

GUIA:

LEI GERAL DE PROTEÇÃO DE DADOS E O VAREJO



SUMÁRIO

APRESENTAÇÃO.....	3
ENTENDA A LEI GERAL DE PROTEÇÃO DE DADOS	4
Alguns conceitos básicos contidos na Lei.....	4
O histórico da Lei.....	4
Como ocorrerá a fiscalização da LGPD?.....	5
Princípios da LGPD.....	5
Quem está sujeito à Lei?.....	5
Entenda se a sua empresa é: controladora, operadora ou encarregada de dados.....	5
Bases legais da Lei Geral de Proteção de Dados.....	6
 NA PRÁTICA: A LGPD E O VAREJO.....	 7
Primeiros passos.....	7
Checklist de atenção.....	9
 DÚVIDAS FREQUENTES.....	 11
 BENEFÍCIOS PARA O EMPREENDEDOR QUE ESTÁ EM CONFORMIDADE COM A LGPD.....	 12
Conhecimento maior sobre seus clientes.....	12
Construção maior sobre seus clientes.....	12
Construção de uma experiência positiva.....	12
POR UMA REDE FORTE E UNIDA.....	13
Referências.....	13

Apresentação



Você já ouviu falar na [Lei Geral de Proteção de Dados?](#) Ela foi sancionada em agosto de 2018 e tem como objetivo determinar regras para o **tratamento dos dados pessoais** e estabelecer penalidades para o caso de descumprimento das regras, para **proteger os direitos fundamentais de liberdade e de privacidade de todos os indivíduos**.

A LGPD (como ficou conhecida a Lei Geral de Proteção de Dados) **é aplicável a toda e qualquer pessoa ou empresa** (independentemente do porte) **que realize o tratamento de dados pessoais**, tais como: nome, CPF, endereço, e-mail, data de nascimento, profissão, raça ou qualquer outro dado pessoal de clientes, parceiros, fornecedores, colaboradores etc.

Neste ebook, a Fapesp e as Associações Comerciais disponibilizam um resumo do que é a lei e explicam quais serão os impactos que ela trará ao setor do varejo, para que você compreenda como ela irá afetar o dia a dia da sua empresa e quais medidas serão necessárias para se adequar à nova legislação.

Boa leitura!

ENTENDA A LEI GERAL DE PROTEÇÃO DE DADOS

Para entendermos de forma bem objetiva o que é, de fato, a Lei Geral de Proteção de Dados (LGPD), vamos começar pensando nas seguintes questões:

- Você abriria as portas da sua casa para uma pessoa estranha e permitiria que ela explorasse seus armários e gavetas?
- Que ela tivesse acesso direto aos seus dados pessoais?
- Que conhecesse todos os seus horários? Ou até mesmo ouvisse suas conversas íntimas?
- E depois de tudo isso ainda compartilhasse as informações com outras pessoas?

Provavelmente sua resposta é NÃO. E esta é uma resposta sensata, porque todas essas informações configuram parte dos seus dados pessoais - de quem você é - e, por isso, o acesso a elas deve ser resguardado apenas a relações seguras, confiáveis ou que interessem a você.

ESTA É A PROPOSTA DA LGPD: ASSEGURAR UM CONJUNTO DE DIREITOS BÁSICOS PARA PRESERVAR OS DADOS PESSOAIS DAS PESSOAS.

ALGUNS CONCEITOS BÁSICOS CONTIDOS NA LEI

- **Dado pessoal** - qualquer informação relacionada à pessoa natural identificada ou identificável (dados não anonimizados).
- **Dado pessoal sensível** - dado pessoal sobre raça/etnia, religião, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político referente à saúde ou à vida sexual, dado genético ou biométrico.
- **Titular** - pessoa natural a quem se refere os dados pessoais que são objeto de tratamento.
- **Tratamento** - toda operação realizada com dados pessoais, tal como coleta, recepção, classificação, utilização, acesso, reprodução, transmissão, arquivamento, armazenamento, eliminação etc.

 [Entenda a LGPD em 2 minutos.](#)

O HISTÓRICO DA LEI

[Lei nº 13.709](#): sancionada como Medida Provisória (MP) em 14/08/2018, pelo Presidente em exercício: Michel Temer.

Antes da aprovação pelo Congresso Nacional, a MP sofreu várias alterações, nos termos do Projeto de Lei de Conversão nº 7 de 2019, até que, em julho de 2019, foi sancionada pelo presidente Jair Bolsonaro como [Lei nº 13.853](#).

COMO OCORRERÁ A FISCALIZAÇÃO DA LGPD?

A Autoridade Nacional de Proteção de Dados (ANPD), vinculada à Presidência da República, será o órgão governamental responsável por articular as estratégias de fiscalização e punições a respeito da LGPD*.

As punições poderão ser aplicadas a partir de 01/08/2021 e levarão em conta não só a gravidade da infração e do dano, mas também as medidas de segurança adotadas pela pessoa/empresa responsável pelo tratamento dos dados pessoais, dentre outros. As multas poderão chegar a **R\$ 50.000.000,00** (cinquenta milhões de reais) por infração!

PRINCÍPIOS DA LGPD

O tratamento de dados pessoais deve obedecer alguns princípios do art. 6 da lei (veja todos [aqui](#)), dos quais destacamos:

FINALIDADE

Deve-se informar aos titulares dos dados especificamente para que suas informações serão utilizadas. Portanto, não se pode “aproveitar” os dados já obtidos para utilizá-los com outra finalidade!

NECESSIDADE

Somente dados necessários para atingir a finalidade devem ser coletados e tratados.

LIVRE ACESSO

Deve-se garantir aos titulares consulta facilitada e gratuita sobre seus dados, sobre forma e duração do tratamento, além da correção de erros ou inexatidões, bem como a exclusão dos dados, se assim for a vontade expressa do titular.

SEGURANÇA

Deve-se garantir aos titulares segurança e proteção de seus dados (físicos ou virtuais) de acessos não autorizados.

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

Deve-se adotar medidas eficazes que comprovem a observância e o cumprimento da LGPD.

QUEM ESTÁ SUJEITO À LEI?

Estão sujeitas à lei **todas as pessoas e empresas de todos os setores e portes que realizem tratamento de dados pessoais**, sejam de seus clientes, fornecedores, colaboradores internos etc.

ENTENDA SE A SUA EMPRESA É: CONTROLADORA, OPERADORA OU ENCARREGADA DE DADOS

- **CONTROLADOR DE DADOS:** pessoa natural ou jurídica que toma as decisões em relação ao tratamento dos dados pessoais.
- **OPERADOR DE DADOS:** pessoa natural ou jurídica que realiza o tratamento dos dados em nome do controlador.
- **ENCARREGADO DE DADOS:** pessoa indicada pelo controlador e operador para fazer a ponte com a ANPD (esta função poderá ou não ser exigida de acordo com o porte da empresa e o volume dos dados trabalhados por ela).
- **AGENTES DE TRATAMENTO:** o controlador e o operador.

**Este guia foi produzido e publicado em novembro de 2020, em conformidade com as informações e definições sobre a LGPD e ANPD em vigor.*

BASES LEGAIS DA LEI GERAL DE PROTEÇÃO DE DADOS

São **10 bases legais** previstas pela LGPD que autorizam o tratamento adequado de dados pessoais e que funcionam independentes umas das outras. Ou seja, cabe à cada empresa entender juridicamente e determinar qual é ou quais são as bases legais mais apropriadas para a sua atuação em relação ao tratamento de dados. Assim, os dados pessoais podem ser tratados nas seguintes hipóteses:

CONTRATOS

Para a execução de procedimentos e obrigações dos contratos.



ESTUDOS POR ÓRGÃOS DE PESQUISA

Para a realização de estudos por órgãos oficialmente credenciados como de pesquisa, garantindo-se, sempre que possível, a anonimização dos dados pessoais.

EXECUÇÃO DE POLÍTICAS PÚBLICAS

Pela administração pública, para a execução de políticas públicas previstas em leis ou respaldadas em contratos.

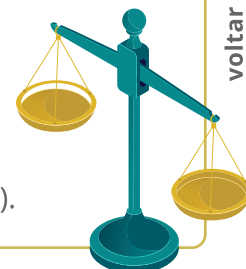


LEGÍTIMO INTERESSE

Para atender os interesses legítimos do controlador ou de terceiro, exceto quando prevalecerem direitos e liberdades fundamentais do titular dos dados.

OBRIGAÇÃO LEGAL

Para o cumprimento de obrigação legal ou regulatória pelo controlador (ou seja, por exigência de outras leis à pessoa/empresa controladora).



PROCESSOS JUDICIAIS

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

PROTEÇÃO DA VIDA

Quando o interesse for vital, ou seja, para a proteção da vida ou da segurança física do titular ou de outra pessoa.

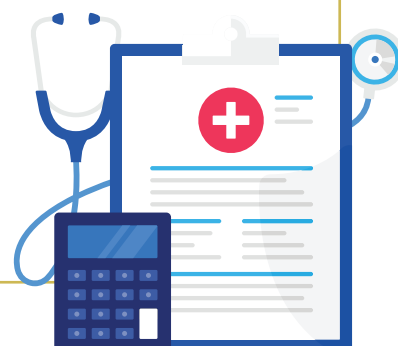


PROTEÇÃO DE CRÉDITO

Para a análise de crédito e dos riscos da transação, é possível que dados pessoais sejam consultados, avaliando o perfil do pagador.

TUTELA DA SAÚDE

Quando profissionais de saúde, serviços de saúde ou autoridade sanitária precisam tratar dados pessoais para identificar riscos à saúde.



Se não houver ocorrência de uma das 9 bases legais acima, deve haver **CONSENTIMENTO INEQUÍVOCO DO TITULAR**:

CONSENTIMENTO DO TITULAR

Consentimento é definido como uma **declaração clara e inequívoca** (que não deixa dúvidas) de que uma pessoa concorda com o uso dos seus dados pessoais para as **finalidades – também claras e inequívocas** - propostas pela empresa.



NA PRÁTICA: A LGPD E O VAREJO

PRIMEIROS PASSOS

A seguir, algumas dicas quanto aos primeiros passos a serem checados para sua empresa entrar em conformidade com a LGPD:

- **Identificar as etapas de tratamento** dos dados pessoais na sua empresa (de clientes, funcionários etc.), lembrando que “tratamento” na LGPD é TODA OPERAÇÃO REALIZADA COM DADOS PESSOAIS (por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração). Exemplo:

1. Coleta

2. Arquivamento/
Armazenamento

3. Processamento

4. Compartilhamento
(transmissão, distribuição, etc.)

5. Eliminação

• **Identificar os meios utilizados para o tratamento dos dados**, os quais podem corresponder a pessoas, bancos de dados, sistemas, locais físicos, equipamentos, documentos etc.



PESSOAS



BANCO DE DADOS



SISTEMAS



LOCAIS FÍSICOS



EQUIPAMENTOS



DOCUMENTOS

• **Mapear cada etapa**, respondendo ao máximo de perguntas possíveis (“quem”, “como”, “quando”, “onde”, “por quê”, “para quê” etc.), bem como fazendo a correspondência com o(s) meio(s) de tratamento correspondente(s).

Exemplos:

a) Etapa da Coleta: **quais** os dados coletados (dados pessoais, dados sensíveis, dados sobre crianças e adolescentes)?; **como** os dados são coletados (durante uma compra, preenchimento de cadastro físico ou digital pelo titular, via website da sua empresa)?; **quem** coletou os dados (foram realmente colhidos por sua empresa)?; **quem** é o responsável pela coleta na sua empresa (ex. equipe de vendas)?; **quando** os dados foram coletados (estão atuais?, quando da coleta, houve consentimento por parte do titular)?;

b) Etapa de Arquivamento: **onde** os dados estão armazenados (nuvem, arquivo físico, banco de dados, equipamento(s), sistemas etc.);? **quem** é responsável pelo arquivamento (essa pessoa está devidamente treinada para garantir a segurança dos dados)?; **quão** seguros são os arquivos?

• **Analisar o mapeamento realizado**, identificando possíveis falhas ou correções,

sejam em relação à **atualização, segurança (técnica ou administrativa) dos dados, obtenção de consentimento**, informação quanto à **finalidade da coleta**, relacionados à **conscientização e capacitação da sua equipe** no tratamento dos dados e relacionamento com seus titulares. Aqui entra todo o tipo de falha, inclusive falhas consideradas simples como esquecer documentos com dados pessoais numa impressora, deixá-los em cima da mesa à vista de todos, armazenar documentos em local pouco seguro etc.

• **Efetuar as correções necessárias.**

NO VAREJO, A LGPD REPRESENTA UMA GRANDE TRANSFORMAÇÃO - para melhor!



Lembre-se de que uma das melhores formas de marketing é a forma como você trata seus clientes. Portanto, tratar dados pessoais com zelo e respeito é necessário, independentemente do porte da sua empresa.

CHECKLIST DE ATENÇÃO

Perguntar é necessário. Dentre as 10 bases legais para aplicação da LGPD, a regra do consentimento recai fortemente sobre o varejo. Portanto, antes de qualquer ação a partir dos dados, tenha certeza do **consentimento do titular** e de que sua empresa tem **mecanismos para comprová-lo**. É necessário também manter seu banco de dados atualizado, **validando a permanência dos dados já existentes**, sempre levando em conta os [princípios da LGPD](#).

Por exemplo, no caso de um cliente, é necessário comunicar diretamente e de forma muito clara como e quando os dados da pessoa poderão ser utilizados, para que ela possa confirmar ou não seu consentimento para permanecer no seu banco. **Dados não consentidos devem ser descartados**, até o descarte deve ser documentado.

Dica: consentimento e validação podem ser feitas conjuntamente e cabe à sua empresa decidir qual a melhor forma de fazê-lo (formulário online com assinatura digital?, concordância com termo de uso/política de privacidade de um website?). Existem também empresas que oferecem plataformas para enviar e assinar documentos eletronicamente em questão de minutos. Consulte seu profissional de T.I.

Outra dica: não existe modelo fixo de escrita, mas é importante dizer que todos os dados informados serão mantidos em sigilo e utilizados apenas para a(s) finalidade(s) em que o titular dos dados (a partir de declaração clara e inequívoca - ou seja, que sua empresa possa provar) dá seu consentimento pelo tempo determinado. As finalidades podem ser separadas, dando a oportunidade do titular marcar quais ele autoriza e quais não.

Compartilhamento de dados. Para consulta a respeito do crédito da pessoa, não é mais autorizado que dados pessoais dos titulares sejam compartilhados entre empresas. Por exemplo, se o consumidor faz compras em determinado estabelecimento e fornece seus dados, as informações coletadas serão restritas a esta relação. Só será possível compartilhar dados sobre o titular nos casos em que ele mesmo dê seu consentimento explícito para isto.

Vender/comprar bases de dados para/ de outras instituições: NEM PENSAR!



• Adote práticas preventivas para segurança

Para ficar em conformidade com a lei, elaborar e adotar novas práticas para os processos que envolvem dados é fundamental. Atente-se para:

a) Adoção e atualização de plataformas de defesa para garantir máxima proteção aos dados coletados e evitar que aconteçam vazamentos. Afinal, existem softwares que são especificamente articulados para gestar e proteger a segurança dos dados que a sua empresa coleta. O ideal é consultar um especialista em proteção de dados.

b) Adesão à criptografia de dados para manter a privacidade resguardada. Por exemplo: no caso de transmissão de dados pessoais online (upload ou download), a entidade precisará fazer uma hospedagem em site https, com certificado ssl. É preciso bloquear o acesso http (site não criptografado).

c) Atualização periódica dos sistemas de software e seguranças adotados por sua empresa, para não cair na obsolescência e deixar as informações vulneráveis a vazamentos.

d) Segurança em arquivos físicos (backup de informações, acesso restrito etc.) – recomendamos passá-los ao formato digital tão logo possível.

Evite possíveis erros. Agilize seus processos o quanto antes para se prevenir.

• Administre os riscos e estabeleça processos para gerir falhas

Construa saídas para possíveis erros e marque também alinhamentos periódicos com os envolvidos no processo, para combinar soluções e procedimentos padronizados. Esta ação é necessária uma vez que todas as pessoas responsáveis por gestar uma base de dados precisarão:

- a) Redigir normas de governança
- b) Replicar boas práticas e adotar certificações necessárias
- c) Elaborar planos de contingência
- d) Realizar auditorias
- e) Resolver incidentes com agilidade

Um exemplo é o risco de sofrer um vazamento de dados. Nesse caso, a ANDP e as pessoas afetadas precisam ser imediatamente informadas. **Todos os agentes de tratamento estão sujeitos à fiscalização e aplicação da lei.**

As falhas de segurança podem resultar em multas de até 2% do faturamento anual da empresa (em um limite de 50 milhões a cada infração). Os níveis de penalidade serão fixados de acordo com a gravidade da falha.

• A transparência é fundamental

Se o titular pediu alguma informação, procure respondê-lo com a máxima rapidez. Além disso, mantenha-o informado durante todo processo, **inclusive se algo der errado.**

Você precisará lidar com as informações pessoais dos seus clientes o mais diretamente possível. Para isso, é necessário:

- a) Deixar claro os reais motivos que fundamentaram a coleta de dados
- b) Explicar como será o armazenamento e tratamento da empresa para com eles
- c) Pontuar meios de contato para que o titular dos dados se comunique com a sua empresa

Além disso, nas situações em que as informações serão compartilhadas em algum sistema, é imprescindível que a empresa deixe isto claro ao usuário. E a partir do momento em que houver clareza e um acordo entre os dois lados, **é importante que a autorização prévia do consumidor para o uso dos seus dados seja registrada.**

• A Lei também se associa a dados fora do ambiente nacional

A LGPD se aplica a empresas que oferecem produtos ao Brasil ou estão no mercado nacional. Então, não importa se a pessoa está em território nacional ou não, se houve o consentimento e os dados delas estão vinculados a alguma empresa eles já entram na lei.



DÚVIDAS FREQUENTES

A LGPD significa que o empreendedor perderá os dados armazenados?

Não!

O que a LGPD determina é a necessidade de informar os consumidores que os dados deles estão armazenados e validar a possibilidade de mantê-los no sistema.

É permitido ou não ter a base de dados dos clientes?

É permitido sim. Mas, novamente, reforçamos que a base de dados deve ser sustentada por endereços eletrônicos e informações de pessoas que consentiram com isso.

Estamos fazendo campanha para atualização dos dados dos nossos clientes, obtenção de consentimento etc., mas alguns não respondem. O que fazer?

Nesse caso, é importante comprovar numa “linha do tempo”, tudo o que foi feito na sua campanha. Exemplo: envio de emails, de “x em x” tempo lembrando da importância do cadastramento, envio de correspondências etc. De qualquer forma, cabe à sua empresa estabelecer um prazo após o qual os dados sem consentimento serão descartados.

E no caso dos colaboradores da sua empresa?

Esta relação está muito conectada à questão do contrato de trabalho entre o empregado-titular e o empregador-controlador. É um processo que traz o compartilhamento de informações pessoais desde o início, por meio dos dados básicos sobre o candidato, seu currículo e histórico, por exemplo. E conforme

a celebração do contrato vai avançando, o fluxo de compartilhamento de dados também vai contemplando pontos como filiação a sindicato, nomes de familiares, escolaridade, situação familiar, chegando até aos acordos empregatícios, como salário, descontos, faltas, motivos de faltas, doenças, acidentes.

Neste caso, é entendido que no contrato de trabalho já existe uma cláusula registrando a coleta de dados dos colaboradores, assim como os fins para os quais eles podem ser utilizados. Porém, é válido rever estas informações e ajustar de forma clara e direta os contratos para garantir que a conformidade deles com a LGPD esteja valendo também para assegurar o sigilo dos dados do funcionário, assim como a integridade da empresa em relação às suas obrigações legais.

Este ponto de atenção é fundamental, uma vez que - segundo o site do Governo Federal - eventualmente:



*“Há, ainda, uma não menos intensa troca de informações entre o empregador-controlador e outros controladores e os órgãos públicos. Toda vez que o empregador repassa qualquer informação de um empregado que possibilite a identificação desse empregado para um terceiro, seja quem for esse terceiro, haverá uma transmissão de dados pessoais nos termos da lei. **Isso envolve, por exemplo, convênios médicos, planos de saúde, vales-refeição, vales-alimentação, e-Social, consultorias contratadas**”.*

Fonte: <https://www.serpro.gov.br>

Para estar em conformidade com a LGPD: precisa ter um departamento jurídico ou especialista no assunto?

Esses profissionais e recursos auxiliam no dia a dia da sua empresa, mas, especificamente para entrar em conformidade com a LGPD, todo empresário pode articular suas estratégias para se adaptar às novas determinações legais.

O departamento jurídico e especialista podem contribuir para tirar dúvidas legais e para ajustar modelos de contratos.



BENEFÍCIOS PARA O EMPREENDEDOR QUE ESTÁ EM CONFORMIDADE COM A LGPD

CONHECIMENTO MAIOR SOBRE SEUS CLIENTES

Conhecer e estar em sintonia com seus públicos é fundamental para o sucesso de qualquer empreendimento. Por isso, estar em legalidade com a LGPD representa recolher de forma responsável os dados dos seus consumidores para explorá-los (de forma consentida) para criar estratégias assertivas que serão benéficas tanto para a sua empresa quanto para o seu cliente.

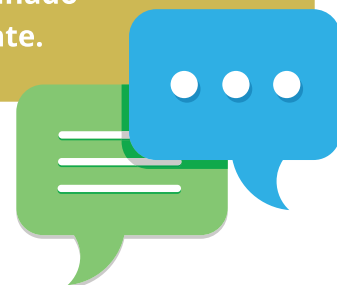
CONSTRUÇÃO DE UMA EXPERIÊNCIA POSITIVA

Construir uma relação sólida com seus consumidores a partir do compartilhamento e armazenamento de dados pode refletir em experiências positivas entre vocês, com a garantia de que ambas as partes estão em comum acordo e com entendimento transparente a respeito do processo todo.

AGILIDADE NA JORNADA DE COMPRA

Para otimizar a rotina de compra dos clientes, é comum que empresas varejistas armazenem dados como nome, número do cartão de crédito, documentos básicos e endereço, com a finalidade de que seus clientes recorrentes não enfrentem todo o procedimento de preencher esses dados a cada compra.

A LGPD não barra esta prática. Porém, ela determina que este processo seja previamente combinado e explicado ao cliente.



POR UMA REDE FORTE E UNIDA!

A LGPD é para todos e representa um importante marco para o indivíduo: a certeza de que seus dados pessoais são tratados de forma adequada e somente para a finalidade para a qual foram entregues aos terceiros que decidiram por confiá-los.

Este ebook é um material produzido pela Fapesp e pelas Associações Comerciais do Estado de São Paulo com o objetivo de auxiliar as entidades e seus associados a entenderem e poderem se adaptar à LGPD. Trata-se de uma visão geral do tema com os principais pontos da nossa área de atuação. Este ebook pode ser distribuído livremente para os associados e demais empresas parceiras.

REFERÊNCIAS

- [1. Lei Geral de Proteção de Dados](#)
- [2. Lei Geral de Dados: devo me preocupar?](#)
- [3. O que são dados pessoais e por que protegê-los](#)
- [4. Bases legais da LGPD](#)
- [5. Governo Federal](#)



