Tudo o que você precisa saber sobre LGPD

sidia

Lei Geral de Proteção de Dados

Lei 13.703/18

Olá! Tudo bem? Vamos falar sobre Proteção de Dados Pessoais?

Ao final de cada capítulo, há um formulário para fixação do seu conhecimento.

É muito importante sua resposta para sabermos o que você entendeu sobre a legislação. Combinado?

Antes de falar sobre a LGPD, sabe por que a proteção de dados é tão importante?

As facilidades da tecnologia somente são possíveis através do **uso de nossas informações pessoais.**

Diversos aplicativos e softwares **armazenam dados pessoais** e, assim, conseguem identificar a **pessoa natural** e o **perfil do usuário,** através do **padrão de pesquisas, preferências, acessos e etc.**

Desta forma se torna mais ágil a **comunicação** e a **oferta de serviços** que mais atendem o usuário, conforme o **perfil identificado**.

No entanto, **sem a proteção de dados**, nossa privacidade fica **vulnerável**, sujeita a **compartilhamentos** e **comercialização de forma indevida.**

Resultando em constante **monitoramento**, propostas de **serviços não solicitados**, o acesso da nossa identidade e perfil para **negócios e até crimes**.

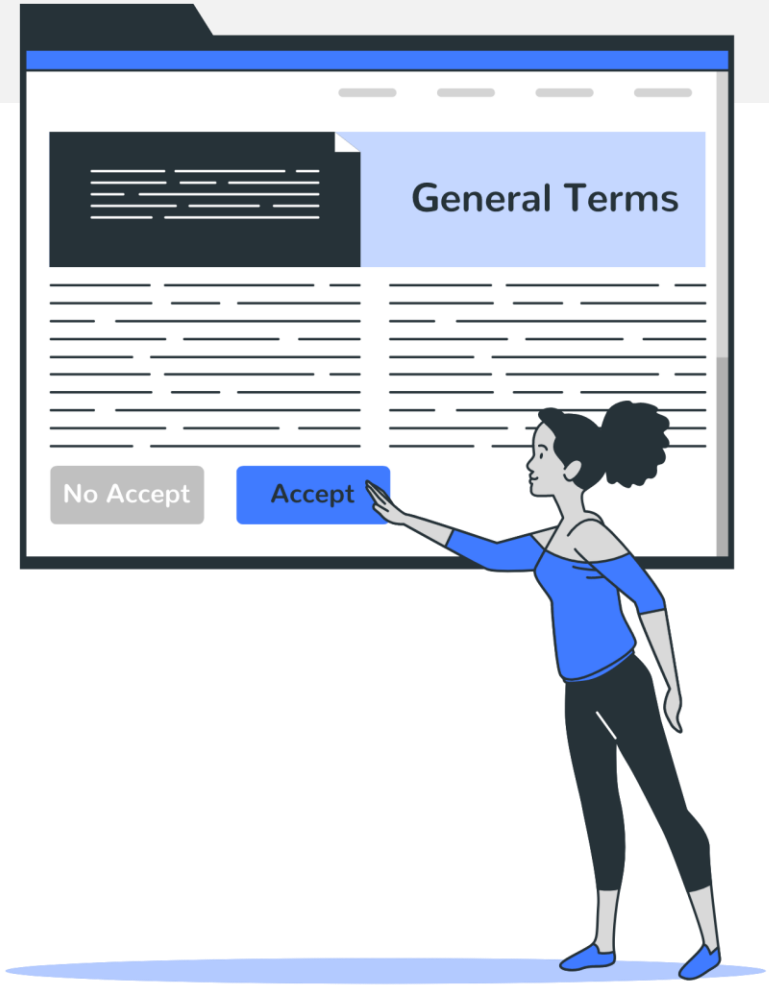
Veja mais sobre a **importância da proteção de dados**: https://youtu.be/TzI5VfvQA6I

Termos da LGPD

Segundo a autora Patrícia Peck Pinheiro, no livro Proteção de Dados Pessoais, comentários à Lei n. 13.709/2018

Titular: Pessoa a quem se referem os dados pessoais que são objeto de tratamento. **É sempre uma pessoa física, natural.** (OBS: Toda Pessoa Jurídica tem seu sócio ou representante, também pessoa física).

Tratamento: Toda operação realizada com algum tipo de manuseio de dados pessoais. Ocorre quando os dados pessoais são utilizados por pessoa ou organização que não seja o titular, como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.



Termos da LGPD

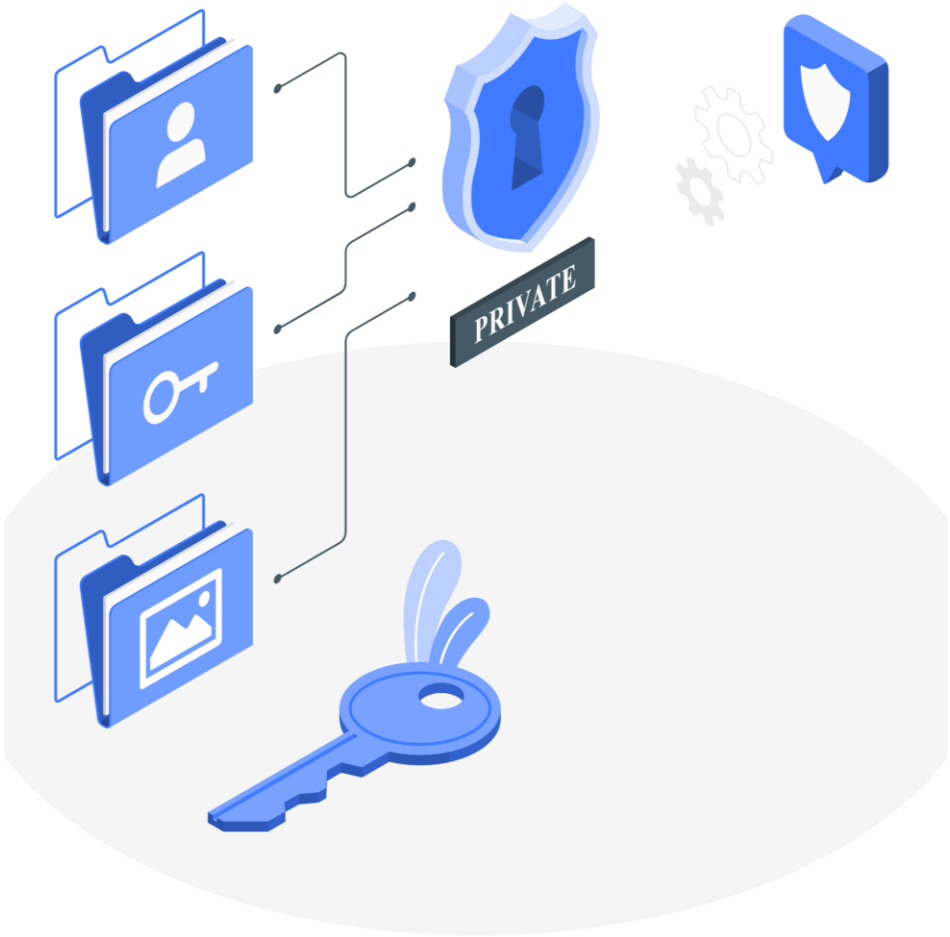
Segundo a autora Patrícia Peck Pinheiro, no livro Proteção de Dados Pessoais, comentários à Lei n. 13.709/2018

Dados Pessoais: Toda informação relacionada a uma **pessoa identificada ou identificável**, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial, ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva.

Dados Pessoais sensíveis: São **dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais**, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Termos da LGPD

Segundo a autora Patrícia Peck Pinheiro, no livro Proteção de Dados Pessoais, comentários à Lei n. 13.709/2018



Dados anonimizados: são dados relativos a um titular que não possa ser identificado, considerado a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento. Se trata de casos cujo uso de dados não é autorizado (ex. relatórios, estatísticas, pesquisas, compartilhamento de dados e etc). Nestes casos, a identificação do titular não pode ser revelada, portanto, deve ser anonimizada.

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

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Existem outros tipos de autorização, decorrente de base legal (quando a norma exige.

Termos da LGPD

Agentes de tratamentos

Controlador (Art. 5º, VI, da LGPD): Pessoa natural ou jurídica, de direito público ou privado, **a quem competem as decisões referentes ao tratamento de dados pessoais (estabelece as regras e diretrizes)**. O **controlador** é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais.

Operador (Art. 5º, X, da LGPD): Pessoa natural ou jurídica, de direito público ou privado, **que realiza o tratamento de dados pessoais em nome do controlador**. O **operador** deverá realizar o tratamento **segundo as instruções fornecidas pelo controlador**, que verificará a observância das próprias instruções e das normas sobre a matéria (Art. 39 da LGPD).

Saiba mais em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf

Termos da LGPD

Agentes de tratamentos

Encarregado (ou DPO – *Data Protection Officer*): Conforme o artigo 41 da LGPD, o controlador de dados deverá **indicar um encarregado pelo tratamento de dados pessoais**. O **encarregado** é o indivíduo responsável por **garantir a conformidade de uma organização, pública ou privada, à LGPD.**

De acordo com o § 2º do art. 41 da LGPD, o **encarregado** possui as seguintes atribuições:
-aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
-receber comunicações da autoridade nacional e adotar providências;
-orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
-executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

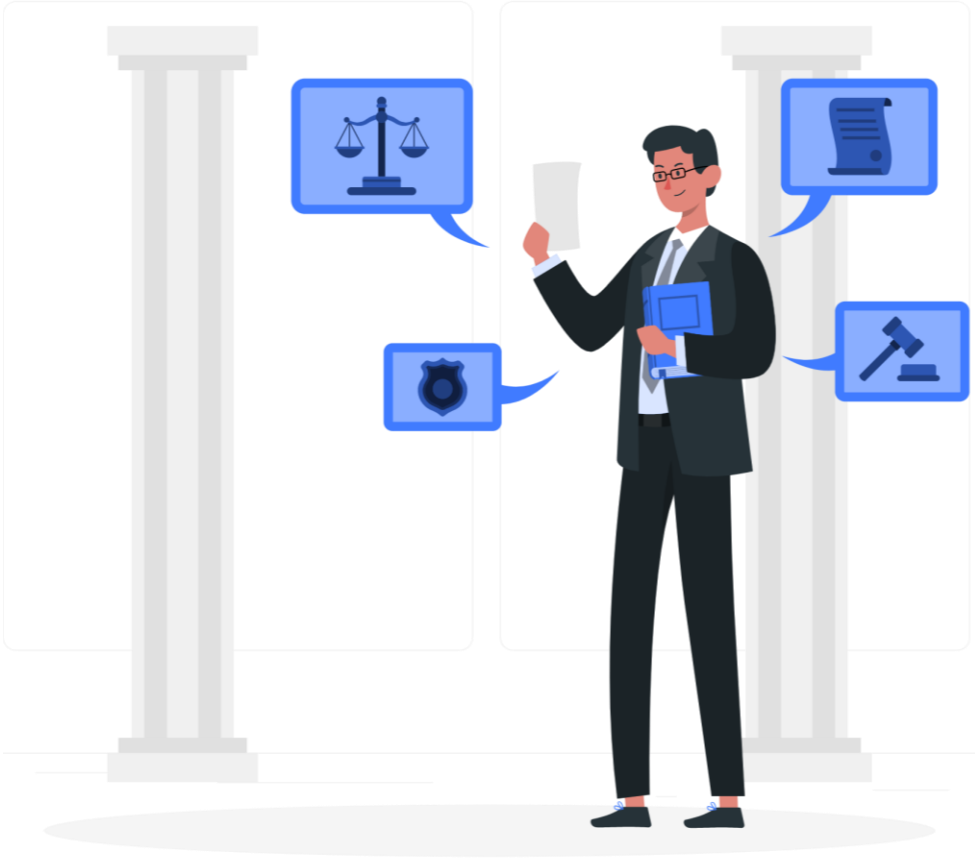
Saiba mais em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf

Termos da LGPD

ANPD

ANPD: A Autoridade Nacional de Proteção de Dados (ANPD) foi criada para trazer mais segurança e estabilidade para aplicação da Lei geral de Proteção de Dados.

A ANPD será responsável pela orientação geral no que tange à adequação e aplicação da Lei Geral de Proteção de Dados no Brasil, além de poder alterar a Lei n. 13.709/2018 (LGPD). A ANPD também será responsável pela fiscalização dos tratamentos e aplicação das sanções e multas previstas pela LGPD.



Exemplos envolvendo agentes de tratamento

Exemplo 1 - **Médica profissional liberal**: Uma médica, profissional liberal, armazena os prontuários e os demais dados pessoais de seus pacientes no computador de seu consultório. A médica, pessoa natural, é a controladora dos dados pessoais.

Exemplo 2 - **Médica empregada de um hospital**: Uma médica é empregada de um hospital, constituído sob a forma de associação civil sem fins lucrativos. Nessa condição, atua como principal representante do hospital junto a um serviço de armazenamento de dados de pacientes em nuvem, inclusive assinando os contratos correspondentes. O hospital, isto é, a associação civil, pessoa jurídica de direito privado, é o controlador na hipótese. A médica, por atuar sob o poder diretivo da organização, não se caracteriza como agente de tratamento.

Exemplo 3 - **Órgão público contratante de um serviço de inteligência artificial**: Um órgão público, vinculado à União, contrata uma solução de inteligência artificial fornecida por uma sociedade empresária com a finalidade específica de realizar o tratamento automatizado de decisões com base em um banco de dados gerido pelo órgão. Seguindo as instruções fornecidas pelo gestor público responsável e estabelecidas em contrato, a sociedade empresária realiza as operações necessárias para viabilizar o tratamento dos dados em questão. A União, pessoa jurídica de direito público, é a controladora na hipótese. Não obstante, o órgão público responsável detém obrigações legais específicas em face dos titulares e da ANPD, conforme previsto na LGPD. A sociedade empresária é a operadora, uma vez que realiza o tratamento dos dados conforme as instruções fornecidas pelo controlador. Por fim, o gestor público responsável, por atuar como servidor público subordinado à União, não se caracteriza como agente de tratamento.

Da responsabilidade e do ressarcimento de danos

É importante salientar que embora existam os agentes de tratamentos responsáveis pela proteção de dados pessoais, **é dever de TODOS zelar pela identidade dos dados de titulares e a sua privacidade**, cabendo **ação de regresso a quem der causa de responsabilização ao agente de tratamento**, vejamos o art. 42 da LGPD:

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. (...)

§ 4º Aquele que reparar o dano ao titular **tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso**.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

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

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

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

Qual é o meu papel para garantir a proteção de dados pessoais?

Seguem alguns exemplos:

Minimização de dados (armazenar somente o essencial)	Controle de acesso aos arquivos de trabalho (mesa limpa, bloqueio de tela, senhas seguras)	Anonimização de Dados (ocultar dados que permitam identificar o titular)
Conhecer e atender às normas internas da empresa e zelar pela Governança em Dados Pessoais	Reportar qualquer ameaça à proteção dos dados ao Encarregado de Dados ou Comitê de Segurança e Privacidade	Propor melhorias nos procedimentos de proteção de dados pessoais
Comunicar ao Encarregado toda mudança de procedimento que envolva dados pessoais	Atender à base legal	Não compartilhar arquivos contendo dados pessoais

Lei Geral de Proteção de Dados

Lei 13.703/18

Neste capítulo, vamos falar sobre os princípios que norteiam a lei?

O que é LGPD?

Lei Geral de Proteção de Dados, ou simplesmente LGPD, é a lei que regulamenta o tratamento de dados pessoais, inclusive nos meios digitais.

A intenção da lei é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Hoje aprenderemos um pouco sobre os princípios que regem a lei. Vamos começar?

Princípio da finalidade

O tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, explícitos e informados. Ou seja, as empresas devem explicar para que usarão cada um dos dados pessoais.

Exemplo: se um aplicativo solicita o e-mail do usuário para a finalidade específica de login, esse dado não pode ser utilizado para enviar publicidade ou ofertas.

Princípio da adequação

Os dados pessoais tratados devem ser compatíveis com a finalidade informada pela empresa. A justificativa para solicitação dos dados deve fazer sentido com o caráter da informação que você pede.

Continuando o exemplo do app: Foi solicitado o endereço do usuário sob a justificativa de traçar rotas mais rápidas para o trabalho. Essa justificativa é adequada ao que o app se propõe. No entanto, solicitar o CPF do usuário não seria adequado.

Princípio da necessidade

As empresas devem utilizar apenas **os dados estritamente necessários** para alcançar as suas finalidades.

Caso o aplicativo desenvolvido tenha como objetivo apenas traçar rotas alternativas mais rápidas para que o usuário se desloque de casa para o trabalho, seguindo o exemplo anterior, **os únicos dados pessoais necessários serão o e-mail para login e o endereço residencial e laboral do usuário. O recolhimento de qualquer outro dado fere o princípio da necessidade.**

Princípio do livre acesso

Garantia, **aos titulares**, de **consulta facilitada e gratuita** sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

É possível **solicitar os seus dados pessoais das empresas com que você e até mesmo perguntar como os dados são geridos**.

Isso vale para a sua operadora de telefonia, para o seu empregador e até mesmo para aquele jogo que solicitou seu e-mail para login.

Princípio da qualidade dos dados

Deve ser **garantido aos titulares** que as **informações** que a empresa tenha sobre eles sejam **verdadeiras e atualizadas**. É necessário ter atenção à **exatidão, clareza e relevância dos dados,** de acordo com a necessidade e com a finalidade de seu tratamento.

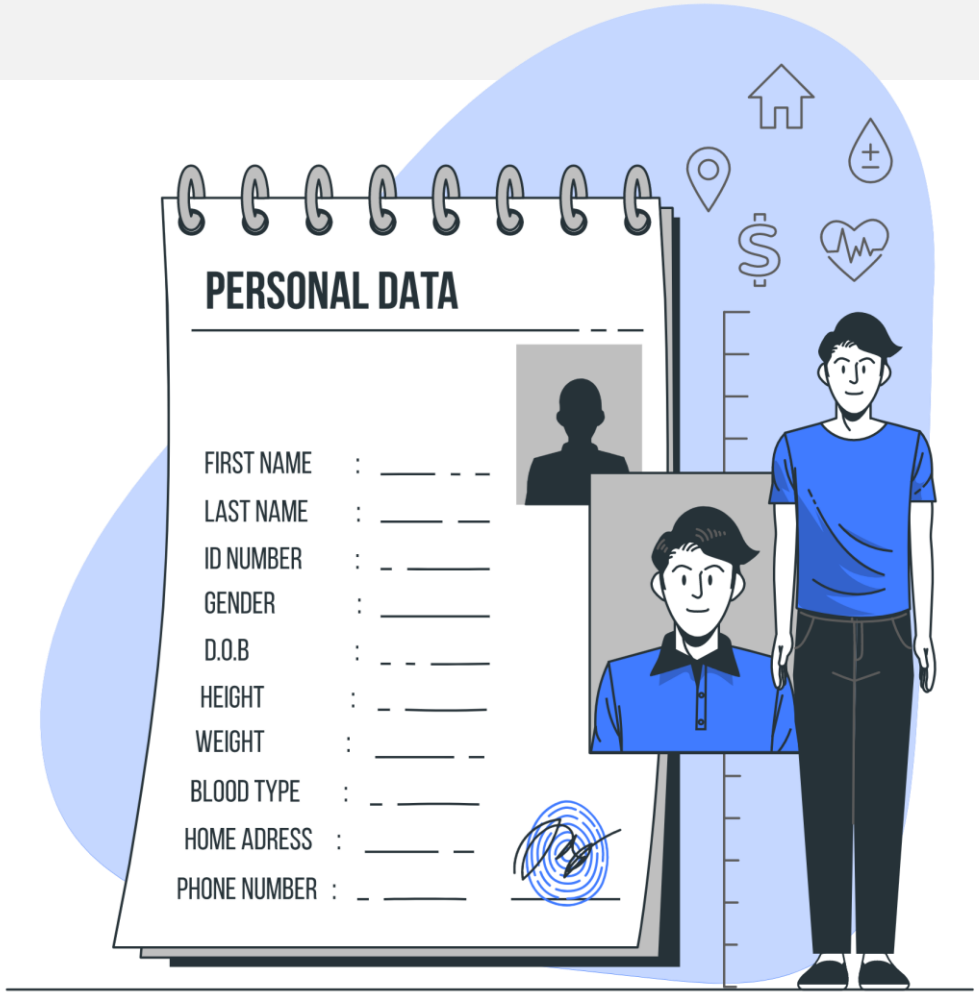
O Sidia, como controlador de dados pessoais, garante a todos os colaboradores a possibilidade de consulta e atualização de seus dados pessoais.

Princípio da transparência

Visa a garantia, aos titulares, de **informações claras, precisas e facilmente acessíveis** sobre a realização do tratamento e os **respectivos agentes de tratamento**, bem como formulada numa linguagem clara e simples.

As políticas e os procedimentos da empresa precisam ser públicos aos colaboradores, especificando quais os responsáveis pelos tratamentos de dados pessoais.

O Canal do Encarregado é um meio para obtenção das informações. No Sidia, você pode contatar a Amanda Moura (dataprivacy@sidia.com), nossa DPO.



Princípio da segurança

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.

Como medidas de proteção Podemos listar o controle de acesso a prédios, o conceito de mesa limpa, a impossibilidade de uso de pen drive em computadores corporativos, o hábito de travar a tela do computador quando se ausentar da mesa.

Princípio da prevenção

As empresas devem **adotar medidas prévias** para evitar a ocorrência de danos em virtude do tratamento de dados pessoais.

Caso você detecte algum risco à proteção de dados na empresa, você mesmo pode indicar ao Encarregado, evitando que o risco se torne uma efetiva ofensa à integridade dos dados.

Todos somos responsáveis pela proteção dos dados. Ajude nosso Encarregado!

Princípio da não-discriminação

Os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares.

Princípio da responsabilização e da prestação de contas

- As empresas deverão demonstrar todas as medidas tomadas para o cumprimento da LGPD;
- Esse informativo, por exemplo, é um meio de cumprimento a este princípio;
- Vamos divulgar entre os nossos colaboradores e amigos os conceitos aprendidos!

Direitos do titular

Confirmação da existência de tratamento

O titular dos dados tem o direito de confirmar se uma empresa realiza o tratamento de seus dados pessoais.

Acesso aos dados

Além de saber se a empresa trata seus dados pessoais, o titular também pode pedir acesso aos seus dados.

Correção de dados incompletos, inexatos ou desatualizados

O titular de dados pode solicitar a correção de dados pessoais quando estes estiverem incompletos, inexatos ou desatualizados.

Anonimização, bloqueio ou eliminação de dados

O titular de dados também tem o direito de solicitar a anonimização (processo que torna um dado impossível de ser vinculado a um indivíduo), bloqueio ou eliminação de dados quando eles forem desnecessários, excessivos ou tratados em desconformidade com a LGPD.

Portabilidade dos dados

O titular de dados pode solicitar a portabilidade dos dados, ou seja, a transferência das suas informações pessoais a outro fornecedor de serviço ou produto.

É necessária uma requisição expressa para que a portabilidade ocorra.

Informações sobre o campartilhamento de dados

É direito do titular saber exatamente com quem o controlador está compartilhando seus dados. Isso inclui entidades públicas e privadas, que deverão ser expressamente nomeadas.

Eliminação dos dados pessoais tratados com o consentimento do titular

Se o titular dos dados consentiu com o tratamento, mas mudou de ideia e não quer mais que a empresa trate seus dados pessoais, ele pode solicitar a eliminação desses dados.

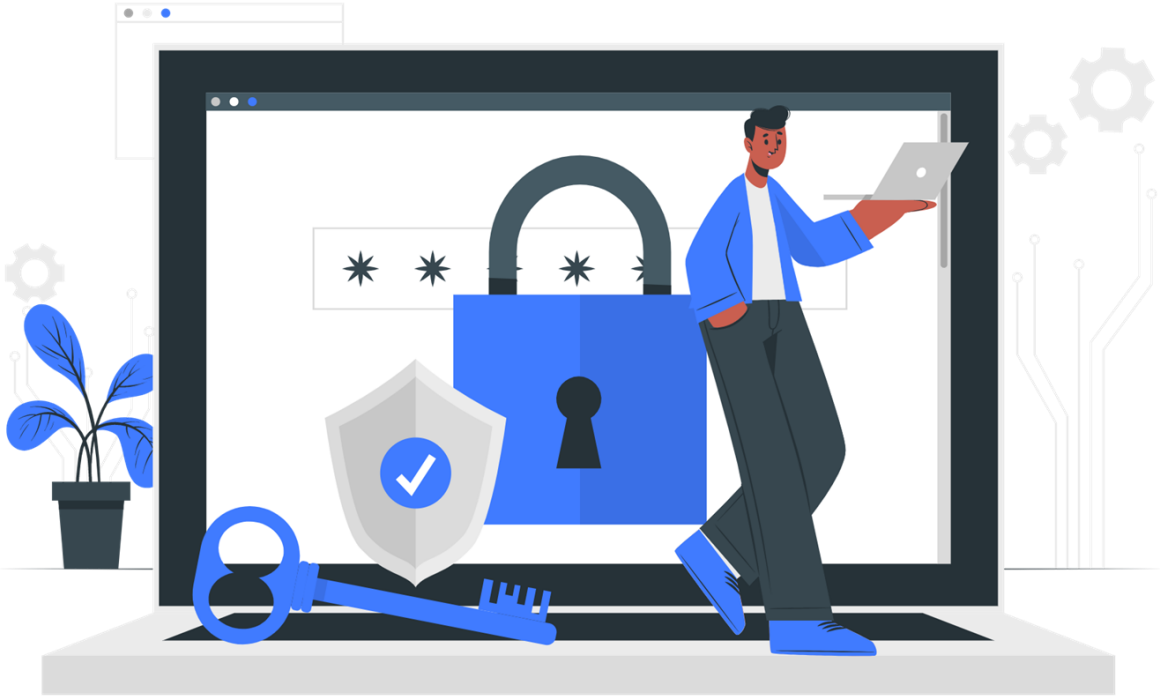
A empresa conservará os dados, mesmo se o titular solicitar a eliminação, nas seguintes situações:

- cumprimento de obrigação legal ou regulatória pelo controlador;
- estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
- uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Revogação de consentimento

Qualquer consentimento dado para o tratamento de dados pessoais pode ser revogado.

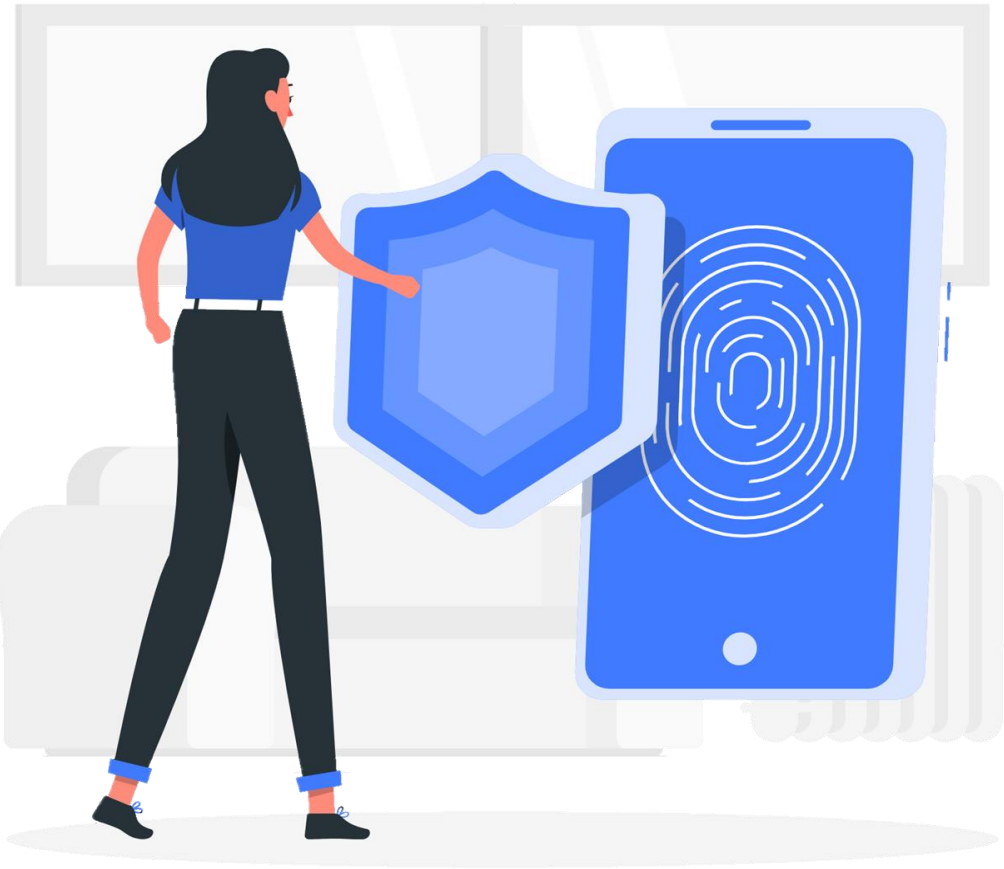
Lembre-se: para a *eliminação* dos dados é necessária *requisição específica*.



Privacy by design

Tem como proposta central incorporar a privacidade e a proteção de dados pessoais em todos os projetos desenvolvidos por uma organização, desde a sua concepção.

Desta forma, garante privacidade e permite que os indivíduos tenham controle sobre seus dados pessoais, o que consequentemente confere vantagem competitiva às organizações que adotam a metodologia.



Princípios do Privacy by design

Proativo e não reativo; preventivo, e não corretivo

- A metodologia Privacy by Design implica em adotar uma postura proativa, em vez de reativa. A ideia é prever e prevenir incidentes de privacidade antes que eles ocorram.

Privacidade como padrão (Privacy by Default)

- A **privacidade** deve ser sempre a **configuração padrão** em qualquer sistema ou mesmo prática de negócio, não exigindo qualquer interação ou configuração por parte do usuário.
- O indivíduo não precisa agir para adotar configurações de privacidade mais restritas: elas já vêm embutidas de forma padrão no produto, tecnologia ou serviço.

Princípios do Privacy by design

Privacidade incorporada ao Design

- Este princípio coloca a privacidade como incorporada ao design e à arquitetura de sistemas de TI e práticas de negócio. Ou seja, a privacidade é um componente essencial do sistema, sem diminuir sua funcionalidade.

Funcionalidade total

- Evitar a existência de falsos dilemas, como privacidade *versus* segurança.
- A ideia é acomodar todos os interesses e objetivos legítimos da organização, e não apenas os relacionados à privacidade.

Princípios do Privacy by design

Segurança de ponta a ponta

- Adoção de medidas robustas de segurança de ponta a ponta, protegendo os dados coletados durante todo seu ciclo de vida.

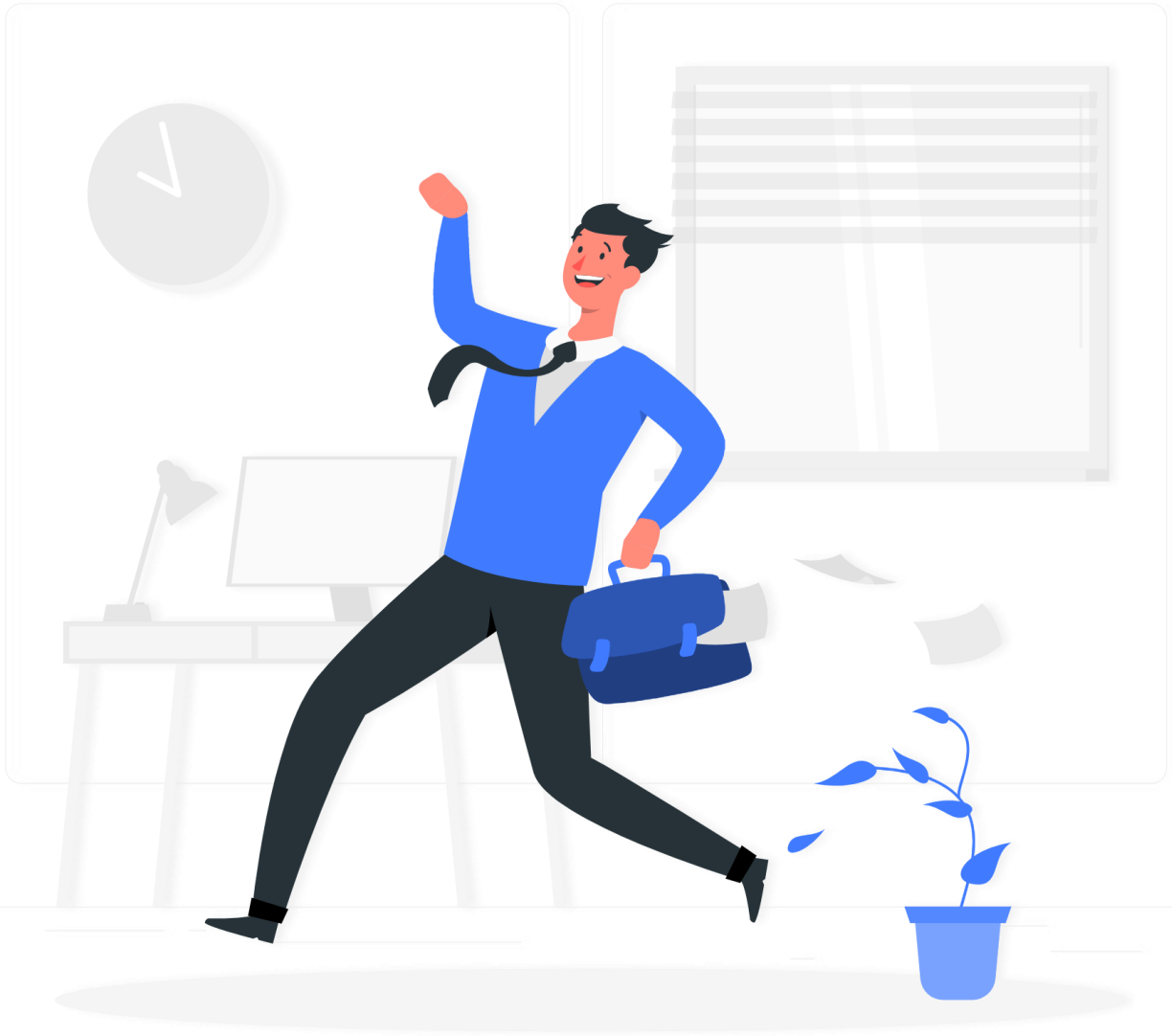
Visibilidade e transparência

- As empresas devem permitir que seja verificado que elas cumprem o que prometem sobre os dados dos usuários, seja diretamente ou por auditorias independentes.

Respeito pela privacidade do usuário

- Garantir a segurança dos dados do usuário envolve diretrizes de segurança da informação capazes de assegurar a confidencialidade, integridade e disponibilidade dos dados e informações durante todo seu ciclo de vida.

Da responsabilidade e do ressarcimento de danos



Casos em que os agentes de tratamento não serão responsabilizados (art. 43):

- Quando provarem que não realizaram o tratamento de dados que lhe está sendo atribuído;
- Quando, ainda que tiver realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
- Quando o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

O tratamento de dados pessoais será irregular quando (art. 44):

- Deixar de observar a legislação; ou
- Não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I – o modo pelo qual é realizado;

II – o resultado e os riscos que razoavelmente dele se esperam;

III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Sanções administrativas LGPD

Tipos de penalidades

O art. 52 da LGPD prevê que os agentes de tratamentos de dados (controlador, operador e encarregado), em razão das infrações cometidas às normas previstas na LGPD, ficam sujeitos às seguintes sanções (art. 52):

I - advertência, com **indicação de prazo para adoção de medidas corretivas**;

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

III - **multa diária**, observado o limite total a que se refere o inciso II;

IV - **publicização da infração** após devidamente apurada e confirmada a sua ocorrência;

V - **bloqueio dos dados pessoais** a que se refere a infração até a sua regularização;

VI - **eliminação dos dados pessoais** a que se refere a infração;

Tipos de penalidades

O art. 52 da LGPD prevê que os agentes de tratamentos de dados (controlador, operador e encarregado), em razão das infrações cometidas às normas previstas na LGPD, ficam sujeitos às seguintes sanções (art. 52):

VII, VIII e IX – VETADO;

X - **suspensão parcial do funcionamento do banco de dados** a que se refere a infração pelo período máximo de **6 (seis) meses**, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

XI - **suspensão do exercício da atividade de tratamento dos dados pessoais** a que se refere a infração pelo período máximo de **6 (seis) meses**, prorrogável por igual período;

XII - **proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados**.

Tipos de penalidades

O §1º do art. 52 da LGPD prevê que as sanções serão aplicadas após procedimento administrativo que permita a ampla defesa, **de forma gradativa, isolada e ou cumulativa**, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

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

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

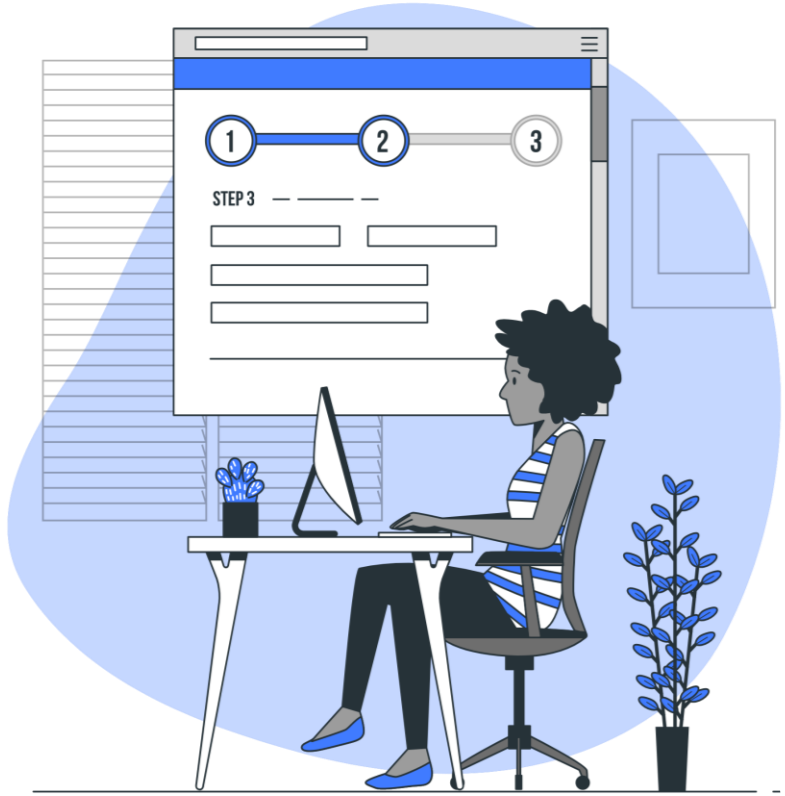
VII - a cooperação do infrator; a gravidade da falta e a intensidade da sanção.

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

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

X - a pronta adoção de medidas corretivas; e

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



Da segurança e das boas práticas

Os agentes de tratamento devem adotar **medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito (art. 46).

Da segurança e das boas práticas

Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança. (art. 50)

O controlador poderá implementar o programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

Mais informações sobre a LGPD

Política de Privacidade do Sidia: https://www.sidia.com/privacidade-e-protecao-de-dados-pessoais/

E-mail: dataprivacy@sidia.com