

Guia do Núcleo de Proteção de Dados do
Conselho Nacional de Defesa do Consumidor

Como proteger seus dados pessoais



Jair Messias Bolsonaro
Presidente da República

Anderson Torres
Ministro da Justiça e Segurança Pública

Waldemar Gonçalves Ortunho Junior
Diretor-Presidente da Autoridade Nacional de Proteção de Dados

Arthur Pereira Sabbat
Joacil Basilio Rael
Miriam Wimmer
Nairane Farias Rabelo Leitão
Diretores da Autoridade Nacional de Proteção de Dados

Juliana Oliveira Domingues
Secretária Nacional do Consumidor

Lilian Claessen de Miranda Brandão
Diretora do Departamento de Proteção e Defesa do Consumidor

Equipe de elaboração da Secretaria Nacional do Consumidor

Daniele Correa Cardoso
Coordenadora-Geral do Sindec

Maria Cristina Rayol dos Santos Sobreira Lopes
Coordenadora-Geral de Articulação e Relações Institucionais

Andiara Maria Braga Maranhão
Coordenação da Escola Nacional de Defesa do Consumidor

Equipe de elaboração da Autoridade Nacional de Proteção de Dados

Alexandra Krastins
Jeferson Barbosa
Gerentes de Projeto

Isabela Maiolino
Coordenadora-Geral de Normatização

Lucas dos Anjos
Servidor da Coordenação-Geral de Tecnologia e Pesquisa

Rodrigo Santana dos Santos
Coordenador de Normatização

Equipe do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor

Laura Schertel Mendes
Relatora do Núcleo de Proteção de Dados

Danilo Doneda
Integrante do Núcleo de Proteção de Dados

Marcela Mattiuzzo
Integrante do Núcleo de Proteção de Dados

Flávia Lira
Representante da Autarquia de Proteção e Defesa do Consumidor do Estado do Rio de Janeiro

Equipe de produção da Universidade de Brasília

Prof. Dr. Ugi Silva Dias
Coordenação

Janaina Angelina Teixeira
Coordenação pedagógica

Angélica Magalhães Neves
Revisão

Israel Silvino Batista Neto
Projeto gráfico e diagramação



1. OS SEUS DADOS PESSOAIS IMPORTAM!

Os dados pessoais são a sua representação na sociedade, por isso, são parte da sua personalidade. Eles devem ser usados de forma leal e segura, conforme as legítimas expectativas. A Lei Geral de Proteção de Dados Pessoais (LGPD) tem a função de garantir que os dados sejam processados de forma lícita, adequada e segura.



Quando seus dados pessoais podem ser tratados:

- ✓ Ao contratar um empréstimo no banco, dados sobre a sua capacidade de pagamento são tratados;
- ✓ Ao interagir em uma rede social, dados pessoais sobre o seu comportamento são processados;
- ✓ Ao participar de um programa de fidelidade de uma empresa, dados sobre o seu consumo podem ser coletados;
- ✓ Para um tratamento de saúde em um hospital, são processados dados pessoais, incluindo dados de cadastro e de saúde.

Vivemos em uma sociedade movida a dados. Muitas atividades do nosso cotidiano envolvem a coleta, o uso e o compartilhamento de dados com empresas ou órgãos governamentais. Na internet, também compartilhamos dados, seja ao fazer compras, seja ao usar redes sociais.

LGPD



2. O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS?

A Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018), conhecida também como LGPD, criou normas para a proteção dos dados pessoais de todos os brasileiros, com o objetivo de garantir os direitos de liberdade, de privacidade e o livre desenvolvimento da personalidade. A LGPD concretiza direitos previstos na Constituição Federal de 1988 e complementa a proteção conferida pelo [Código de Defesa do Consumidor](#) e pelo [Marco Civil da Internet](#).

A proteção de dados é importante tanto para o cidadão, como para a economia e para a sociedade como um todo. Ela dá poder ao cidadão para controlar os seus dados e fortalece o exercício da liberdade de expressão, do acesso à informação e dos direitos à intimidade, à honra e à imagem. A lei está atenta também ao desenvolvimento econômico do País, ao incentivar a criação de novas tecnologias em setores estratégicos pelas empresas de pequeno porte, como as microempresas e *startups*, que possuem regime diferenciado pela lei.

2.1 Quem é a Autoridade?

A LGPD criou obrigações e padrões para quem trata dados pessoais e instituiu a Autoridade Nacional de Proteção de Dados (ANPD) para regular a coleta, o uso, o processamento e compartilhamento de dados no País. O cidadão pode enviar reclamações e denúncias sobre tratamentos indevidos de dados diretamente à ANPD. Para ter mais informações sobre as competências e atuação da ANPD, o cidadão pode consultar o site (www.gov.br/anpd).



2.2 Papel da LGPD para a segurança jurídica

A LGPD também gera mais segurança jurídica tanto para consumidores, quanto para empresas, ao definir de forma mais clara as situações em que se pode legalmente coletar, processar, armazenar e transferir dados pessoais, atividades comuns em uma economia cada vez mais digitalizada.



Quais são os riscos para o consumidor quando há um tratamento ilícito de dados?

- ✓ Monitoramento de seu comportamento e restrição a liberdades fundamentais;
- ✓ Discriminação;
- ✓ Prejuízos econômicos;
- ✓ Restrição de acesso a bens e serviços;
- ✓ Violação da intimidade;
- ✓ Fraudes que afetam a sua identidade;





3. CONCEITOS IMPORTANTES

O que é um dado pessoal?

A LGPD define como dado pessoal qualquer “informação relacionada a pessoa natural identificada ou identificável”. Na prática, isso quer dizer que são informações que podem ser associadas a uma pessoa, seja para identificá-la diretamente, seja para associar esses dados a um contexto que permita a sua identificação.

Como os dados pessoais circulam intensamente identificação e definição do perfil de uma pessoa, a partir de informações menos diretas, como um endereço de e-mail, um número de telefone celular, uma localização ou uma postagem na internet. Todos esses dados podem ser considerados dados pessoais.





Podem ser considerados DADOS pessoais, ENTRE OUTROS:

- ✓ Nome e sobrenome;
- ✓ Endereço residencial;
- ✓ Endereço de e-mail (se ele tiver elementos que ajudem a identificar o dono, como nome e sobrenome);
- ✓ Gênero;
- ✓ Data de nascimento;
- ✓ Número de documentos cadastrais, como RG, CPF e Carteira de Trabalho;
- ✓ Dados de geolocalização de um telefone celular;
- ✓ Número de telefone pessoal;

Quem é titular de dados?

De acordo com a LGPD, o titular de dados pessoais é toda pessoa natural a quem se referem os dados tratados. Portanto, qualquer pessoa é titular de dados pessoais em algum contexto.

Quem são os agentes de tratamento?

Por sua vez, as pessoas naturais ou jurídicas, públicas ou privadas, que tratam dados pessoais, para quaisquer finalidades previstas na LGPD, são consideradas agentes de tratamento. No caso, a LGPD elenca como agentes de tratamento o controlador e o operador de dados.

Os **agentes de tratamento** são aqueles que realizam a coleta, o uso, o compartilhamento ou outra atividade com os dados pessoais. A lei prevê dois agentes de tratamento com funções e responsabilidades distintas: o **controlador** e o **operador**.

O **controlador** é o agente de tratamento responsável por tomar as principais decisões referentes ao tratamento de dados pessoais, bem como por definir a sua finalidade e os elementos essenciais desse tratamento.

Ele é o responsável pelo atendimento aos direitos criados pela LGPD aos titulares de dados. Caso o controlador não conceda esses direitos, o titular poderá fazer uma reclamação perante a ANPD. Por exemplo, ao ser solicitado, o controlador é obrigado, por lei, a informar quais dados possui sobre o titular de dados. A recusa em apresentar

essa informação consiste em descumprimento à LGPD e o controlador poderá ser fiscalizado e punido.

Já o **operador** é o agente de tratamento que atua em nome do controlador, devendo tratar os dados somente de acordo as suas instruções e em conformidade com a lei.

Quem é o encarregado de dados?

A LGPD estabelece que os agentes de tratamento - como empresas e órgãos públicos - indiquem um **encarregado de dados**. Ele é uma figura criada para facilitar a comunicação entre os agentes de tratamento com os titulares de dados e a ANPD. Assim, o titular poderá requerer os direitos sobre os seus dados pessoais perante o encarregado, salvo na eventualidade da ANPD afastar essa obrigação, o que pode acontecer em determinados setores e situações específicas.

3.1 Tratamento de Dados Pessoais

3.1.1 Definições

A LGPD define o tratamento de dados como toda operação realizada com dados pessoais, por exemplo: produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.



Guia orientativo sobre agentes de tratamento:

https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf

3.1.2 Hipóteses de Tratamento

A LGPD limita as situações em que é possível o tratamento de dados pessoais. Para isso, a lei elenca as bases legais que podem ser usadas em cada caso. São dez as hipóteses para o tratamento de dados pessoais:



- ✓ com o consentimento do titular dos dados pessoais;
- ✓ se o controlador precisa tratar esses dados para cumprir com uma obrigação legal ou regulatória;
- ✓ quando a administração pública executa políticas públicas ou no desempenho de suas funções institucionais;
- ✓ para a realização de estudos por órgão de pesquisa;
- ✓ para a execução de um contrato do qual seja parte o titular, a pedido do titular dos dados;
- ✓ para o exercício de direitos em um processo judicial, administrativo ou arbitral;
- ✓ para a proteção da vida e da segurança física do titular;
- ✓ para a proteção da saúde em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- ✓ quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; e
- ✓ para a proteção do crédito;



No caso do tratamento de dados pessoais definidos como sensíveis, existem outras bases legais que devem ser observadas.

4. QUAIS SÃO OS PRINCÍPIOS QUE ORIENTAM O TRATAMENTO DE DADOS NO BRASIL

É importante identificar em qual base legal o tratamento de dados se apoia no caso concreto. Assim, pode-se verificar se as atividades estão de acordo com a LGPD. O tratamento de dados pessoais deve respeitar os princípios da LGPD. São eles:



- ✓ **finalidade:** o tratamento de dados pessoais deve ter um objetivo específico, claro e ser informado ao titular. O tratamento não pode acontecer com fins genéricos;
- ✓ **necessidade:** devem ser tratados apenas os dados pessoais estritamente necessários para atingir o objetivo inicialmente definido;
- ✓ **adequação:** o tratamento de dados pessoais deve ser coerente com a finalidade que o motivou;
- ✓ **transparência:** o titular deve ser informado de forma clara e adequada sobre os aspectos e as características relevantes do tratamento de seus dados;
- ✓ **livre acesso:** o titular deve ter garantido o acesso aos seus dados pessoais, a qualquer tempo e de forma gratuita e facilitada;
- ✓ **qualidade dos dados:** os dados pessoais tratados devem estar corretos, precisos e atualizados;
- ✓ **segurança:** os dados pessoais devem ser tratados com as medidas físicas e lógicas necessárias à proteção, evitando acessos não autorizados;
- ✓ **prevenção:** quem trata dados pessoais deve adotar medidas que evitem o tratamento em desconformidade à LGPD;
- ✓ **não-discriminação:** nenhum tratamento pode ser realizado para fins discriminatórios, ilícitos ou abusivos;
- ✓ **responsabilização e prestação de contas:** o agente de tratamento deve garantir e demonstrar, de forma documentada, que tomou todas as medidas necessárias, eficazes e suficientes para adequar o tratamento à legislação;

EXEMPLO DE APLICAÇÃO EM UMA COMPRA:

Pergunta 1

Qual é o objetivo desse tratamento de dados? Para que ele serve?

Para que uma loja possa entregar o produto comprado pela pessoa no endereço indicado, é preciso que ela tenha essa informação.

Pergunta 2

Que dados são necessários para atingir esse objetivo?

No caso de uma entrega, são necessários o nome da pessoa, o endereço de entrega e um telefone para contato (no caso de não ser possível localizar a pessoa no endereço).

Pergunta 3

Os dados que são utilizados efetivamente servem para alcançar esse objetivo?

Se é possível fazer a entrega com base nas informações coletadas da pessoa, a resposta é afirmativa, mas se os dados não servirem àquele objetivo, o tratamento precisa ter como base alguma outra finalidade. Por exemplo, o CPF da pessoa pode ser necessário para emitir a nota fiscal, mas não para fazer a entrega.

Pergunta 4

A pessoa consegue saber que esse tratamento está sendo realizado e por quem ele é realizado?

Se a pessoa entrar em contato com a loja, ela precisa ser informada de que o tratamento está acontecendo para o objetivo de entrega do produto, e também saber quais dados estão sendo usados para essa finalidade. É também importante que a pessoa saiba que é aquela loja em específico que está tratando os dados, inclusive, se for o caso, que a loja tem contrato com outras empresas para fazer a entrega do produto (como uma transportadora).

Pergunta 5

Os dados são atualizados e precisos?

Se isso não for verdade, sequer será possível fazer a entrega. A loja deve se preocupar em ter informações corretas, inclusive para atingir o objetivo daquele tratamento. É claro que as informações podem mudar ao longo do tempo, por isso é importante ter mecanismos que permitam que a pessoa atualize as suas informações (por exemplo, se ela for fazer uma nova compra, precisa confirmar que o endereço permanece o mesmo).

Pergunta 6

Os dados estão seguros e medidas de prevenção de problemas foram adotadas?

É importante que os dados estejam armazenados em sistemas seguros e que somente as pessoas autorizadas tenham acesso a eles. A loja também não deve permitir que todos os seus funcionários tenham acesso ao endereço de quem fez uma compra, mas sim aquelas pessoas que precisam dessa informação para fazer o seu trabalho – quem faz o contato com a transportadora, por exemplo.

Pergunta 7

Os dados são utilizados de forma discriminatória, isto é, de modo a tratar diferentemente situações que deveriam ser tratadas de forma semelhante?

É fundamental que o tratamento de dados não gere efeitos discriminatórios para o titular, uma vez que a lei proíbe a discriminação abusiva e ilícita.

Pergunta 8

O tratamento de dados ocorre de forma transparente e de modo que outros atores possam controlar e acompanhá-lo?

O princípio da responsabilização e prestação de contas exige a demonstração pelo agente da adoção de medidas que comprovem o cumprimento da legislação de proteção de dados.



5. QUAIS SÃO OS DIREITOS DOS TITULARES DE DADOS?

A LGPD garante aos titulares de dados o direito de acompanhar e de exercer controle sobre seus dados pessoais, de forma gratuita e facilitada. Abaixo, são apresentados os direitos específicos estabelecidos pela LGPD.

“ Em atenção ao princípio da **transparência**, a lei estabelece o direito do titular de dados à **informação**, isto é, o direito de ser informado sobre como o tratamento de dados ocorrerá. ”

Assim, devem ser fornecidas informações adequadas sobre o tratamento, tais como a finalidade, forma e duração do tratamento, identificação do controlador e eventuais compartilhamentos com terceiros.

O titular também tem direito à **confirmação** sobre a existência de um tratamento de seus dados por um controlador, e quando se confirmar o tratamento, ele terá o **livre acesso** aos seus próprios dados pessoais. Tanto a confirmação quanto o acesso aos dados pessoais pelo titular devem ser providenciados imediatamente pelo controlador, e para pedidos que envolvam a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade devem ser atendidos em até 15 dias.

O titular possui o direito à **correção** de seus dados pessoais que estejam incorretos. Esse direito de correção compreende a possibilidade de atualização dos dados e, quando necessário, até mesmo a inserção de novos dados ao tratamento.

Sempre que dados pessoais forem tratados em desconformidade com a lei ou seu tratamento não for necessário, cabe ao titular a possibilidade de pedir a sua **anonimização**, o seu **bloqueio** ou mesmo a sua **exclusão**. Ainda, cabe ao titular o direito de solicitar a sua **portabilidade** a outro controlador para o qual deseje migrar a operação de tratamento.

Para os tratamentos de dados pessoais que possuem o consentimento como base legal, cabe ao titular o direito de solicitar a sua **eliminação**, de forma incondicionada e sem necessidade de explicar a motivação.

Além disso, o titular poderá **revogar o consentimento** que forneceu ao tratamento de seus dados a qualquer momento, sem necessidade de fundamentação, e o controlador deverá facilitar esse procedimento.

O titular tem o direito de **solicitar informações** sobre as entidades com quem houve uso compartilhado de seus dados pessoais e sobre as consequências de não fornecer o seu consentimento para o tratamento de dados pessoais quando o pedem. O titular pode também solicitar informações sobre a finalidade do tratamento, a sua forma e duração, identificação e informações de contato do controlador, as informações sobre o uso compartilhado de dados pelo controlador e a finalidade, responsabilidades dos agentes que realizarão o tratamento, além de qualquer outra informação que seja relevante para o tratamento específico.

Quando dados pessoais são utilizados para que se tomem decisões automatizadas que sejam capazes de influenciar concretamente seus interesses, cabe ao titular o direito de solicitar a **revisão** dessas decisões para ter ciência dos critérios e parâmetros utilizados e contestá-los quando for o caso.

É garantido o direito de **solicitar explicação** sobre os critérios e procedimentos adotados para que se tome a decisão.

O titular **não poderá ser cobrado** pelos custos do exercício de seus direitos. Os prazos para atendimento dos seus pedidos serão estabelecidos em regulamento pela ANPD.

Por fim, a requisição de direitos pelo titular poderá ser realizada perante a ANPD e também perante os órgãos de defesa do consumidor **sempre que o tratamento de dados ocorrer no contexto de uma relação de consumo**.



Como as organizações públicas e privadas devem atuar no tratamento de dados pessoais?

- ✓ **Garantindo** que todo tratamento de dados pessoais tenha uma base legal;
- ✓ **Mantendo** registro das operações de tratamento de dados;
- ✓ **Elaborando** relatório de impacto à proteção de dados pessoais quando o tratamento puder gerar riscos às liberdades civis e aos direitos fundamentais dos titulares;
- ✓ **Concebendo** sistemas seguros e que protejam os dados desde a sua concepção;
- ✓ **Informando** ao titular dos dados e a ANPD as violações de segurança dos dados pessoais que possam causar risco ou dano relevantes, com as devidas medidas de contenção ou mitigação;
- ✓ **Informando** ao titular dos dados, caso haja alguma alteração na finalidade para a coleta de dados;
- ✓ **Reparando** danos causados em razão do tratamento de dados pessoais, em violação à legislação;
- ✓ **Confirmando** a existência ou providenciar o acesso a dados pessoais, mediante requisição do titular;
- ✓ **Divulgando** os tipos de dados coletados;
- ✓ **Descrevendo** a metodologia utilizada para a coleta e compartilhamento de dados;
- ✓ **Descrevendo** a metodologia utilizada para garantir a segurança das informações;
- ✓ **Avaliando** de forma permanente as salvaguardas e mecanismos de mitigação de riscos adotados;
- ✓ **Indicando** o Encarregado de Dados Pessoais e divulgando publicamente as suas informações de contato;
- ✓ **Aceitando** reclamações, comunicações e prestar esclarecimentos aos titulares de dados;



Como o titular de dados pode proteger os seus dados pessoais?

- ✓ **Criando** *backups* dos dados armazenados, principalmente em nuvem;
- ✓ **Ativando** a criptografia nos discos e mídias externas, como pendrives;
- ✓ **Criando** senhas fortes, que contenham a combinação de caracteres especiais, letras maiúsculas, minúsculas e números, evitando utilizar dados pessoais ou palavras comuns;
- ✓ **Habilitando** a verificação de senhas em duas etapas, sempre que disponível, principalmente em sistemas de armazenamento em nuvem e aplicativos de mensagens;
- ✓ **Instalando** somente aplicativos de fontes e lojas oficiais;
- ✓ **Atualizando** sempre o sistema operacional e os aplicativos;
- ✓ **Apagando** os dados armazenados antes de se desfazer dos equipamentos e das mídias;
- ✓ **Desconfiando** de *links* recebidos por aplicativos de mensagens;
- ✓ **Limitando** a divulgação ou fornecimento de dados pessoais na internet, inclusive para redes sociais, ou para empresas, aos casos estritamente necessários;

Referências:

<https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao-de-dados.pdf>

<https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf>



O que fazer em caso de violação aos meus direitos? Quem devo procurar?

Caso seus direitos tenham sido violados, reúna todas as evidências que possui, como e-mails, prints de aplicativos de mensagens, notícias de jornal, comunicação da organização sobre o incidente, entre outras provas. Quando for uma relação de consumo, é possível registrar uma reclamação perante o Consumidor.gov.br e/ou perante as autoridades de proteção e defesa do consumidor, como Procons, Defensorias Públicas, Ministérios Públicos, etc.



Procure a empresa para solucionar o seu problema

Com o máximo de informações em mãos, procure imediatamente a empresa responsável, informe o ocorrido, anote os dados do atendimento (número de protocolo, orientações recebidas etc.), guarde as mensagens e os e-mails encaminhados. E caso não obtenha a solução para a sua reclamação, procure a autoridade competente para denunciar a violação aos seus direitos. Com esse contato direto com a empresa, é possível que as solicitações do titular dos dados sejam rapidamente atendidas.



Entre em contato com a ANPD

Caso a sua solicitação não seja atendida pelo agente de tratamento responsável, você pode apresentar reclamação à ANPD, seguindo as informações disponíveis nos canais de atendimento <https://www.gov.br/anpd>. É possível a instauração de processo administrativo contra a organização, culminando na aplicação das sanções previstas na LGPD.

E se o desrespeito aos meus direitos acontecer em uma relação de consumo?

Acesse o Consumidor.gov.br



Consumidor.gov.br

Você pode iniciar uma comunicação diretamente com a empresa por meio da plataforma Consumidor.gov.br, de forma mais rápida e desburocratizada, sem sair de casa. A plataforma é um serviço público, integralmente gratuito, mantido pela Secretaria Nacional do Consumidor (Senacon), do Ministério da Justiça e Segurança Pública (MJSP).

A plataforma conta, atualmente, com mais de 1000 empresas participantes e tem um índice médio de solução de 78%, em um prazo de cerca de 8 dias.

Como funciona o Consumidor.gov.br?

a. Primeiro, o consumidor deve verificar se a empresa contra a qual quer reclamar está cadastrada no sistema.

b. O consumidor registra sua reclamação no site e, a partir daí, inicia-se a contagem do prazo de 10 dias para a manifestação da empresa. Durante esse prazo, a empresa tem a oportunidade de interagir com o consumidor antes da postagem de sua resposta final.

c. Após a manifestação da empresa, é garantida ao consumidor a chance de comentar a resposta recebida, classificar a demanda como Resolvida ou Não Resolvida, e ainda indicar seu nível de satisfação com o atendimento recebido.

Procons

Você também conta com os Procons, que têm atendimento presencial e eletrônico. Quando a reclamação é apresentada no Procon, a empresa é chamada para esclarecer a demanda, sendo oportunizada audiência de conciliação com o consumidor. Você não precisa estar acompanhado de advogado. Não sendo realizado o acordo, poderá ser aberto um processo administrativo pelo Procon, e a empresa poderá ficar sujeita às penalidades indicadas no Código de Defesa do Consumidor. Caso seja necessário, você pode iniciar um processo perante o Poder Judiciário.

Atenção!

Se houver indícios de fraude ou suspeita de roubo de identidade, o titular deve formalizar denúncia, por meio de boletim de ocorrência, perante a autoridade policial competente. Isso pode evitar prejuízos como clonagem de cartões de crédito e débito, invasão a contas de e-mails ou de redes sociais, ou mesmo a utilização da sua identidade para realização de empréstimos não autorizados ou outros tipos de fraude.



