

GUIA

DESCOMPLICANDO A LGPD

1. Sumário



2. Apresentação	2
3. Nosso Papel	2
4. Histórico	3
5. O que é a Lei Geral de proteção de dados - LGPD?	4
6. E o que são dados pessoais?	4
7. O que é tratamento de dados pessoais?	5
8. O que é um dado pessoal sensível?	5
9. Por que as empresas devem fazer o controle de dados pessoais?	6
10. Quais são os fundamentos da LGPD?	6
11. Quais são os princípios da LGPD?	7
12. Para quais dados não se aplica LGPD?	8
13. Quem são os agentes de tratamento?	8
13.1 Quem é o Controlador?	8
13.2 Quem é o Operador?	8
13.3 Quem é o encarregado de Dados ou DPO (Data Protection Officer)?	9
13.4 O que é o relatório de impacto a proteção de dados pessoais?	9
13.5 Quem são os titulares de dados?	9
13.6 Quais são os direitos dos titulares de dados?	10
14. O que é o consentimento do titular?	10
15. Quando os dados poderão ser tratados sem consentimento?	11
16. Como solicitar o consentimento do titular?	12
17. Como tratar dados sensíveis?	12
18. O que é anonimização de dados?	13
19. Quem fiscaliza e regulamenta o tratamento de dados pessoais no Brasil?	13
20. Quais são as sanções para o descumprimento da LGPD?	14
21. Quando a LGPD entrou em vigor?	15
22. Conclusão	15
23. Perguntas Frequentes	15
24. Histórico de Alterações	18



2. Apresentação

Durante a evolução social e tecnológica da humanidade, a discussão sobre a proteção de dados, proteção cibernética e segurança da informação, nunca foi tão presente.

Nas últimas décadas, as discussões quanto à privacidade e a proteção de dados se intensificaram, o que estimulou os debates sobre a necessidade da regulamentação no tratamento de dados pessoais.

Com o tempo, diversas legislações surgiram ao redor do mundo, e, no Brasil, tivemos a promulgação da Lei Geral de Proteção de Dados, a LGPD, em 2018, responsável por estabelecer regras, dentro outras disposições, sobre o tratamento de dados no país.

Na sequência, a Emenda Constitucional nº 115 a privacidade passou a fazer parte dos direitos fundamentais do cidadão, uma vez que é um direito inerente a dignidade humana. Ainda, pelo fato do seu uso poder gerar ampla vantagem concorrencial no mundo de negócios, podendo causar inúmeros danos aos titulares de dados.

3. Nosso Papel

A adequação à LGPD vai além de uma atualização cadastral ou modificação dos contratos. A norma estabelece uma cultura de melhoria contínua que valoriza a proteção de dados pessoais e acompanha a evolução do tema.

Essa cartilha tem o objetivo de auxiliar o entendimento sobre a Lei. Vale lembrar que este material não visa esgotar todos os temas abordados pela LGPD, mas de informar e apresentar os conceitos básicos trazidos pela lei.



4. História

A Europa, berçário de evoluções legislativas, entre as décadas de 70 e 80 sancionou a primeira norma sobre o tema de forma oficial no Estado da Alemanha. Nesse período, o avanço da computação e da indústria nos países mais desenvolvidos impulsionou o estado alemão a criar normas para regular a privacidade no país.

Em outubro de 1995 o Parlamento Europeu e o Conselho da União Europeia criaram um regulamento que estabelecia regras para serem cumpridas por todos os países da UE. No texto, é perceptível que o conceito de proteção de dados e a interpretação de seus propósitos estão muito mais desenvolvidos e bem próximos das legislações atuais.

No Brasil, a privacidade passou a ser tutelada a partir do Marco Civil da Internet, promulgado em 2013. Assim, foram introduzidos conceitos como neutralidade de rede, liberdade de expressão e foram definidas as obrigações dos órgãos públicos no fornecimento de internet.

Observando os grandes casos de vazamento de dados, a utilização e comércio de informações pessoais, a União Europeia decidiu revisitar suas regras de proteção de dados.

O GDPR, legislação de proteção de dados pessoais que vigora na Europa desde 2018, passou a obrigar empresas de todo mundo a mudar a forma como coletam e tratam dados. Várias leis locais derivam do GDPR, sendo a lei brasileira uma delas.

A Lei Geral de Proteção de Dados (Lei 13.709/18), seguindo os padrões da legislação europeia, dispõe sobre o tratamento de dados pessoais em âmbito nacional, com o objetivo de proteger os direitos fundamentais dos titulares de dados, bem como de garantir a liberdade, privacidade e a livre formação da personalidade de cada indivíduo. A aplicação da LGPD é obrigatória para todas as organizações que tratam dados no território nacional, sejam públicas ou privadas.

5. O que é a Lei Geral de Proteção de dados - LGPD?

A LGPD – Lei Geral de Proteção de Dados visa regular e conscientizar o uso e o tratamento de dados pessoais. Para isso, estabelece princípios e diretrizes que orientam os controladores e operadores de dados para o tratamento responsável de dados.

A Lei define no Art. 1º quem são os responsáveis pelo tratamento:

(...) o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

6. E o que são dados pessoais?

Segundo a LGPD, dados pessoais são informações relacionadas à pessoa natural identificada ou identificável, ou seja, são aquelas informações que permitam a identificação do titular de dados.

Como exemplo, podemos citar os típicos dados cadastrais como nome, endereço, telefone, e-mail, entre outros.



7. O que é tratamento de dados pessoais?

Tratamento de dados pessoais é toda e qualquer operação realizada com dados pessoais, de forma automatizada ou não. A LGPD define como formas de tratamento a coleta, o processamento, a análise, o compartilhamento (externo e interno), o armazenamento, reutilização e a eliminação de dados pessoais.

No artigo 6º, a lei estabelece 10 princípios norteadores do tratamento de dados. Extraímos que as empresas e demais agentes de tratamento de dados somente devem tratar os dados estritamente necessários (princípio da necessidade) e ponderar se coleta de dados está atrelada a uma finalidade específica e informada aos titulares de dados.



Atenção: A LGPD é aplicável a TODOS os dados existentes, sejam eles digitais (cadastros, e-mails) ou físicos (formulários, contratos, currículos). Portanto, deve-se avaliar a real necessidade da coleta de informações, principalmente quando estamos lidando com dados pessoais sensíveis.

8. O que é um dado pessoal sensível?

Dados pessoais sensíveis são dados que contêm informações que possam discriminar o titular de dados de alguma maneira, ou seja, podem ser utilizados de maneira a segregar as pessoas, dividi-las. Por possuir elevado potencial ofensivo, podem causar maiores danos aos titulares.

O artigo 5º, inciso II, estabelece quais são os dados pessoais sensíveis para fins da legislação:

“dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural”.

A lei traz um rol taxativo, ou seja, os dados considerados sensíveis serão somente os constantes no trecho acima.

9. Por que as empresas devem fazer o controle de dados pessoais?

Em regra, todas as empresas em algum momento tratam dados pessoais. Esses dados podem ser relativos a usuários, funcionários, terceirizados ou outros. Ao fazerem isso se tornam “guardiões” de dados e, portanto, se submetem às regras estipuladas pela LGPD.

Desta forma, é importante que todos agentes de tratamento de dados pessoais mantenham controle dos dados pessoais que utiliza, a fim de evitar o seu uso de forma indevida e prevenir eventual responsabilização por descumprimento da lei.

Para tanto, as empresas adotam um programa de privacidade eficaz, que garanta o cumprimento das diretrizes legais.

10. Quais são os fundamentos da LGPD?



11. Quais os Princípios da LGPD?

Princípios são valores que norteiam o tratamento de dados pessoais, estabelecendo diretrizes a serem respeitadas em toda a atuação dos operadores e controladores. São princípios da LGPD:

- **Finalidade:** Diz respeito a razão da empresa colher e tratar os dados que é responsável. Deve ser sempre realizado a fim de cumprir finalidades específicas (uma ou mais), as quais devem ser informadas ao titular de dados;
- **Adequação:** O tratamento dos dados deve ser compatível com as finalidades informadas ao titular;
- **Livre acesso:** Diz respeito a garantir o exercício de direitos dos titulares de dados, de forma facilitada e gratuita, sobre informações a respeito do tipo, forma, duração de tratamento, exclusão, entre outros direitos.
- **Não discriminação:** É a impossibilidade de realização de tratamento para fins discriminatórios, ilícitos ou abusivos;
- **Necessidade:** Diz respeito ao tratamento de dados estritamente necessários, não abusivos ou excessivos;
- **Prevenção:** Diz respeito a adoção de medidas técnicas e administrativas a fim de prevenir danos aos titulares de dados em decorrência incidentes;
- **Qualidade dos dados:** Busca garantir aos titulares a exatidão, clareza, relevância e atualização dos dados coletados;
- **Responsabilidade e prestação de contas:** Necessidade de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas relativas à proteção dos dados pessoais;
- **Transparência:** Deve ser garantido ao titular de dados informações claras e precisas sobre o tratamento de seus dados pessoais;
- **Segurança:** Devem ser adotadas medidas técnicas e administrativas de segurança a fim de proteger os dados pessoais tratados.



12. Para quais dados não se aplica a LGPD?

A LGPD não se aplica aos dados utilizados para fins exclusivamente particulares e não econômicos, jornalísticos ou artísticos, para fins acadêmicos, investigações, repressão de crimes ou em casos de segurança pública e defesa nacional.

13. Quem são os agentes de tratamento?

São considerados agentes de tratamento de dados o controlador e operador de dados.

A lei declara que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. A qualquer momento pode ser necessária a demonstração clara dessas operações, podendo os mesmos serem responsabilizados por eventual infração à LGPD.

13.1 Quem é o Controlador?

O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referente ao tratamento de dados pessoais. Ou seja, é a empresa ou o responsável pelas decisões quanto ao tratamento de dados pessoais: é ele quem possui o poder de decisão sobre o que fazer, como fazer e porquê fazer.

13.2 Quem é o Operador?

O operador é responsável por executar o tratamento dos dados, em regra, sob ordens e orientação do controlador. Assim como o controlador, podem ser pessoas naturais ou jurídicas. São possíveis exemplos de operadores: escritório de contabilidade, agência de marketing ou empresa de arquivo.





13.3 Quem é o Encarregado de Dados ou DPO (Data Protection Officer)?

É um profissional de conhecimento ímpar e multidisciplinar, que figura como protagonista para que os órgãos e entidades estejam em conformidade com a LGPD. Deverá ser indicado pelo controlador e atuará como um canal de comunicação entre todos os agentes atuantes no âmbito da LGPD (controlador, titulares de dados e a Autoridade Nacional de Proteção de Dados).

Suas informações de contato e identificação deverão ser divulgadas publicamente, de forma clara pelo controlador.

13.4 O que é o Relatório de Impacto à proteção de dados pessoais?

Documento fundamental para alguns processos de tratamento de dados pessoais, contém a descrição das fases de tratamento, a identificação de quem acessa os dados e a descrição quanto os mecanismos de privacidade, segurança e mitigação de riscos. Este documento poderá ter sua produção ordenada pela Autoridade Nacional de Dados – ANPD ou, ainda, ser requisitada para vistoria a qualquer tempo.

13.5 Quem são os titulares de dados?

O titular de dados é a PESSOA NATURAL (física) a quem se referem os dados pessoais tratados. Como exemplo, podem ser os usuários dos serviços prestados pelas empresas que tratam os dados, assim como os seus funcionários e prestadores de serviço.



13.6 Quais os direitos dos titulares de dados?

A LGPD estabelece os seguintes direitos aos titulares de dados:

- Confirmação de existência de tratamento de dados pela empresa ou seus agentes;
- Acesso aos dados tratados pela empresa, através de requisição ao controlador;
- Correção e/ou atualização facilitada dos dados pessoais tratados;
- Anonimização, bloqueio ou eliminação de dados que tenham sido coletados em excesso ou que tenham cumprido ou perdido a sua finalidade, e ainda daqueles tratados de maneira diversa ao legalmente permitido;
- Portabilidade/transferência de seus dados entre controladores;
- Eliminação dos dados tratados sem consentimento ou que se desviem de sua finalidade;
- Informações sobre o compartilhamento de seus dados; e;
- Ser informado quanto a possibilidade de não fornecer o seu consentimento;

14. O que é o consentimento do titular?

É a concordância e autorização do titular quanto ao tratamento de seus dados pessoais nos casos em que seus dados serão tratados com a base legal de “consentimento do titular”.

O consentimento deve ocorrer de forma livre, informada, inequívoca e para uma finalidade determinada. Ele pode ser dado por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

IMPORTANTE

Eventuais consentimentos que estejam redigidos de forma genérica serão considerados nulos.

15. Quando os dados poderão ser tratados sem consentimento?

O consentimento é apenas uma das bases legais que permitem o tratamento de dados pessoais. Assim, dados pessoais poderão ser tratados sem o consentimento caso seja utilizada qualquer outra base legal estabelecida pela LGPD. São consideradas, assim, bases legais ou hipóteses para tratamento de dados sem o consentimento do titular:

- cumprimento de obrigação legal ou regulatória.ex. cumprimento de obrigações frente a receita federal;
- uso pela administração pública;
- estudos realizados por órgãos de pesquisa;
- necessário para o devido cumprimento de contratos;
- exercício regular de direito em processo judicial, administrativo ou arbitral;
- proteção da vida e integridade física;
- tutela da saúde em procedimento realizado por profissionais de saúde/ serviços de saúde/agência sanitária;
- legítimo interesse do controlador ou de terceiros; e
- proteção ao crédito.



Atenção: No tratamento de dados pessoais sensíveis, não poderão ser utilizadas as hipóteses de tratamento de legítimo interesse, a execução de contrato e proteção ao crédito para tratar dados sem consentimento do titular.

Lembre-se:

O enquadramento da base legal deverá ser feito de forma extremamente cuidadosa, pois a escolha da base legal deverá manter uma relação direta com a finalidade da coleta e tratamento dos dados.

16. Como solicitar o consentimento do titular?

O consentimento do titular de dados poderá ser solicitado a partir da assinatura de um termo, que deverá ter redação clara e indicar a finalidade específica do tratamento.

Esse consentimento poderá ser revogado a qualquer tempo, bastando requerimento expresso do titular, por procedimento gratuito e facilitado.

17. Como tratar dados sensíveis?

O tratamento de dados pessoais sensíveis deve ter maior cautela, por apresentar maior potencial danoso aos titulares de dados, devendo se dar especial atenção aos princípios e direitos dos mesmos, uma vez que eventual incidente de segurança com esses tipos de dados pode trazer consequências mais gravosas aos direitos e liberdades dos titulares, e por isso precisam de um grau superior de proteção e responsabilidade.

Analisando sob a ótica das bases legais para tratamento de todos os dados pessoais, são estas: 1) consentimento; 2) obrigação legal ou regulatória; 3) para execução de políticas públicas pela administração pública; 4) estudos por órgão de pesquisa; 5) execução de contrato; 6) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; 7) proteção da vida ou da incolumidade física do titular ou de terceiro; 8) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; 9) interesse legítimo/ e 10) proteção ao crédito.

Por sua vez, as bases legais que autorizam o tratamento dos dados pessoais sensíveis, estão previstas no artigo 11 da Lei Geral de Proteção de Dados. Da leitura dos incisos podemos inferir que há vedação ao tratamento de dados sensíveis para:

- Execução de contrato;
- Com base em interesse legítimo; e
- Para a proteção ao crédito.

Demais possibilidades, ainda que com algumas restrições, são possíveis.



18. O que é Anonimização de dados?

O dado anonimizado não permite a identificação de seu titular, uma vez que passou pelo processo técnico irreversível de anonimização.

Assim, o dado anonimizado não poderá, de qualquer forma, voltar a “identificar” quem era seu titular, perdendo sua qualidade de dado pessoal.

O dado pseudonimizado, ao contrário, poderá ser revertido e utilizado para identificar seu titular.

Lembre-se

Dados efetivamente anonimizados não estão sujeitos à LGPD. Porém, dados pseudonimizados devem seguir a legislação por se tratar de dados pessoais.

19. Quem fiscaliza e regulamenta o tratamento de dados pessoais no Brasil?

A fiscalização é responsabilidade da Autoridade Nacional de Proteção de Dados – ANPD e demais órgãos públicos fiscalizadores, reguladores ou judiciais.

Insta salientar que a ANPD é uma Autarquia Federal responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados no Brasil, cabendo a ela a responsabilidade de aplicar as sanções administrativas definidas na lei, como multas e suspensão do tratamento de dados.





20. Quais são as sanções para o descumprimento da LGPD?

Descumprido algum dos princípios ou normas estabelecidos pela LGPD, o controlador ou operador poderão ser sancionados pela ANPD.

As sanções são previstas nos artigos 52 e seguintes da LGPD. São eles:

- Advertência com prazo para adoção de medidas corretivas;
- Multa simples de até 2% (dois por cento) do faturamento anual da empresa, limitada a 50 milhões de reais por infração;
- Multas diárias de até 2% (dois por cento) do faturamento anual da empresa, limitada a 50 milhões de reais por infração
- Publicar a infração após apurada;
- Bloqueio de dados pessoais;
- Eliminação de dados incorretamente tratados;
- Suspensão do funcionamento do banco de dados por até 6 meses sendo prorrogável por mais 6 meses;
- Suspensão do exercício da atividade de tratamento dos dados pessoais por até 6 meses sendo prorrogável por mais 6 meses;
- Proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados;



Atenção: No momento de aplicação de sanção em razão de eventual incidente, a ANPD irá avaliar, dentre outros aspectos, se a empresa se adequou aos princípios e normas da LGPD, podendo atenuar a sanção nos termos do art. 52, §1º, inciso VIII.

21. Quando a LGPD entrou em vigor?

A LGPD entrou em vigor, em quase sua totalidade, no dia 18 de setembro de 2020. Em agosto de 2021 iniciou a vigência das sanções administrativas previstas na lei.

22. Conclusão

Diante desse contexto de constante evolução social e tecnológica, em que os dados pessoais desenvolvem diariamente o papel de protagonista das relações interpessoais, é fundamental que as empresas tratem dados pessoais em estrita observância aos princípios e regras da LGPD.

Cientes de que a adequação legal exigirá não somente a redação de documentos e melhoria de processos corporativos, mas também uma evolução constante da cultura empresarial, a High Compliance elaborou esta cartilha para simplificar o entendimento da lei e se coloca à disposição para auxiliá-los a seguir este caminho tão importante.

23. Perguntas Frequentes:

1) A Lei proíbe o tratamento de dados pessoais?

Não. A LGPD não proibiu o tratamento de dados, mas sim estabeleceu maior rigor e medidas de segurança para sua proteção. A lei traz direitos, deveres e responsabilidades do titular e dos agentes de tratamento de dados pessoais, obrigando-os a cumprir com princípios e bases legais de tratamento estabelecidos pela lei.

2) Em caso de vazamento de dados o que devo fazer?

Antes de pensar em materialização de um vazamento, é importante que a empresa identifique e adote medidas preventivas razoáveis para mitigar o risco de incidente com dados pessoais tratados.

Em caso de incidente com dados pessoais, segundo o art. 48 da LGPD, o agente de tratamento deverá comunicar a ANPD e ao titular, descrevendo os dados afetados, as informações sobre titulares envolvidas os riscos e quais medidas foram tomadas a fim de sanar ou mitigar esse vazamento.

3) A quem se aplica a LGPD?

A LGPD se aplica a qualquer pessoa física ou jurídica que realize o tratamento de dados pessoais de maneira lucrativa.

4) A LGPD vale somente para dados digitais?

Não. A Lei se aplica a todos os dados pessoais tratados, sejam eles físicos (contratos, currículos, pastas) ou digitais (cadastros, sistemas internos, e-mails).

5) A LGPD já está em vigor?

Sim, salientando que desde 1º de agosto de 2021 as sanções administrativas estão em vigor.

6) O tamanho da empresa importa para a LGPD?

Não. A LGPD se aplica a todas as empresas que realizam tratamento de dados, não havendo distinção quanto ao seu tamanho.

7) Existem condições em que a LGPD não se aplica?

A LGPD não se aplicará ao tratamento de dados não pessoais, bem como dos dados pessoais voltados para fins particulares e não econômicos.

8) Existe um prazo para tratamento de dados pessoais?

A LGPD não determina um prazo específico para o tratamento de dados. Desta forma, havendo cessado a finalidade do tratamento, este deverá ser descartado. Ainda, o art. 15 da LGPD apresenta outras hipóteses para o fim do tratamento de dados, quais sejam

- Revogação de consentimento;
- Fim do período de tratamento; e
- Determinação da ANPD.

9) O usuário pode requerer a exclusão de seus dados pessoais?

Qualquer titular que tenha seus dados tratados por algum controlador poderá requerer a exclusão de seus dados, além de solicitar a transferência de dados para outro fornecedor de serviços.

O controlador, entretanto, poderá se opor à exclusão dos dados solicitados pelo titular, apresentando razões fundamentadas acerca da continuidade/guarda das informações. Por exemplo, na área da saúde, pode-se recusar a exclusão de dados de prontuários médicos, ainda que solicitados pelo paciente, haja vista a obrigação legal de guarda ou compartilhamento desses dados.

Insta salientar que, em regra, os direitos dos titulares devem ser respeitados, contudo, há exceções vinculadas a bases legais específicas que podem inviabilizar.

23. Histórico de Alterações

Revisão	Referências	Elaborador	Design gráfico	Responsável	Aprovado por	Resumo da Alteração
	A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709	High Compliance	Gabriel de Carvalho, e Monique Soares	Simone Domiciano	Aline Alvarenga, e Leandro Oliveira	Primeira Versão
1ª						
2ª						
3ª						
4ª						
5ª						
6ª						

Cartilha Descomplicando a LGPD – Lei Geral de Proteção de Dados

Elaboração: Gerência de Gestão Estratégica e Gerência Ceivap

Texto: Gerência de Gestão Estratégica

Design Gráfico: Gabriel Barboza (Estagiário) / Monique Soares (Especialista Administrativa-Comunicação)