, seja por pessoa natural ou jurídica de direito público ou privado.

Tal regulamentação se destina a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, ou seja, de clientes e usuários, impondo padrões de segurança e responsabilidade pela sua manutenção e utilização, além da previsão de sanções de cunho reputacional e pecuniário.

Inserida em um contexto global, e claramente inspirada no Regulamento Europeu – General Data Protection Regulation (GDPR), que passou a ser obrigatório em 25 de maio de 2018 e aplicável a todos os países da União Europeia –, decorre também de um movimento global de demanda pela adoção de padrões de tratamento de dados pessoais, com maior segurança e transparência, principalmente em decorrência do valor comercial dos dados pessoais, vistos atualmente como verdadeiro ativo de grande lucratividade.

2

Fundamentos da LGPD

Conforme o artigo 2º, são fundamentos da LGPD:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

3

Aplicação da lei

Essa lei se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;

III - os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

4

Exceções quanto à aplicabilidade

A LGPD não se aplica ao tratamento de dados pessoais quando: realizado por pessoa natural para fins exclusivamente particulares e não econômicos; realizado para fins exclusivamente jornalísticos e artísticos ou acadêmicos, de segurança pública, de defesa nacional, de segurança do Estado ou atividades de investigação e repressão de infrações penais; provenientes de fora do território nacional e que não seja objeto de comunicação, uso compartilhado com agentes de tratamento brasileiros ou objeto de transferência de dados com outro país que não o de proveniência, desde que este país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nessa Lei.

5

Conceitos

Alguns termos são indispensáveis para entendermos a Lei Geral de Proteção de Dados Pessoais e sua abrangência.

Dado pessoal: informação relacionada à pessoa natural identificada ou identificável

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural

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

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento

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

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)

Agentes de tratamento: o controlador e o operador

Tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção,

classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo

Pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

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

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados

Eliminação: exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre estes e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados

Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco

Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos, legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico

Autoridade Nacional de Proteção de Dados – ANPD: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional

6

Bases legais para o tratamento de dados pessoais

O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

Com consentimento do titular

Para o cumprimento de obrigação legal

Pela administração pública, para execução de políticas públicas

Para a realização de estudos por órgão de pesquisa

Para a execução de contrato

Para a proteção da vida

Para a tutela da saúde

Para atender aos interesses legítimos do controlador

Para proteção do crédito

Para o exercício regular de direitos em processo judicial, administrativo ou arbitral

7

Tratamento de dados pessoais sensíveis

Somente poderá ocorrer nas seguintes hipóteses:

Com o consentimento do titular, de forma específica e destacada para finalidades específicas.

Sem o consentimento do titular, nas hipóteses em que for indispensável:

- Para o cumprimento de obrigação legal
- Pela administração pública, para execução de políticas públicas
- Para a realização de estudos por órgão de pesquisa
- Para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral
- Para a proteção da vida
- Para a tutela da saúde
- Para a garantia da prevenção à fraude e segurança do titular

8

Compartilhamento de dados pessoais sensíveis

A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores, com o objetivo de obter vantagem econômica, poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional.

9

Tratamento de dados pessoais de crianças e de adolescentes

O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, bem como com o consentimento específico e destaque dado por, pelo menos, um dos pais ou responsável legal. Nesse caso, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para livre acesso aos dados pelo titular.

Poderão ser coletados dados pessoais de crianças sem o consentimento quando a coleta for necessária para contatar pais/responsável legal, podendo ser utilizada uma única vez e sem armazenamento, ou para a proteção delas. Em nenhum caso, esses dados poderão ser repassados a terceiro.

Os controladores não deverão condicionar a participação dos titulares com consentimento dos pais ou responsável legal em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

10

Dados pessoais anonimizados

Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

11

Término do tratamento de dados

O término do tratamento de dados deverá ocorrer: quando for alcançada a finalidade ou os dados deixarem de ser necessários ou pertinentes; ao final do período de tratamento; a partir da solicitação do titular, resguardado o interesse público; por determinação da ANPD, quando houver violação da LGPD.

Os dados pessoais deverão ser eliminados após o término do seu tratamento, no âmbito e nos limites técnicos das atividades.

É autorizada a conservação dos dados pessoais 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; uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que essa comunicação seja comprovadamente impossível ou implique esforço desproporcional.

12

Direitos do titular

A Lei estabelece que o titular dos dados pessoais tem direito a receber do controlador, a qualquer momento e mediante solicitação expressa do titular ou de representante legal:

- confirmação da existência de tratamento de dados;
- acesso aos dados;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei;
- portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, observados os segredos comercial e industrial (exceção para dados já anonimizados pelo Controlador);
- eliminação dos dados pessoais, ressalvadas as exceções aqui tratadas.
- informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- revogação do consentimento.

O controlador deverá atender à solicitação do titular em formato simplificado e imediatamente ou por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 dias, contado da data do requerimento do titular.

Os dados serão fornecidos a critério do titular, por meio eletrônico, seguro e idôneo ou sob a forma impressa.

O titular também tem o direito de rever as decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem os seus interesses. Os critérios e procedimentos para decisão automatizada devem ser fornecidos sempre que solicitados.

Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

A defesa do interesse e dos direitos dos titulares poderá ser exercida em juízo, individual ou coletivamente.

No caso de processo civil, o juiz poderá inverter o ônus da prova a favor do titular dos dados quando for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

13

A LGPD e o Poder Público

O tratamento de dados pessoais por empresas do Poder Público deverá ser realizado, observadas as determinações da LGPD, para atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

O Poder Público não pode transferir para empresas privadas dados pessoais constantes em suas bases de dados, exceto: para a execução de atividade descentralizada que exija a transferência para esse fim específico; quando os dados forem acessíveis publicamente; quando houver previsão legal ou contrato; para prevenção de fraudes ou irregularidades.

14

Transferência internacional de dados

A transferência internacional de dados será avaliada pela ANPD e somente poderá ocorrer, conforme artigo 33:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação

jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade prevista na lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades;

IX - quando necessário para atender obrigação legal ou regulatório pelo controlador, execução de contrato ou para proteção da vida.

15

Relatório de Impacto

A ANPD poderá determinar ao controlador que elabore um relatório de impacto à proteção de dados pessoais, inclusive dados sensíveis, referente a suas operações de tratamento de dados, observados os segredos comercial e industrial.

Esse relatório deve conter, no mínimo, a descrição dos tipos de dados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação às medidas, salvaguarda e mecanismos de mitigação de risco adotados.

16

Responsabilidades dos agentes de tratamento

O operador deverá realizar o tratamento dos dados de acordo com as instruções do controlador. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.

O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Qualquer pessoa que intervenha em uma das fases de tratamento obriga-se a garantir a segurança da informação.

O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da LGPD ou quando não tiver seguido as instruções lícitas

do controlador – hipótese em que o operador equipara-se ao controlador. E o controlador que estiver diretamente envolvido no tratamento do qual decorrerem danos ao titular também responde solidariamente.

Conforme o artigo 43, os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados;

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

O controlador deverá indicar um encarregado pelo tratamento de dados pessoais, que terá sua identidade e informações divulgadas publicamente, de forma clara e objetiva, preferencialmente no site do controlador.

O encarregado será responsável por aceitar reclamações e comunicações dos titulares e prestar esclarecimentos; receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e os contratados a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

17

Tratamento irregular de dados pessoais

O tratamento de dados pessoais será tido como irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular espera, consideradas as circunstâncias relevantes: modo pelo qual é realizado, o resultado e os riscos que razoavelmente dele se esperam, as técnicas de tratamento disponíveis à época em que foi realizado.

18

Segurança dos sistemas utilizados

Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança, aos princípios previstos na LGPD e às demais normas regulares.

A LGPD trata da segurança dos dados observando a tecnologia disponível na época do tratamento.

19

Comunicação sobre incidentes

O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A comunicação deverá ser feita em prazo razoável e conter, conforme o artigo 48:

- descrição da natureza dos dados pessoais afetados;
- informações sobre os titulares envolvidos;
- indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- riscos relacionados ao incidente;
- motivos da demora, no caso de a comunicação não ter sido imediata;
- medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A ANPD poderá, caso seja necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a ampla divulgação do fato em meios de comunicação e a adoção de medidas para reverter ou mitigar os efeitos do incidente.

20

Sanções

Em razão de infrações cometidas às normas previstas na LGPD, a ANPD poderá aplicar:

1. advertência, com indicação de prazo para adoção de medidas corretivas;

2. multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

3. multa diária, observado o limite total a que se refere o item 2;

4. publicização da infração após devidamente apurada e confirmada a sua ocorrência;

5. bloqueio dos dados pessoais aos quais se refere a infração até a sua regularização;

6. eliminação dos dados pessoais aos quais se refere a infração;

7. suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

8. suspensão do exercício da atividade de tratamento dos dados pessoais aos quais se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

9. proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Conforme o artigo 52, as sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas;

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

As sanções referentes aos itens 7, 8 e 9 somente poderão ser aplicadas após já ter sido imposta, ao menos, uma das sanções de que tratam os itens 2, 3, 4, 5 e 6 para o mesmo caso concreto e em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos.

Os vazamentos individuais ou os acessos não autorizados poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades previstas na LGPD.

O valor da sanção de multa diária aplicável às infrações da Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela ANPD.

21

Orientações iniciais para o atendimento à LGPD

Para atender às exigências da LGPD, estabeleceu-se um roteiro, apresentado a seguir, com as principais ações a serem adotadas pelas organizações.

• Orientar seus empregados sobre a LGPD, ressaltando a responsabilidade de cada um na preservação dos dados pessoais de clientes e colaboradores.

• Providenciar a nomeação do Encarregado de Proteção de Dados – pessoa física ou jurídica responsável pela interlocução entre Autoridade Nacional de Proteção de Dados (ANPD), organização e titulares.

• Disponibilizar, de forma clara e objetiva, preferencialmente no site da organização, a identidade e as informações de contato do Encarregado.

• Estabelecer o canal de comunicação que receberá as solicitações dos titulares, preparando-se, portanto, para processá-las e atendê-las no que couber.

• Revisar os instrumentos jurídicos (como contrato de trabalho, contrato de prestação de serviço e convênio) e estabelecer cláusula contratual de proteção de dados.

• Realizar o mapeamento dos fluxos de dados: levantar todas as atividades que utilizam dados pessoais, considerando quando e por que são coletados, onde são armazenados, quem são os responsáveis, para que são utilizados e quando são eliminados.

• Realizar um diagnóstico de proteção de dados: executar análise de alinhamento dos processos que utilizam dados pessoais com as exigências da LGPD, bem como uma análise da maturidade da organização e a avaliação de riscos no tratamento de dados pessoais.

• Estabelecer ou revisar a política de Segurança da Informação, incluindo diretrizes sobre os cuidados necessários para a preservação dos dados pessoais.

• Estabelecer ou revisar a política de Privacidade, incluindo diretrizes que promovam a proteção dos direitos dos titulares dos dados pessoais.

• Estabelecer e implementar planos de ação para a adequação de processos e meios, visando atender às exigências da lei.

• Definir mecanismo contínuo de monitoramento da efetividade das ações de proteção de dados implementadas.

• Orientar os empregados sobre as práticas relacionadas à proteção de dados adotadas pela organização.

Para obter mais informações sobre este tema, acesse o site da FIEMG.


FIEMG