INFORMATIVO LGPD

Lei Geral de Proteção de Dados

SSBM

SCAVAZZINI SURIANO BENINI MINELLI ADVOGADOS

Sobre

Elaborado pelo SSBM ADVOGADOS, este informativo é um ponto de partida para você conhecer a Lei Geral de Proteção de Dados, a LGPD.

Este material foi elaborado no formato de perguntas e respostas e tem como objetivo facilitar a compreensão de uma lei que terá amplo impacto social, abrangendo as relações de trabalho, consumo, educação, saúde e que vai alterar o modo como nos relacionamos com a internet.

Informar e tornar acessível o entendimento da lei, estes os objetivos que guiaram o nosso trabalho.

Índice

Introdução

O que é a LGPD?

> “Os dados são o novo petróleo. Clive Humby.”

LGPD é a sigla da “Lei Geral de Proteção de Dados”, lei nº 13.709 de 2018. A lei possui como objetivo regular o uso dos dados pessoais pelas empresas públicas e privadas.

Como destacou o matemático britânico Clive Humby, os dados pessoais são tão valiosos quanto o petróleo. A partir da análise dos nossos dados, que são compartilhados por ocasião das nossas relações de consumo e trabalho, é possível extrair infinitas aplicações, seja para descobrir nossos gostos e interesses com a criação de perfis de consumo de modo a possibilitar ofertas cada vez mais personalizadas e permitir que transações fraudulentas sejam descobertas com base na análise dos padrões de uso do cartão de crédito.

De modo prático, muito provavelmente você já constatou que uma simples pesquisa da palavra “tênis” no seu navegador faz com que ofertas desse item de consumo apareçam em todas as suas redes sociais.

O uso indiscriminado das nossas informações passou a gerar incômodo na sociedade e preocupação dos governos, a exemplo dos casos que envolveram a rede de lojas de departamentos americana TARGET[1] e a denúncia do FACEBOOK no caso CAMBRIGDE ANALYTICA[2], objeto do documentário “Privacidade Hackeada”.

Tais ocorrências, que tornaram público o que pode ser feito com o uso inadequado dos nossos dados pessoais, aceleraram o processo de elaboração de leis e regulações e, aqui no Brasil, da LGPD.

É fundamental destacar que a LGPD não proíbe o uso dos dados pessoais, ela apenas dispõe como podem ser utilizados.

A adequação à LGPD, portanto, é a regra. Tanto o setor privado como público devem iniciar o processo de adequação, com a implementação de programas de proteção de dados.

Muito embora o processo de adequação não seja fácil, a sua implementação apresenta inúmeras vantagens, principalmente para as empresas privadas. O desenvolvimento do programa de proteção dos dados pessoais contribui para formar uma imagem de confiança perante o consumidor.

Porém, caso nada seja feito, é possível sofrer, além das penalidades previstas na lei, a perda de credibilidade com os parceiros comerciais e consumidores com o abalo da imagem da empresa infratora.

Mas, o que é um dado pessoal? Quais os princípios desta lei? Qual o órgão governamental que regula a sua aplicação?

Principalmente, o que a LGDP visa proteger?

As respostas a estas e outras perguntas você encontra aqui.

[1] https://ssbm.com.br/caso-target/
[2] https://pt.wikipedia.org/wiki/Esc%C3%A2ndalo_de_dados_Facebook%E2%80%93Cambridge_Analytica

O que é um dado pessoal? E dado pessoal sensível?

Dado pessoal

É toda informação relacionada à pessoa natural identificada ou identificável, como por exemplo: nome, RG, CPF, e-mail, número de IP, dados de geolocalização, entre outros. Assim, toda e qualquer informação que identifica ou pode identificar uma pessoa é considerada dado pessoal.

Dado pessoal Sensível

É todo dado pessoal 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, quando vinculado a uma pessoa natural.

A LGPD trata de forma muito cuidadosa os dados sensíveis, pois são informações capazes de gerar atos de discriminação aos seus titulares.

Para que alguém possa coletar este tipo de informação, a LGDP, salvo algumas exceções, exige o prévio consentimento do titular de dados, o que também será explicado neste informativo.

PARA ANOTAR: Dados de Pessoa Jurídica (como CNPJ, endereço da sede, telefone) não são considerados dados pessoais.

Quais os fundamentos da LGPD?

Os fundamentos da LGPD são:

• o respeito à privacidade;
• a autodeterminação informativa;
• a liberdade de expressão, de informação, de comunicação e de opinião;
• a inviolabilidade da intimidade, da honra e da imagem;
• o desenvolvimento econômico e tecnológico e a inovação;
• a livre iniciativa, a livre concorrência e a defesa do consumidor; e
• os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A LGDP pretende garantir, em resumo, que o uso das nossas informações não seja feito com invasão à nossa privacidade, que possamos ter o controle sobre o uso dos nossos dados (autodeterminação informativa) e também, ao mesmo tempo, seja mantido o nosso direito à livre manifestação de pensamento.

Igualmente, o controle sobre o uso dos nossos dados não pode ser feito de modo a inviabilizar o desenvolvimento econômico, muito menos impedir a evolução tecnológica em conjunto com os inúmeros benefícios trazidos pelas práticas inovadoras que utilizam nosso dados pessoais.

A LGPD busca preservar o desenvolvimento econômico e do próprio mercado, ao regular e não proibir a utilização dos nossos dados pessoais, combinados com o direito ao exercício do nosso poder de cidadania.

E quais são os princípios da LGPD?

A LGPD apresenta uma série de princípios que devem ser considerados no tratamento de dados pessoais.

São eles:

I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades;

IV - Livre acesso: os titulares devem poder consultar, de maneira facilitada e gratuita, sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - 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;

VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - 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;

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

IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - 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, inclusive, da eficácia dessas medidas.

Assim, todo e qualquer uso dos dados pessoais deve ter uma finalidade específica, garantindo ao titular de dados o direito ao acesso sobre suas informações de modo transparente e seguro, as quais não podem ser utilizadas para fins que causem prejuízo.

O que significa tratamento de dados?

O tratamento de dados pessoais é qualquer operação realizada com os dados pessoais de uma pessoa, contemplando inúmeras atividades. Exemplificando: coleta, utilização, transmissão, arquivamento, eliminação, avaliação, distribuição, reprodução, processamento, entre outras.

Assim, sempre que você ouvir falar sobre "tratamento de dados", basta pensar que é a ação que abrange todo e qualquer uso dos dados pessoais.

PARA ANOTAR: A LGDP se aplica tanto aos dados armazenados em meio físico como digital.

A quem a LGPD se aplica?

A LGPD se aplica a todos aqueles que realizam o tratamento de dados pessoais no âmbito das relações privadas – de uma microempresa até uma multinacional - e públicas, desde que a operação de tratamento seja realizada no Brasil, ou que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos situados no Brasil.

Independentemente do tamanho da empresa, se você trata de dados pessoais, incide a LGPD.

Quem é quem na LGPD?

Além da figura do titular dos dados, que é toda pessoa física, a LGDP também apresenta a figura do controlador, do operador e do encarregado, também conhecido pela sigla em inglês, DPO (Data Protection Officer).

Controlador e operador são considerados agentes de tratamento, ou seja, as pessoas que realizam as operações de tratamento com dados pessoais.

Vamos descobrir aqui qual o papel de cada um.

• **TITULAR DE DADOS:** o titular é a pessoa física a quem os dados pessoais são vinculados.

• **AGENTES DE TRATAMENTO:**

Controlador – o controlador é a pessoa responsável por tomar as decisões referentes aos dados pessoais. O controlador pode ser pessoa física ou jurídica do setor privado e público e é responsável por determinar como os dados serão usados.

Operador – o operador é a pessoa que realiza o tratamento de dados em nome do controlador. Também pode ser pessoa física ou jurídica e do setor público ou privado. Na hipótese de descumprimento das regras da LGDP, o operador responde pelos eventuais danos em conjunto com o controlador.

• **ENCARREGADO** – o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, o titular de dados e a Autoridade Nacional de Proteção de Dados (ANPD), órgão sobre o qual falaremos mais adiante.

O encarregado também pode ser pessoa física ou jurídica, podendo ser externo ou que já trabalha na instituição. Os seus dados de contato devem ser divulgados publicamente, de forma clara e objetiva, de preferência no site da empresa que controla os dados pessoais.

Como é a figura do CONTROLADOR e OPERADOR na prática?

Por exemplo, imagine uma empresa X que comercializa aparelhos de ar condicionado. Neste caso, a empresa X figura como CONTROLADORA dos dados dos seus clientes. Porém, ao contratar uma empresa de transportes Y para entregar os aparelhos, a transportadora será a OPERADORA.

Caso algum dos clientes da empresa X tenha dúvidas sobre como a empresa Y cuida dados pessoais, ele poderá ser atendido pelo Encarregado da empresa X.

PARA ANOTAR: a figura do encarregado é obrigatória. Contudo, a ANPD poderá estabelecer situações em que o encarregado pode ser dispensado, o que irá depender da natureza, do porte e do volume de dados da entidade.

Quando é possível o tratamento de dados?

A LGPD regula as hipóteses de tratamento dos dados pessoais: toda e qualquer operação feita com dados pessoais.

Cada uma das hipóteses de uso dos dados pessoais é chamada de base legal. O tratamento somente pode ser feito se atendida pelo menos uma base legal.

Assim, o tratamento de dados pode ser realizado:

Sem o consentimento quando

• Para o cumprimento de obrigação legal ou regulatória pelo controlador;

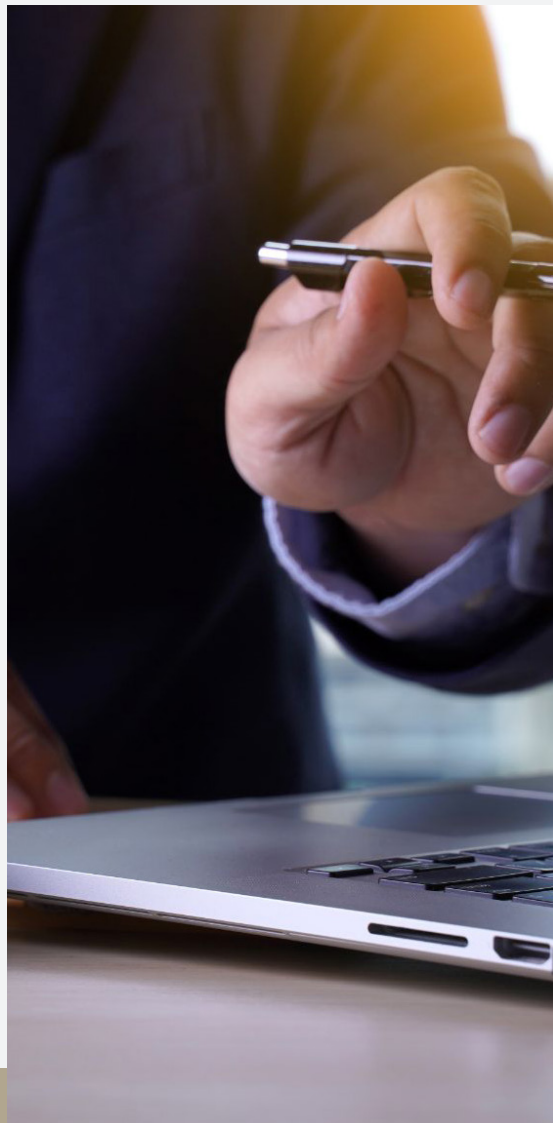
• Pela administração pública com o objetivo de execução de políticas públicas;

• Para a realização de estudos por órgão de pesquisa, garantindo, sempre que possível, tornar os dados anônimos;

• Para a execução de contrato ou de procedimentos preliminares relacionados a contrato em que o titular seja parte;

• Para o exercício legal do direito;

• Para a proteção da vida ou da incolumidade física do titular ou de terceiros;



• Para a tutela da saúde, apenas em procedimentos realizados por profissionais da saúde, serviços de saúde ou autoridade sanitária;

• Para atender ao interesse legítimo do controlador ou de terceiros. Existe o legítimo interesse quando a finalidade do tratamento visa apoiar ou promover as atividades do controlador. Neste caso, só podem ser tratados os dados estritamente necessários, com respeito aos direitos e liberdades do titular. Exemplo: o tratamento de dados voltado para a finalidade específica de proteção e prevenção à fraude.

• Para a proteção do crédito.

Com o consentimento quando

• Não se enquadrar em nenhuma outra base legal.

PARA ANOTAR: Na hipótese do uso de dados pessoais de criança e adolescente, é preciso o consentimento específico e em destaque dado pelo responsável legal.

Caso os dados sejam necessários para contatar o responsável legal ou para a proteção, é possível o tratamento sem o consentimento, desde que seja uma única vez, sem armazenamento e sem compartilhamento.

O que é consentimento?

O consentimento é uma manifestação livre, consciente e informada em que o titular dos dados concorda com o tratamento para uma finalidade determinada. É apenas uma das bases legais que fundamentam o tratamento e deve ser feito quando não for possível utilizar as outras hipóteses legais, isto porque **o consentimento possui várias regras para ser considerado válido.**

O consentimento pode ser feito por escrito ou por outro meio que demonstre a vontade do titular. Caso seja por escrito, deve estar em cláusula destacada e específica. O importante é que o meio usado para dar o consentimento não dê margem à dúvida quanto à intenção do titular. Como cabe ao controlador e/ou o operador comprovarem a existência do consentimento (guardando os registros de quando, para que e como o titular consentiu) a empresa deve manter todas as informações atualizadas, sob o risco de não poder utilizar posteriormente como meio de prova.

A revogação do consentimento pode ser feita a qualquer momento pelo titular de dados e, para o exercício desta opção, dever ser disponibilizada uma forma fácil e acessível.

O que o consentimento deve conter?

• A finalidade do tratamento de modo específico, lembrando-se que deve ser livre, consciente e informado.

• Informações sobre o compartilhamento de dados (caso o dado seja compartilhado, indicar com quem poderá ocorrer o compartilhamento);

• O período de duração do tratamento;

• A possibilidade de o titular recusar e as consequências da negativa.

PARA ANOTAR: a LGPD considera nulas as cláusulas genéricas de consentimento. Assim, janelas que pedem um aceite para a coleta de "cookies", com frases como "ao continuar navegando você aceita nossas condições", não caracteriza consentimento para fins de atendimento à LGPD.

E os meus direitos como titular dos dados?

A LGDP garante uma série de direitos ao titular de dados. São eles:

- Confirmação da existência do tratamento;
- Acesso aos dados;
- Correção de dados;
- Anonimização, bloqueio e eliminação de dados;
- Portabilidade de dados;
- Eliminação dos dados tratados com o consentimento do titular;
- Informação sobre compartilhamento de dados pessoais;
- Informação sobre a possibilidade de não consentir com o tratamento e as consequências da negativa;
- Revogação do consentimento;
- Direito de petição perante à ANPD em relação aos dados e contra o controlador;
- Revisão das decisões tomadas unicamente com base em tratamento automatizado dos dados.

Para as empresas que precisam se adequar à LGDP, é muito importante disponibilizar ao consumidor caminhos de fácil acesso para que seus clientes possam exercer com facilidade seus direitos, de preferência indicando-os de maneira expressa, a exemplo do quadro que segue[3]:

Confirmação da Existência de Tratamento	Acesso aos Dados	Anonimização
Bloqueio	Eliminação de Dados	Portabilidade dos Dados
Eliminação dos Dados Pessoais Tratados com o Consentimento do Titular	Informações das Entidades Públicas e Privadas	Oposição ao Uso de Dados
Revogação do Consentimento	Revisão de Decisões Automatizadas	

PARA ANOTAR: Em caso de vazamento de dados, o titular de dados deve ser informado sobre a ocorrência do incidente de segurança na hipótese de eventual risco ou dano.

[3] https://privacyportal-br.onetrust.com/webform/d36b4f83-ef4d-49be-8caa-4e431e6be768/c0cabc58-8a34-4f2b-a-762-38c584eeaebe

O que é a Autoridade Nacional de Proteção de Dados - ANPD?

A Autoridade Nacional de Proteção de Dados – ANPD www.gov.br/anpd/pt-br é o órgão responsável pela fiscalização, controle, implementação e regulamentação da LGPD, sendo também a autoridade responsável pela aplicação das sanções, ou seja, as penalidades pelo descumprimento da lei – com início de vigência a partir de 1º de agosto de 2021.

Além da ANPD, outros órgãos como o PROCON e o Ministério Público, podem exigir a adequação à LGPD, demandando a responsabilização dos infratores, inclusive por danos morais. É fundamental, portanto, que a adequação à LGPD ocorra o mais rápido possível.

PARA ANOTAR: é importante um acompanhamento constante da ANPD, pois a LGPD contém vários pontos que dependem da sua regulamentação. Isso significa que nem todas as obrigações estabelecidas pela lei estão claras, o que reforça a necessidade de atenção com o tema.

Em quais hipóteses a lei não se aplica?

A LGPD não se aplica a toda e qualquer operação de tratamento de dados, sendo que os dados podem ser utilizados sem necessário enquadramento nas respectivas bases legais nas seguintes hipóteses:

- Uso particular e não econômico;
- Matérias jornalísticas;
- Fins artísticos;
- Pesquisas acadêmicas;
- Para fins de segurança pública, defesa nacional, segurança do Estado e para atividades de investigação e repressão de infrações penais.

A lei também não se aplica a dados de origem estrangeira que não se comunicam e nem são compartilhados com agentes de tratamento brasileiros.

O que são incidentes de segurança?

Os dados pessoais devem ser protegidos por meio de medidas técnicas e administrativas eficazes, de modo a evitar acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.

Quando essa proteção é violada, ocorre um incidente de segurança. Nesses casos, a ANPD recomenda que seja realizada:

• A avaliação do incidente, considerando a natureza, categoria e quantidade de titulares e dados afetados, assim como as consequências concretas e prováveis.

• A comunicação do incidente ao Encarregado de Proteção de Dados Pessoais, ao controlador (caso a violação ocorra com o operador) e à ANPD e ao titular de dados, em caso de risco ou dano relevante aos titulares. Nesse último caso, a atual recomendação é que a comunicação seja feita em até 2 dias úteis.

• A elaboração de documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, a fim de cumprir o princípio de responsabilização e prestação de contas.

Quais são as penalidades para o descumprimento da lei?

Em caso de descumprimento da lei, os infratores estão sujeitos às seguintes penas:

• Advertência, com indicação de prazo para adoção de medidas corretivas;

• Multa: que pode ser simples ou diária de até 2% (dois por cento) do faturamento 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;

• Publicização: após devidamente apurada e confirmada a sua ocorrência, com possibilidade de sanção em caso de vazamento de dados pessoais;

• Bloqueio dos dados a que se refere a infração até a sua regularização;

• Eliminação dos dados a que se refere a infração;

E quais os critérios e parâmetros para aplicação das multas?

A ANPD irá aplicar as sanções de acordo com o caso concreto e considerando os seguintes critérios e parâmetros:

• A gravidade e a natureza das infrações e dos direitos pessoais afetados;

• A boa-fé do infrator;

• A vantagem obtida ou pretendida pelo infrator;

• A condição econômica do infrator;

• A reincidência;

• O grau do dano;

• A cooperação do infrator;

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

• A adoção de política de boas práticas e governança;

• A pronta adoção de medidas corretivas;

• A proporcionalidade entre a gravidade e a intensidade da sanção.

O que deve ser feito?

A empresa deve elaborar um plano de trabalho multidisciplinar para traçar quais os principais pontos que precisam ser abordados, estabelecendo prioridades para fins de implementar o programa de proteção de dados.

Escolhida a equipe de trabalho, a empresa deve indicar o Encarregado, profissional que coordenará as ações de treinamento e conscientização da equipe, mapeamento de dados, revisão das minutas contratuais e implementação da política de descarte de dados.

Em síntese, as fases de implementação do programa são:

Conscientização: a LGPD significa, sobretudo, uma mudança de cultura. Assim, é fundamental orientar todos os funcionários da empresa, que devem aprender o que muda com a LGPD.

Mapeamento de dados: nesta fase, é realizada a análise do fluxo de dados pessoais, desde a coleta, passando por todas as fases de tratamento, terminando com o descarte das informações.

Adequação do site: Muitas vezes, o site da empresa representa o primeiro contato entre ela e o cliente. É importante que o site contenha uma política de privacidade, em um lugar acessível e destacado, assim como um aviso de *cookies*[4] e um formulário de cadastro atualizado nos termos da LGPD.

[4] Cookies são arquivos enviados pelo servidor do site para o computador dos usuários, com a finalidade de identificá-lo e obter os dados de acesso, como páginas navegadas ou links clicados, permitindo, desta forma, personalizar a navegação de acordo com o perfil dos usuários.

Manter uma política de descarte dos dados: A LGPD impõe como padrão que os dados sejam apagados depois de utilizados. A eliminação dos dados ocorre quando não é mais possível justificar a sua manutenção. Fique atento: apagar é diferente de manter no backup, pois o backup também precisa de uma base legal para ser justificado. Assim, é recomendável estruturar os prazos internos que determinam quando os dados podem ser eliminados.

Ter um plano para incidentes de segurança: Incidentes de segurança acontecem cotidianamente. De fato, segundo o Estudo de Segurança Global do Instituto Ponemon[5], em 2019, 63% das pequenas e médias empresas sofreram algum incidente com vazamento de dados. Esse número apenas reforça a importância de investimentos em uma política interna para enfrentamento de incidentes de segurança. Assim, é preciso elaborar um Plano de Respostas a Incidentes, sempre pensando no que se encaixa ou não na sua empresa.

No dia a dia da empresa, o impacto da LGPD será significativo, pois inicialmente a lei demanda uma revisão de todos os procedimentos em que os dados pessoais são necessários, em todos os departamentos da empresa (como o marketing, jurídico, análise de dados, atendimento ao cliente).

[5] https://www.keepersecurity.com/pt_BR/ponemon2019.html

Sócio responsável
Mauricio Suriano

Colaboradores
Eduardo Benini
Gabriel Khayat
Isabella M. Pawlak

Quer saber mais?
Entre em contato

SSBM

SCAVAZZINI SURIANO BENINI MINELLI ADVOGADOS

ssbm.com.br

Av. Presidente Vargas, 2121, sala 2401
Ribeirão Preto, SP