LGPD
Lei Geral de Proteção de Dados
Lei nº 13.709/2018

LGPD

E SEGURANÇA DA INFORMAÇÃO

safecomply

Aqui você terá acesso à **conteúdos atualizados sobre a LGPD**, além de informações relevantes sobre **Segurança da Informação** e sua aplicação no âmbito da Lei Geral de Proteção de Dados Pessoais.

1 - FUNDAMENTO E **PRINCÍPIOS DA LGPD**

O que é a LGPD – Lei Geral de Proteção de Dados Pessoais

· **Lei federal** nº 13.709 publicada em 14 de agosto de 2018;

· Versa sobre o **tratamento de dados pessoais** de pessoa física, não atingindo diretamente os dados de pessoas jurídicas;

· Regulamenta o uso e **estabelece regras sobre o tratamento de dados** pessoais no brasil;

· Objetivo de **proteger os direitos fundamentais** de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

safecomply

LINHA DO **TEMPO**

2010

• Consulta pública sobre anteprojeto de lei de proteção de dados pessoais

2011

• Sancionada a Lei de Acesso à Informação (dados pessoais de acesso público)

• Proposto o projeto de lei sobre o Marco Civil da Internet (direitos e deveres de usuários e provedores)

2012

• Proposto um projeto de lei na Câmara sobre o tratamento de dados pessoais

2013

• Proposto um projeto de lei no Senado sobre proteção, tratamento e uso de dados pessoais

2014

• Entra em vigor o Marco Civil da Internet

2016

• Aprovação da GDPR (Regulamento Geral de Proteção de Dados) na Europa

2018

• Entra em vigor a GDPR na Europa

• Sancionada a LGPD, após a unificação dos projetos de lei da Câmara e do Senado

2019

• Aprovada a criação da ANPD (Autoridade Nacional de Proteção de Dados)

• Iniciada a discussão sobre a inclusão da proteção de dados pessoais entre os direitos fundamentais do cidadão

2020

• Entra em vigor a LGPD

2021

• Entra em vigor as sanções administrativas previstas na LGPD

2022

• A ANPD regulamenta a LGPD para Agentes de Tratamento de Pequeno Porte

• O Congresso define a proteção de dados pessoais como garantia fundamental do cidadão

• A ANPD se torna uma autarquia, com autonomia em suas decisões

• Está em discussão a metodologia de cálculo para aplicação das multas previstas na LGPD

Fundamentos da LGPD

Estruturada em 10 capítulos, a LGPD abrange a proteção de dados pessoais de forma ampla, dispondo sobre as operações relacionadas ao tratamento de dados pessoais por qualquer atividade que envolva a sua utilização, independentemente do formato e do meio (do físico ao digital, online e offline), realizada por pessoa natural (o que podemos chamar de pessoa física) ou por pessoa jurídica de direito público ou privado, ou seja, abrange a maioria das atividades econômicas e sociais.

A LGPD apresenta sete fundamentos básicos, intimamente relacionados aos direitos fundamentais abarcados na Constituição Federal Brasileira de 1988. São eles:

· Respeito à **privacidade**
· **Inviolabilidade** da intimidade, da honra e da imagem
· **Tutela dos direitos humanos**, a dignidade, o exercício da cidadania e o livre desenvolvimento da personalidade do indivíduo.
· **Autodeterminação** informativa
· **Liberdade de expressão**, de informação, de comunicação e de opinião.
· Desenvolvimento **econômico e tecnológico**
· A inovação e a livre iniciativa, a livre concorrência e a **defesa do consumidor**

Princípios para o tratamento de dados pessoais

A LGPD apresenta onze princípios direcionadores das atividades relacionadas ao tratamento de dados procurando, assim, garantir um conjunto de instrumentos que proporcionem aos titulares dos dados mecanismos para a efetiva autodeterminação informativa e o controle do uso de sua informação por terceiros, assegurando os direitos fundamentais de liberdade e privacidade.

1- Princípio da boa-fé: notadamente conhecido uma vez que já faz parte do ordenamento jurídico brasileiro estando, inclusive, expressamente referido em outras importantes legislações, como o Código de Defesa do Consumidor, e o Código Civil brasileiro;

2- Princípio da finalidade: estabelece que quando da realização do tratamento de determinado dado pessoal este deverá atender a propósitos legítimos específicos, explícitos e antecipadamente informados ao titular, sem que exista a possibilidade de ser realizado qualquer tipo de tratamento posterior e/ou de forma incompatível com as finalidades informadas inicialmente a ele;

3- Princípio da adequação: necessidade de observância da compatibilidade do tratamento de dados com as finalidades doravante informadas ao titular, fomentando o resultado pretendido bem como suas expectativas quando do fornecimento do ativo;

4- Princípio da necessidade: determina que a coleta de dados deve se limitar a somente os dados necessários, pertinentes e indispensáveis para a realização da finalidade pretendida;

5- Princípio do livre acesso: concede a garantia de que os titulares de dados tenham acesso simples e facilitado, livre de ônus, sobre a forma e duração de tratamento de seus dados, além da checagem de sua integralidade, podendo obter cópia do que está armazenado, corrigindo informações incorretas ou solicitando a sua exclusão;

6- Princípio da qualidade dos dados: visa garantir aos titulares que os seus dados são armazenados e tratados com cuidado observando padrões, normas e boas práticas nacionais e internacionais de segurança;

7- Princípio da transparência: garante aos titulares de dados, de forma facilitada, clara e precisa o acesso às informações específicas sobre como se dá a realização do tratamento de seus dados, bem com quem são os agentes e os responsáveis por tais ações;

8- Princípio da segurança: prevê que o uso de dados deve ser realizado mediante a utilização de técnicas e estratégias que visem à proteção dos dados pessoais a acessos não autorizados, bem como a segurança relacionada a situações acidentais ou ilícitas de deleção, perda, modificação, roubo ou difusão;

9- Princípio da prevenção: requer que o responsável pelo tratamento adote medidas que visem prevenir a ocorrência de danos de qualquer ordem quando do uso dos dados pessoais.

10- Princípio da não discriminação: fixa a impossibilidade de realização do tratamento dos dados para fins abusivos, discriminatórios e ilícitos que possam mitigar direitos dos seus titulares.

11- Princípio da responsabilização e prestação de contas: determina que, quando da análise de incidentes no tratamento dos dados, o responsável deverá demostrar que adotou e adota medidas adequadas e eficazes para evitar o dano, observando e cumprindo as normas de proteção observando e cumprindo as normas de proteção.

2 - ENTENDENDO OS PRINCIPAIS CONCEITOS DA **LGPD E SEUS OPERADORES**

O que é tratamento de Dados Pessoais?

Amplo conjunto de operações que abrangem:

- Coleta
- Processamento
- Armazenamento
- Compartilhamento
- Exclusão

É um conjunto de ações que envolvem todo o **ciclo de vida do dado pessoal.**

Dado Pessoal

Toda a informação relativa à pessoa natural identificada ou identificável.
Exemplo: nome civil, registro geral, cadastro de pessoa física, endereço, (informação que pode ser considerada identificada) ou IP, dados de localização, dados de navegação, etc. (informação considerada identificável).

Dado Pessoal Sensível

Dado mais íntimo do seu titular, que pode relevar informações sobre sua origem racial ou étnica, sua convicção religiosa e política, suas informações sobre saúde e vida sexual, bem como seus dados biométricos e dados de identificação genética.

Dado Pessoal de Menores

Apesar de a LGPD não categorizar os dados de crianças e adolescentes como dados pessoais ou dados pessoais sensíveis, ela determinou que o tratamento de dados desses titulares só poderá ocorrer mediante **consentimento, específico e em destaque, de pelo menos um dos pais ou responsável legal.**

Mas quem é o Titular de Dados?

Como titular dos dados a Lei considerada toda a pessoal natural, mais conhecida como pessoa física, a quem se referem os dados pessoais que são objeto de tratamento.

Agentes de Tratamento

Outros atores centrais da LGPD são o **controlador, o operador e o encarregado**, chamados de "**agentes de tratamento**". Eles têm papel fundamental para garantir a dinâmica das relações envolvidas no cenário da proteção de dados.

O CONTROLADOR

Pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Em resumo, o controlador é quem irá **tomar todas as decisões relacionadas ao tratamento dos dados.**

O OPERADOR

O segundo agente de tratamento é chamado operador, conceituado como sendo pessoa natural ou jurídica, também de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, ou seja, é quem processa os dados pelo controlador e deverá fornecer garantias de que implementa as medidas técnicas adequadas dentro do modelo de tratamento de dados solicitado.

O ENCARREGADO

A LGPD também determina que qualquer organização que trate de dados pessoais deverá contar com um encarregado (DPO - Data Protection Officer)

O encarregado tem um papel importante e fundamental nas organizações, já que ele é a pessoa indicada pelo controlador para atuar como canal de comunicação entre ele, os titulares dos dados, e a Autoridade Nacional de Proteção de Dados (ANPD).

Responsável por acompanhar todas as etapas do ciclo de vida dos dados pessoais, como verificar se os agentes de tratamento estão em Compliance com a Lei, os aconselhando sobre melhores práticas de segurança da informação, monitorando a conformidade das operações, cooperando com as autoridades públicas, como a ANPD, gerenciando reclamações de titulares de dados e executando as diretrizes do controlador.

A ANPD - Autoridade Nacional de Proteção de Dados

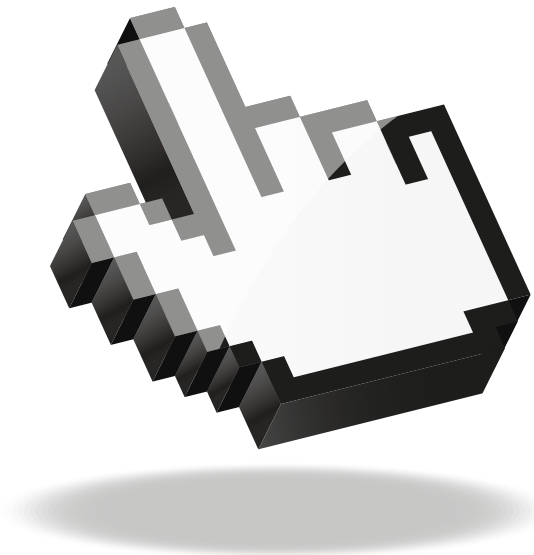
Autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública.
Papel central na adaptação da LGPD pela sociedade e pelo mercado.

COMPETÊNCIAS:

- Zelar pela proteção de dados;
- Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e Privacidade;
- Fiscalizar e aplicar sanções em caso de tratamento de dados inadequado;
- Receber denúncias e petições dos titulares de dados;
- Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade.

3 - HIPÓTESES DE TRATAMENTO DE DADOS ***PESSOAIS NA LGPD***

Existem **11 hipóteses, ou bases legais, de tratamento de dados pessoais na Lei**. São como condições necessárias para que o tratamento de dados seja permitido.



HIPÓTESE 1: Fornecimento de consentimento pelo titular

Hipótese em que o titular consente, ou seja, ele aceita espontaneamente que seu dado seja tratado para determinada finalidade. O consentimento deve ser livre, informado e destacado, não podendo ser genérico, sendo proibido o tratamento de dados pessoais mediante vício de consentimento.

No caso de tratamento de dados de **crianças e adolescentes deverá ser solicitado o consentimento**, específico, de pelo menos um dos pais ou responsável legal do titular do dado.

HIPÓTESE 2: Cumprimento de obrigação legal ou regulatória

Aplicável para os casos em que se faz necessário **processar os dados pessoais para cumprir alguma obrigação** legal ou regulatória específica.

HIPÓTESE 3: Execução de políticas públicas

Aplicável para o tratamento e uso compartilhado de dados pessoais que sejam **necessários para a execução de políticas públicas previstas** em leis e regulamentos. Só deve ser realizada por controladores que sejam pessoas jurídicas de direito público.

HIPÓTESE 4: Realização de estudos e pesquisas

Aplicável quando se faz necessária a **realização de estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais dos titulares.

HIPÓTESE 5: Execução de contrato

Aplicável para o tratamento de dados necessário à **execução de contrato ou de procedimentos preliminares** relacionados a contrato do qual seja parte o titular.

HIPÓTESE 6: Exercício de direitos em processo judicial, administrativo ou arbitral

Aplicável para o exercício regular de **direitos do titular seja em processo judicial, administrativo ou arbitral**, e abrange quaisquer das partes envolvidas.

HIPÓTESE 7: Proteção da vida ou da incolumidade física

Aplicável para o tratamento de dados quando da necessidade de **proteção da vida ou de perigo iminente** do titular ou de terceiros.

HIPÓTESE 8: Tutela da saúde

Aplicável para o tratamento de dados em função da **proteção da saúde** e exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

HIPÓTESE 9: Legítimo Interesse

Aplicável quando se pretende atender aos **interesses legítimos do controlador ou de terceiros**, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular, ou seja, o legítimo interesse precisa respeitar as legítimas expectativas do titular em relação ao tratamento de seus dados.

HIPÓTESE 10: Proteção do crédito

Aplicável para o tratamento de dados para **proteção do crédito do titular**.
Como exemplo desse tratamento temos o sistema de cadastro positivo.

HIPÓTESE 11: Prevenção à fraude e à segurança do titular

Aplicável para o tratamento de dados pessoais sensíveis quando necessário assegurar a identificação e autenticação do titular em **cadastros de sistemas eletrônicos**, visando à prevenção de fraudes e à garantia da segurança do titular.

4 - OS DIREITOS DO TITULAR DE DADOS PESSOAIS

A LGPD estabelece uma série de direitos aos titulares de dados que devem ser **garantidos pelas organizações**, de direito público ou privado, durante toda a existência do tratamento de dados pessoais.

Confirmação da existência de tratamento

Direito de confirmar se a organização possui seus dados e se realiza algum tipo de tratamento com eles. Essa confirmação pode ser dada de imediato em formato simplificado ou por meio de declaração completa que indique origem dos dados, existência de registro, critérios utilizados para captação e finalidade do tratamento.

Acesso aos dados

O titular poderá solicitar à organização informações e cópia de seus dados e a forma como são tratados.

- Consulta deve ser facilitada e gratuita
- Prazo: 15 dias.

Correção de dados incompletos, inexatos ou desatualizados

O titular de dados pode solicitar que seus dados sejam completados, corrigidos e atualizados.

Anonimização, bloqueio ou eliminação de dados desnecessários

Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

Titular pode solicitar que sejam excluídos dados desnecessários, excessivos ou tratados em desconformidade com LGPD.

Informações sobre o uso compartilhado de dados

Direito de ser informado se existe compartilhamento de seus dados com entidades públicas ou privadas, independente de solicitar ou não essa informação.

Portabilidade dos dados a outro fornecedor de serviço ou produto

Direito de solicitar a portabilidade de seus dados, em um formato estruturado e interoperável.

Revogação do consentimento

- Direito de revogar o seu consentimento, pedindo inclusive a eliminação dos dados;
- Quando obrigatória a guarda, o controlador não poderá mais usar os dados para aquelas hipóteses em que o titular deu consentimento.

Se opor ao consentimento, se irregular

• Direito de ser informado de que não é obrigatório o seu consentimento;
• Informações sobre os efeitos negativos da não concessão.

Peticionar em relação aos seus dados contra o controlador perante a ANPD

• Fazer reclamação de qualquer organização junto a ANPD
• Requerimento expresso
• Sem custo.

Direito de revisão das decisões automatizadas e explicação

• Decisões automatizadas por sistema de algoritmo;
• Direito a obter informações sobre os critérios e procedimentos empregados no processo de decisão;
• Direito a solicitar a revisão dessas decisões.

5 - SEGURANÇA DA INFORMAÇÃO E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A segurança da informação tem como objetivos garantir a confidencialidade, integridade e disponibilidade dos dados, por meio do uso de tecnologia, processos e pessoas, detectando, prevenindo e respondendo às ameaças digitais.

Estes objetivos são alcançados através da **implementação de um conjunto adequado de controles**, incluindo políticas, processos, procedimentos, estrutura organizacional, além da utilização de softwares e hardwares adequados.

Os controles precisam ser **estabelecidos, implementados, monitorados, analisados criticamente e melhorados** periodicamente, para assegurar a segurança da informação da organização e a continuidade do negócio.

A organização precisa tomar medidas que contemplem pessoas, processos e tecnologia, levando em consideração:

· A parte tecnológica;
· A governança;
· A conformidade documental (adequação jurídica de termos, contratos e políticas de privacidade e de proteção de dados); e
· A conscientização.

O capítulo 7 da LGPD trata "Da Segurança e Boas Práticas" e foi dividido em 2 seções:

· **Seção I** - Da Segurança e do Sigilo de Dados (Art. 46 a 49)
· **Seção II** - Das Boas Práticas e da Governança (Art. 50 a 51)

O que as organizações devem fazer?

A LGPD diz que, além das medidas de segurança técnicas, também é necessário adotar medidas administrativas para proteger os dados pessoais, e que estas medidas devem ser observadas desde a concepção até a execução dos serviços.

Alguns exemplos de medidas administrativas:

· Definição de políticas e procedimentos;
· Treinamentos e capacitações;
· Assinatura de contratos e acordos; e
· Aplicação de sanções para infrações cometidas;

As questões tecnológicas também possuem papel importante no processo de adequação. Portanto, é necessário que as organizações verifiquem se os sistemas que elas utilizam atendem a estes requisitos e que, além disso, cobrem dos fornecedores que tratam dados pessoais, que eles também sigam estas medidas.

Qualquer um que participe do tratamento dos dados está obrigado a garantir a segurança da informação prevista na LGPD. Isto significa que além dos colaboradores da organização, os estagiários, terceirizados e fornecedores que tratam dados pessoais também estão obrigados a respeitar a Lei.

O que as organizações devem comunicar?

As organizações devem a comunicar as ocorrências de incidentes de segurança que possam acarretar riscos ou danos relevantes aos titulares. Esta comunicação deve ser realizada em um prazo razoável e deve conter, no mínimo, as seguintes informações:

1 - Descrição da natureza dos dados afetados;
2 - Informação sobre os titulares envolvidos;
3 - As medidas utilizadas para a proteção dos dados;
4 - Os riscos relacionados ao incidente;
5 - Os motivos pela não comunicação imediata;
6 - As medidas utilizadas para reverter ou diminuir os efeitos do prejuízo.

Como manter a adequação à LGPD?

A melhor maneira das organizações se manterem adequadas à LGPD é implementando um Programa de Governança em Privacidade que englobe:

- O inventário de dados pessoais;
- Os envolvidos no tratamento dos dados pessoais;
- Os riscos relacionados ao tratamento de dados pessoais;
- Os controles implementados para tratar estes riscos; e
- Evidências da eficiência dos controles implementados.

OS REQUISITOS MÍNIMOS PARA ESTE PROGRAMA DE GOVERNANÇA EM PRIVACIDADE SÃO:

1 - Demonstrar o comprometimento do controlador em cumprir normas e boas práticas relativas à proteção de dados pessoais;
2 - Ser aplicado a todo o conjunto de dados pessoais que estejam sob seu controle;
3 - Ser adaptável à estrutura, à escala e ao volume das operações da organização;
4 - Estabelecer políticas e salvaguardas adequadas com base na avaliação sistemática de riscos;
5 - Ter o objetivo de estabelecer relação de confiança com o titular;
6 - Estar integrado à estrutura geral de governança e possuir mecanismos de supervisão internos e externos;
7 - Conter planos de resposta a incidentes e remediação; e
8 - Ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

Se você chegou até aqui, é porque entende a **importância da LGPD** e está comprometido em **garantir a privacidade** dos dados da sua organização.

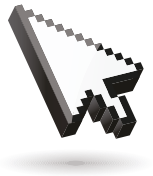
Mas você sabe em que nível de adequação ela esta?

Não deixe essa dúvida te preocupar!

Com alguns cliques e em poucos minutos, você terá em mãos um **relatório sobre a sua situação atual**, além de receber sugestões para **melhorar seu nível de adequação**.

Clique no link abaixo ou aponte a câmera do seu celular para o **QRcode** e acesse a **Calculadora Inteligente SafeComply**!

calculadora.safecomply.com.br



safecomply