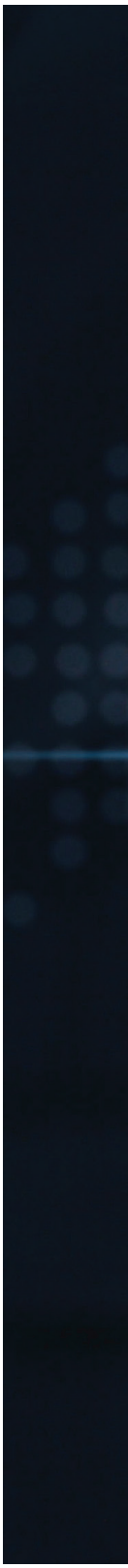
GUIA LGPD

Lei Geral de Proteção de Dados SIMPLIFICADA

ÍNDICE



1

LGPD

DEFINIÇÕES IMPORTANTES SOBRE LGPD

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD), Lei 13.709/2018, tem como objetivo regulamentar o tratamento de dados pessoais pelas empresas, uma vez que os dados pessoais ganharam grande importância na economia moderna, pois permitem fazer predições, analisar perfis de consumo, opinião, entre outras atividades.

HOJE, MAIS DE 126 PAÍSES NO MUNDO possuem leis para a proteção de dados pessoais visando à regulamentação do tratamento de dados das empresas, evitando-se o mau uso destes, bem como a responsabilização das empresas por isso, bem como por incidentes e acidentes com dados pessoais.

A LGPD tem como objetivos:

- Proteção à privacidade;
- Liberdade de expressão, informação, comunicação e opinião;
- Inviolabilidade da intimidade, honra e da imagem;
- Desenvolvimento econômico, tecnológico e inovação;
- Livre iniciativa, livre concorrência e a defesa do consumidor;
- Direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania.

A LGPD se aplica:

- Aos dados pessoais de indivíduos localizados no Brasil;
- Quando o tratamento se dá no Brasil;
- Quando houver oferta de bens e serviços para indivíduos no Brasil.

A LGPD não se aplica:

- Para dados provenientes e destinados a outros países, que apenas transitem pelo território nacional;
- Uso pessoal;
- Uso não comercial;
- Fins jornalísticos;
- Acadêmicos;
- Segurança pública.

2

LGPD

DADOS PESSOAIS

O QUE SÃO DADOS PESSOAIS?

Dados Pessoais (art. 5º, I) são os dados que permitem identificar uma pessoa ou torná-la identificável. São exemplos de dados pessoais:

- Nome
- Endereço
- Números Únicos Identificáveis (RG, CPF, CNH)
- Geolocalização
- Hábitos de Consumo
- Exames Médicos
- Dados referentes à saúde
- Biometria
- Perfil Cultural

Uma subcategoria de dados pessoais é denominada de **dados pessoais sensíveis (art. 5º, II)**, que por sua relevância e importância demandam mais proteção do um dado pessoal comum. São estes: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Outro conceito é **dado anonimizado:** dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Assim, a anonimização é entendida como a 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.

O **titular dos dados pessoais** é toda pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

O QUE É TRATAMENTO DE DADOS PESSOAIS?

Trata-se de toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

3

LGPD

AGENTES DE TRATAMENTO

SEGUNDO A LEI, SÃO O CONTROLADOR E O OPERADOR DOS DADOS PESSOAIS. O **controlador** é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Já o **operador** é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador

EM CASO DE ATO CONTRÁRIO AOS TERMOS DA LGPD, tanto o operador como o controlador podem responder diretamente, de forma subjetiva, e solidária com a empresa para quem atuam sobre o incidente de **dados** pessoais.

A Lei também prevê a criação do cargo de **encarregado ou DPO** – ***Data Protection Officer***, o qual poderá ser pessoa física ou jurídica, cujas atividades serão aceitar reclamações, prestar esclarecimentos aos titulares e às autoridades, orientar as respectivas empresas e executar as diretrizes do diretor. O DPO terá sua identidade disponibilizada aos titulares e autoridades e seu contato deverá ser disponibilizado de forma simples e de fácil acesso.

DOCUMENTOS ESSENCIAIS QUE AS EMPRESAS DEVEM PROVIDENCIAR PARA ESTAR EM CONFORMIDADE COM A LGPD:

Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais (Ciclo dos Dados) que podem gerar riscos (Risk Assessment) às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco, tais como mapeamentos, treinamentos, auditorias, alterações de contrato e criação de políticas de proteção de dados.

4

LGPD

PRINCÍPIOS DA LGPD

PRIVACY BY DESIGN (PRIVACIDADE DESDE A CONCEPÇÃO)

Este princípio de governança previsto no art. 46 da LGPD determina que todas as empresas devem incorporar a privacidade a todos os estágios (modelagem, operação e gerenciamento e encerramento) de um determinado sistema, projeto ou negócio.

Outros princípios da LGPD são os seguintes:

FINALIDADE:

O tratamento precisa ter um resultado único, específico e legítimo que deve ser alcançado com tal tratamento;

NECESSIDADE:

Devem ser tratados apenas os dados pessoais necessários para aquela finalidade descrita, dispensando-se os excessivos ou desnecessários;

ADEQUAÇÃO:

Tem como objetivo evitar a desvirtuação das finalidades informadas com o real tratamento dispensado;

LIVRE ACESSO:

O titular dos dados deve ter livre acesso aos seus dados pessoais tratados de forma grátis e ágil;

QUALIDADE DE DADOS:

Os agentes de tratamento devem garantir aos titulares de dados a exatidão, clareza, relevância e atualização dos dados, sempre em conformidade com a necessidade e finalidade do tratamento;

TRANSPARÊNCIA:

Deve-se garantir sempre informações claras, precisas e acessíveis aos titulares com relação ao tratamento de seus dados pessoais, inclusive sobre os agentes de tratamento;

SEGURANÇA:

Os agentes de tratamento deverão sempre buscar utilizar medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de incidentes que levem à quebra da integridade dos dados (perda, alteração, difusão, etc.)

PREVENÇÃO:

Os agentes de tratamento devem adotar medidas preventivas contra a ocorrência de incidentes sobre os dados pessoais;

NÃO DISCRIMINAÇÃO:

É vedado tratar os dados para fins discriminatórios ilícitos ou abusivos;

RESPONSABILIDADE E PRESTAÇÃO DE CONTAS *(ACCOUNTABILITY)*

Impõe que os agentes de tratamento deverão demonstrar a adoção de medidas eficazes e capazes de comprovar a observância do cumprimento das normas de proteção de dados pessoais, inclusive as de segurança da informação, demonstrando a sua eficácia.

5

LGPD

BASES LEGAIS PARA O TRATAMENTO DE DADOS

Para cada finalidade, o tratamento de dados deve estar justificado em uma das bases legais previstas no art. 7º da LGPD:

- **CONSENTIMENTO PELO TITULAR** – meio pelo qual o titular de dados pessoais tem para determinar o nível de proteção e garantir a extensão do fluxo dos seus dados, dando a sua anuência expressa (art. 8º) para as finalidades descritas nos termos de consentimento;

- **CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA PELO CONTROLADOR** – quando o tratamento é necessário para atender o interesse público, justificado pela obrigação legal ou regulatória. Não depende de consentimento do titular. Exemplos: coleta de dados para emitir uma nota fiscal; tratamento de dados pessoais do empregado para à Caixa Econômica Federal em razão da obrigação do FGTS;

- **EXECUÇÃO DE POLÍTICAS PÚBLICAS** – o tratamento de dados é previsto para execução de políticas públicas tais como vacinação, epidemia, verificação de qualidade de ensino;

- **ESTUDOS POR ÓRGÃO DE PESQUISA** – tratamento de dados para fins de pesquisa, sendo que, sempre que possível, se deve proceder com a anonimização dos dados pessoais. Exemplo: Censo;

- **EXECUÇÃO DE CONTRATO** – o tratamento de dados é lícito quando necessário para a execução de um contrato no qual o titular dos dados é parte ou para procedimentos preliminares a sua formação;

- **EXERCÍCIO REGULAR DE DIREITOS EM PROCESSO JUDICIAL, ARBITRAL OU ADMINISTRATIVO –** o tratamento de dados no curso do processo é base legal para a produção de provas e uso para o devido processo legal.

- **PARA A PROTEÇÃO DA VIDA OU DA INTEGRIDADE FÍSICA** – os dados podem ser tratados para a proteção da vida ou integridade física pelos agentes de saúde (médicos, enfermeiros, agentes sanitários)

- **PARA A TUTELA DA SAÚDE** – Os dados tratados em âmbito da saúde devem servir para garantir a qualidade de vida da sociedade e a redução d riscos ao adoecimento.

- **LEGÍTIMO INTERESSE** – configurado nas situações em que se tem uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, na qual a finalidade do tratamento é tida como razoavelmente esperada pelo titular do tratamento, sem que lhe cause prejuízos, devendo, sempre, ser avaliada no caso concreto por meio de um teste de legítimo interesse.

- **PARA A PROTEÇÃO DO CRÉDITO** – os dados pessoais podem ser tratados para proteção ao crédito de forma a tornar a economia do país mais segura e conceder mais benefícios a quem cumpre com suas obrigações.

6

LGPD

DIREITOS DO TITULAR

DIREITOS DO TITULAR (ART. 18)

- Confirmar existência de tratamento de seus dados pessoais;
- Acessar seus dados pessoais;
- Corrigir os dados pessoais;
- Anonimizar, bloquear ou eliminar dados pessoais;
- Portabilidade de dados pessoais;
- Obter informações sobre o compartilhamento de dados pessoais;
- Revogar o consentimento dado.

TRATAMENTO IRREGULAR

ART. 44º: O QUE É? QUEM RESPONDE?

Considera-se tratamento irregular quando deixar de observar a legislação ou quando não fornecer segurança necessária.
Responde pelos danos decorrentes da violação da segurança dos dados a empresa junto com o controlador ou o operador, mesmo após o fim do tratamento.

8

LGPD

GOVERNANÇA

As empresas devem documentar procedimentos entre o controlador e o operador para facilitar a demonstração dos procedimentos à Autoridade Nacional de Proteção de Dados (ANPD). Ademais, as empresas devem promover ações educativas e treinamentos aos seus membros e colaboradores visando à mitigação de riscos e a devida informação aos titulares de dados.

INCIDENTE DE SEGURANÇA

INCIDENTE DE SEGURANÇA (ART. 48)

Quando houver um incidente de segurança que acarrete risco ou dano relevante aos titulares, caberá à empresa tomar as seguintes providências:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos;
- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata;
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

10

LGPD

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Órgão de natureza federal vinculada à Presidência da República nos primeiros dois anos de sua implementação, com funções de natureza normativo-interpretativa, fiscalizatória e integrativa e com competência para:

- Editar normas e procedimento sobre a proteção de dados pessoais;
- Requisitar informações, a qualquer momento, aos controladores e operadores de dados pessoais que realizem operações de tratamento de dados pessoais;
- Fiscalizar e aplicar sanções na hipótese de tratamento de dados em descumprimento com a legislação mediante processo administrativo que assegure o contraditório e ampla defesa;
- Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países;
- Editar normas e procedimentos diferenciados de modo a facilitar a adequação à LGPD para as empresas de pequeno porte e microempresas.

A ANPD será composta por um Conselho Diretor (5 membros) indicados pelo Conselho Nacional de Proteção de Dados e Privacidade, composto por 23 membros (art. 58); por uma Corregedoria e uma Ouvidoria. Possuirá, também, órgão de aconselhamento jurídico próprio, podendo servir como órgão consultivo para as empresas adotarem as melhores práticas de cumprimento à lei e prevê unidades administrativas específicas.

SANÇÕES

A ANPD poderá aplicar as seguintes sanções sobre incidentes de dados:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples, de até 2% 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;
- Multa diária, observado o limite total a que se refere o inciso II;
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência.

As empresas deverão atuar diretamente junto aos titulares dos dados quando houver um incidente de vazamento de dados, pois o § 7º do art. 52 prevê que a conciliação direta entre controlador e titular para reparação e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo.

11

LGPD

APLICAÇÃO DO CÓDIGO DE DEFESA DO CONSUMIDOR

A LGPD está contida dentro do Sistema Nacional de Defesa do Consumidor (art. 45) e por tal razão, os direitos dos titulares dos dados, tratados como consumidores by standard, lhes são garantidos tais como: a presunção de hipossuficiência; a inversão do ônus da prova, o direito à informação e explicação entre outros.

No entanto, a LGPD também poderá ser aplicada em outros contextos jurídicos como nas relações de trabalho.

11 PASSOS PARA IMPLANTAR A LGPD NA SUA EMPRESA

1. Estudo da LGPD e demais leis que regulamentam o seu negócio
2. Mapear a entrada e o tratamento dos dados pessoais
3. Mapear os riscos do tratamento
4. Elaborar o Relatório de Impacto
5. Criar a política de proteção de dados e adaptar os documentos internos e externos
6. Gerenciar os pedidos dos titulares e dos órgãos
7. Treinamento das equipes que tratam dados pessoais
8. Ser compliance com a proteção de dados mediante governança
9. Exigir o compliance da proteção de dados de seus fornecedores
10. Concepção de novos produtos com o princípio de privacy by design
11. Eleger um DPO com conhecimentos regulatórios sobre proteção de dados