

## LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – 13.709/18

### INTRODUÇÃO

Com a aprovação em 2018 da **Lei Geral de Proteção de Dados Brasileira**, fica ainda mais evidente a urgência do assunto e necessidade de atenção das empresas como um todo para o tratamento de dados pessoais coletados no dia a dia.

Após mais de oito anos de debates foi sancionada, em 14 de agosto de 2018, a Lei Geral de Proteção de Dados brasileira (LGPD – Lei 13.709/18). **O prazo para adequação se encerra em agosto de 2020.**

A LGPD tem aplicação a qualquer pessoa, seja natural ou jurídica de direito público ou privado que realize o tratamento de dados pessoais, *online e/ou offline*. Assim, podemos inferir que a Lei possui aplicação ampla e abrangente, que abarca grande parte de projetos e atividades do cotidiano empresarial.

ALGPD dispõe sobre 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, estabelecendo regras e limites para empresas a respeito da coleta, armazenamento, tratamento e compartilhamento de dados.

Em linhas gerais, os Titulares dos dados passarão a ter total controle sobre todo o processamento dos seus dados pessoais, do que decorrem diversas obrigações para os controladores (a quem competem as decisões sobre o tratamento dos dados) e operadores (aqueles que tratam os dados de acordo com o estipulado pelos controladores).

Um dos princípios mais relevantes é o da finalidade, por meio do qual os dados deverão ser utilizados apenas para as **finalidades específicas para as quais foram coletados** e devidamente informados aos titulares, juntamente com o princípio da minimização da coleta, isto é, somente devem ser coletados os dados mínimos necessários para que se possa atingir a finalidade, e o da retenção mínima, o qual determina a **imediate exclusão dos dados, após atingida a finalidade pela qual eles foram coletados**.

### MOTIVOS PARA SE PREOCUPAR COM O TEMA E A LEI

Empresas de todos os setores e de todos os portes tratam dados pessoais. **A Lei vale para todas elas;**

Todos os departamentos das empresas usualmente tratam dados pessoais: RH; Logística; Marketing; Análise de Dados; Desenvolvimento de Software e TI; Jurídico; Compliance, apenas para citar alguns exemplos;

O tratamento de dados pessoais somente poderá ser realizado se estiver em conformidade com uma das bases legais previstas na Lei;

A Lei apresenta relevantes princípios para nortear o tratamento de dados pessoais, como finalidade (propósitos legítimos), adequação (compatibilidade), necessidade (mínima coleta) e transparência;

Os titulares de dados pessoais passam a ter os seguintes direitos (OnLine):

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização;
- Portabilidade;
- Eliminação;
- Informação a respeito do compartilhamento de dados;
- Possibilidade de receber informação sobre não fornecer o consentimento;
- Revogação do consentimento.

Empresas precisarão adotar medidas de segurança, governança e boas práticas;

Empresas deverão contar com a figura do Encarregado (responsável internamente por orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais bem como por orientar e avaliar o cumprimento da Lei);

A MP nº 869/18 criou uma Autoridade Nacional de Proteção de Dados para fiscalizar o cumprimento da Lei e aplicar sanções em caso de violação;

A multa pelo descumprimento da lei pode chegar a **R\$50 MILHÕES**.

## CONCEITOS RELEVANTES

### O QUE SÃO DADOS PESSOAIS?

**Dado Pessoal** (art. 5º, I): segundo a Lei, dado pessoal é informação relacionada à pessoa natural identificada ou identificável.

Assim, a LGPD traz um conceito amplo e aberto, pois qualquer dado, que isoladamente (dado pessoal direto) ou agregado a outro (dado pessoal indireto) possa permitir a **identificação** de uma pessoa natural, pode ser considerado como dado pessoal.

Exemplos: dados cadastrais, telefones, data de nascimento, profissão, dados de GPS, identificadores eletrônicos, nacionalidade, gostos, interesses e hábitos de consumo, entre outros.

**Dado Pessoal Sensível** (Art. 5º, II): dado pessoal sensível é o dado pessoal que versa sobre:

- Origem racial ou étnica;
- Convicção religiosa; ou 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. São aqueles dados relacionados a pessoa natural identificada ou identificável por meio dos quais **uma pessoa pode ser discriminada** e, por tal motivo, devem ser considerados e tratados como dados sensíveis.

### O QUE NÃO É DADO PESSOAL?

Dados anonimizados ou que passam por processo de anonimização não são dados pessoais (art. 5º, III e XI): o dado anonimizado é relativo ao titular que não possa ser identificável.

### O QUE A LEI CONSIDERA COMO TRATAMENTO DE DADOS?

Tratamento (art. 5º, X): toda operação realizada com dados pessoais, como as que se referem à **coleta**, produção, recepção, classificação, **utilização**, **acesso**, reprodução, transmissão, **distribuição**, **processamento**, arquivamento, armazenamento, eliminação, **avaliação** ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Para se tratar dados pessoais, o que inclui a prática da coleta e todas as demais citadas pelo dispositivo legal como a recepção, classificação, arquivamento e transferência, sempre é necessário ter um fundamento legal. Nesse ponto, mostra-se importante observar que o **CONSENTIMENTO** se torna uma das melhores hipóteses legais para o tratamento de dados.

## TERMOS RELEVANTES

**Titular** (art. 5º, V): pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

**Controlador** (art. 5º, VI): pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

**Operador** (art. 5º, VII): pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

**Agentes de tratamento** (art. 5º, IX): o controlador e o operador. Pela MP nº 869/18 o encarregado, também conhecido como *Data Protection Officer* (“**DPO**”), **não precisa mais ser uma pessoa natural**, abrindo espaço, desta forma, para a possibilidade de indicação de pessoas jurídicas, comitês, ou grupos de trabalho, que podem exercer tais funções. Ainda, deixa clara a **possibilidade de terceirização de tal serviço**.

## PRINCÍPIOS GERAIS DA PROTEÇÃO DE DADOS PESSOAIS

A LGPD lista 10 princípios que devem ser levados em consideração no tratamento de dados pessoais:

**FINALIDADE:** tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

**ADEQUAÇÃO:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

**NECESSIDADE:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

**LIVRE ACESSO:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais;

**QUALIDADE DOS DADOS:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados;

**TRANSPARÊNCIA:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;

**SEGURANÇA:** utilização de 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;

**PREVENÇÃO:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

**NÃO DISCRIMINAÇÃO:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

**RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

## BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

As empresas deverão comprovar ao menos uma das seguintes bases legais para realizar o tratamento dados pessoais (art. 7º):

- **Consentimento pelo titular:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- Cumprimento de obrigação legal ou regulatória pelo controlador;
- Pela administração pública,
- Para a realização de estudos por órgão de pesquisa;
- **Para a execução de contrato** ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular;
- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- Quando necessário para atender aos interesses legítimos do controlador ou de terceiro,
- Para a proteção do crédito.

Quando os dados forem sensíveis, o tratamento somente poderá ocorrer nas seguintes hipóteses (art. 11):

- **Consentimento pelo titular**, de forma específica e destacada, para finalidades específicas;
- Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
- Cumprimento de obrigação legal ou regulatória pelo controlador;
- Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas;
- Realização de estudos por órgão de pesquisa;
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- Proteção da vida ou da incolumidade física do titular ou de terceiro;
- Tutela da saúde.

## QUAIS SÃO AS SANÇÕES PREVISTAS NA LEI?

A LGPD implementa a aplicação de **severas sanções** para empresas que descumprirem as disposições legais e por tal motivo, mostra-se relevante a adequação das empresas ao disposto na Lei. Ademais, observa-se que a **Autoridade Nacional de Proteção de Dados**, dentre outros elementos, deverá observar no caso de aplicação de uma sanção não somente o grau do dado proporcionado, mas também as medidas, mecanismos e procedimentos internos adotados previamente pela empresa, o que demonstra a clara necessidade de adequação e implementação de boas práticas de governança, segurança e prevenção.

## COMO SE ADEQUAR À LEI?

A LGPD entrará em vigor em 08/2020. A estimativa para adequação completa nas empresas pode variar, normalmente, de **4 (quatro) a 14 (quatorze) meses**, de acordo com, entre outros, os seguintes critérios:

- O nível de maturidade da empresa no assunto;
- As regras e procedimentos já existentes;
- A quantidade de áreas e projetos que tratam dados pessoais;

- O nível de sensibilidade dos referidos dados objeto do tratamento;
- O orçamento previsto para a adequação.

Assim, visando a adequação da legislação em referência, sugerimos a **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA** a fim de:

- (I) Buscar o envolvimento dos executivos desde o início do plano de adequação para que a proteção de dados pessoais esteja incorporada aos valores da empresa e assim o tema ganhe o engajamento e a força necessária;
- (II) Estabelecer as ações e um líder para o plano, identificando os principais projetos e áreas da empresa afetadas pela LGPD e eventuais legislações setoriais;
- (III) Criar um programa de governança em proteção de dados com a elaboração de medidas e controles para o acompanhamento da implantação de padrões que estejam em conformidade com a LGPD e legislações setoriais aplicáveis;
- (IV) Estruturar a área com a indicação (ou contratação) do **Encarregado da Proteção de Dados (DPO)**;
- (V) Elaborar e rever documentos jurídicos com a realização de eventuais adendos aos contratos existentes para adequação aos padrões de proteção de dados, principalmente para aqueles que envolvam o tratamento e compartilhamento de dados pessoais;
- (VI) Garantir o exercício dos direitos dos titulares, mediante a confirmação da implementação de medidas técnicas e organizacionais;
- (VII) Realizar treinamentos internos para apresentação das novas políticas de proteção de dados pessoais e disseminação da cultura empresarial sobre o tema.