FIESP DEPARTAMENTO DE DEFESA E SEGURANÇA

# LGPD

## LEI GERAL DE PROTEÇÃO DE DADOS

FIESP CIESP

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 da sociedade como um todo para o tratamento de dados pessoais coletados no dia a dia.

Com a intenção de apoiar as Empresas no período de adequação à nova lei, a Federação das Indústrias do Estado de São Paulo, FIESP, e o Centro das Indústrias do Estado de São Paulo, CIESP, elaboraram a **Cartilha de Proteção de Dados Pessoais**.

Desde 2015, com a criação de grupos de trabalho dedicados e através de Congressos e Seminários, a FIESP e o CIESP se debruçam sobre o tema da Segurança e Defesa Cibernética e promovem conhecimento para toda a sociedade.

De forma objetiva e simplificada, a Cartilha apresenta as principais informações sobre a nova Lei Geral de Proteção de Dados para que as empresas possam avaliar os riscos futuros de sua forma de atuação e planejar mudanças e adequação.

FIESP CIESP

# CARTILHA DE PROTEÇÃO DE DADOS PESSOAIS – FIESP

## INTRODUÇÃO

Após mais de oito anos de debates, com base no *General Data Protection Regulation (GDPR)*, Regulamento de Proteção de dados da União Europeia, 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 16 de fevereiro 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.

A Lei também tem aplicação extraterritorial, ou seja, às empresas que (i) não só tenham estabelecimento no Brasil; mas também (ii) ofereçam serviços ao mercado consumidor brasileiro; ou (iii) coletem e tratem dados de pessoas localizadas no país.

Com a LGPD o Brasil se insere em um seleto e importante grupo de países que contam com um nível elevado de legislação em termos de proteção de dados pessoais, superando o atual estágio de tratamento setorial.

Referida Lei é importante para o Brasil em razão da harmonização e atualização de conceitos, gerando maior segurança jurídica; atração de

investimentos do exterior, diante do nível de proteção legal que agora contamos; assim como, do fomento cultural em proteção de dados pessoais.

A LGPD  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, o que favorece o desenvolvimento econômico.

Em linhas gerais, os titulares de dados passarão a ter maior controle sobre todo o processamento dos seus dados pessoais, do que decorrem diversas obrigações para 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 informadas 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 **imediata exclusão dos dados, após atingida a finalidade pela qual eles foram coletados**.

Assim, a LGPD trará mais segurança jurídica para empresas e maior proteção aos direitos dos titulares dos dados, sendo crucial entender os conceitos relevantes desta nova norma para compreensão dos seus impactos na prática.

## A) 10 MOTIVOS PARA SE PREOCUPAR COM O TEMA E A LEI

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

2. 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;

3. A utilização de dados pessoais pelas empresas de todos os portes é crucial para o desenvolvimento econômico e tecnológico; a inovação; a livre iniciativa; e a livre concorrência;

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

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

6. Os titulares de dados pessoais passam a ter os seguintes direitos: i) confirmação da existência de tratamento; (ii) acesso aos dados; (iii) correção de dados incompletos, inexatos ou desatualizados; (iv) anonimização; (v) portabilidade; (vi) eliminação; (vii) informação a respeito do compartilhamento de dados; (viii) possibilidade de receber informação sobre não fornecer o consentimento e suas consequências; (ix) revogação do consentimento;

7. Empresas devem adotar medidas de segurança, governança e boas práticas;

8. 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;

9. Será criada uma Autoridade Nacional de Proteção de Dados para fiscalizar o cumprimento da Lei e aplicar sanções em caso de violação;

10. A multa pelo descumprimento da lei pode chegar a R$50 MILHÕES de reais.

## B) CONCEITOS RELEVANTES PARA COMPREENDER A LGPD

### O QUE SÃO DADOS PESSOAIS?

Um dos mais relevantes ativos para o exercício de qualquer atividade empresarial, pessoal ou social, assim como para a concretização de políticas públicas, não há dúvida sobre a importância do tratamento do dado pessoal para o desenvolvimento econômico global.

Dados pessoais (art. 5º, I): segundo a Lei, dado pessoal é informação relacionada a 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, 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 verse sobre (i) origem racial ou étnica; (ii) convicção religiosa; (iii) opinião política; (iv) **filiação a sindicato** ou a organização de caráter religioso, filosófico ou político; (v) dado referente à saúde ou à vida sexual; (vi) **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 identificado**, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Já a anonimização é 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 uso de dados anonimizados se mostra primordial para possibilitar o desenvolvimento e aprimoramento de novas tecnologias, como a Internet das Coisas e a Inteligência Artificial, porém a dificuldade é enorme de se comprovar que meios técnicos razoáveis e disponíveis na ocasião do tratamento não possam levar a identificação do titular.

A Lei também não atinge diretamente documentos confidenciais, segredos de negócios, fórmulas, algoritmos, direitos autorais ou propriedade industrial, que são protegidos por outras normas, mas somente eventuais dados pessoais que estejam dentro de tal tipo de conteúdo.

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

Assim como o conceito amplo a respeito dos dados pessoais, a LGPD apresenta um conceito aberto e um rol exemplificativo das ações que são consideradas como tratamento de dados pessoais.

Tratamento (art. 5º, X): 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.

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 fundamental legal. Nesse ponto, mostra-se importante observar que o consentimento se torna uma das 10 (dez) hipóteses legais para o tratamento de dados, conforme veremos a seguir.

**OUTROS CONCEITOS 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.

Eliminação (art. 5º, XIV): exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Relatório de impacto à proteção de dados pessoais (art. 5º, XVII): documentação do controlador que deve conter a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de prevenção e mitigação de risco.

## C) PRINCÍPIOS GERAIS DA PROTEÇÃO DE DADOS PESSOAIS

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

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

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

**III** - 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;

**IV** - 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;

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

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

**VII** - 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;

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

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

**X** - 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.

## D) QUAIS SÃO AS 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):**

**I** - consentimento pelo titular: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

**II** - cumprimento de obrigação legal ou regulatória pelo controlador;

**III** - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas;

**IV** - para a realização de estudos por órgão de pesquisa;

**V** - para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular;

**VI** - para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

**VII** - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

**VIII** - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

**IX** - quando necessário para atender aos interesses legítimos do controlador

ou de terceiro, consideradas a partir de situações concretas, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

**X** - para a proteção do crédito.

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

**I** – consentimento pelo titular, de forma específica e destacada, para finalidades específicas;

**II** - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

**a)** cumprimento de obrigação legal ou regulatória pelo controlador;

**b)** tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

**c)** realização de estudos por órgão de pesquisa;

**d)** exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

**e)** proteção da vida ou da incolumidade física do titular ou de terceiro;

**f)** tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou

**g)** garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

## E) SEGURANÇA DE DADOS PESSOAIS, GOVERNANÇA E BOAS PRÁTICAS

A LGPD apresenta a segurança, prevenção e a adoção de medidas para o estabelecimento de boas práticas e governança no tratamento de dados pessoais como pilares, sendo relevante observar que a Autoridade Nacional de Proteção de Dados poderá dispor sobre os padrões técnicos mínimos para tornar aplicável os padrões de segurança e governança, em especial para o tratamento de dados pessoais sensíveis.

Segurança (art. 46): as empresas 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

Boas práticas e Governança (art. 50): as empresas poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Encarregado ou *Data Protection Officer*: pessoal natural indicada pelo controlador, será o responsável dentro da empresa por zelar pelo cumprimento das regras previstas na lei e orientar os funcionários e os contratados da instituição a respeito das práticas a serem tomadas em relação à proteção de dados pessoais. Assim, dentre as funções do Encarregado, destacamos: (i) recepcionar e atender demandas dos titulares de dados; (ii) interagir com a Autoridade Nacional de Proteção de Dados e (iii) orientar funcionários e contratados quanto a práticas de proteção de dados. O Encarregado se reporta diretamente ao mais alto nível de direção, deve ser dotado de autonomia e estabilidade, independência orçamentária e se mostra obrigatório para empresas que tratam dados pessoais como controladoras.

## F) *PRIVACY BY DESIGN E PRIVACY BY DEFAULT*

O *Privacy by design* representa o emprego de mecanismos/soluções de privacidade durante todo o ciclo de vida dos dados. Por referido conceito, **a privacidade é incorporada à própria arquitetura dos sistemas e processos** desenvolvidos, de modo a garantir, pela infraestrutura do serviço prestado, condições para que o usuário seja capaz de preservar e gerenciar sua privacidade e a coleta e tratamento de seus dados pessoais.

Por seu turno, *Privacy by default* representa a obrigatoriedade de que todas essas ferramentas estejam acionadas como padrão. Ou seja, estabelecer como **configuração padrão a maior privacidade possível ao titular dos dados**.

Os agentes de tratamento devem, portanto, desde a concepção do produto ou do serviço, até a sua execução, 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, §2º).

## G) QUEM FISCALIZARÁ O CUMPRIMENTO DA LEI?

Autoridade Nacional (art. 5º, XIX e art. 55° vetado): órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei. Peça essencial do marco normativo em questão, com competências de promoção de estudos e da cultura de proteção de dados, cooperação com as demais autoridades nacionais e internacionais, edição de regulamentos, fiscalização, sancionamento, entre outros. A experiência internacional reforça a necessidade de criação de tal instância reguladora, com **características de independência, especialização técnica** e poderes efetivos de *enforcement*. Espera-se que tal Autoridade seja estabelecida por Lei ou Medida Provisória que reproduza os artigos que foram objeto de veto da LGPD.

## H) 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.

Sanções administrativas (art. 52º): os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas na Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

**(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.

**Responsabilidade e ressarcimento de danos (seção III):**

1. 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.

2. O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador;

3. Os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente.

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

5. Os agentes de tratamento só não serão responsabilizados quando provarem: que não realizaram o tratamento de dados pessoais que lhes é atribuído; não houve violação à legislação de proteção de dados; ou que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

6. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: o modo pelo qual é realizado; o resultado e os riscos que razoavelmente dele se esperam; as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

## I) COMO SE ADEQUAR À LEI?

**A LGPD entrará em vigor em 16.02.20**. 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 algumas ações básicas, como:**

**(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 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, mediamente 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.

# FICHA TÉCNICA

## ELABORAÇÃO

**Rony Vainzof**
Diretor do Departamento de Defesa e Segurança da FIESP e Coordenador do Grupo de Trabalho de Segurança e Defesa Cibernética

**Luciana Nunes Freire**
Diretora Executiva Jurídica da FIESP

**Caio Oliveira**
Colaborador do Grupo de Trabalho de Segurança e Defesa Cibernética

## COORDENAÇÃO

**Luciano Villela Coelho**
Gerente do Departamento de Defesa e Segurança da FIESP e membro do Grupo de Trabalho de Segurança e Defesa Cibernética


**Av. Paulista, 1313**
**São Paulo - SP | CEP: 01311-923**
**deseg@fiesp.com.br**
**www.fiesp.com.br**