LGPD para PMEs

Principais aplicações da Lei Geral de Proteção de Dados Pessoais para Pequenas e Médias Empresas

Edição atualizada: fev - mar/2025

GISELE TRUZZI

TECH LEGAL ADVISORY

Sumário

O que é a LGPD

LGPD é a abreviação para a "**Lei Geral de Proteção de Dados Pessoais**" – Lei nº 13.709/2018, que entrou em vigor em setembro/2020 e visa garantir a cada cidadão os direitos básicos relacionados aos dados pessoais, tendo em vista uma crescente digitalização de todos os tipos de relações.

Entre os objetivos principais da LGPD, estão:

1

Regular o tratamento de dados pessoais;

2

Definir princípios fundamentais para o tratamento de dados pessoais pelos agentes responsáveis (controlador e operador);

3

Garantir direitos básicos aos titulares dos dados pessoais (pessoas físicas);

4

Impor sanções a quem eventualmente viole a Lei.

A quem se aplica a LGPD

A LGPD é aplicável a todas as pessoas físicas ou jurídicas de direito público (órgãos, entidades) e de direito privado (empresas) que realizam qualquer tipo de tratamento de dados pessoais. Tanto em ambiente online (bancos de dados) quanto em ambiente *offline* (arquivos físicos em papeis).

Não importa o tamanho da estrutura, seja pequena, média ou grande - havendo tratamento de dados pessoais, ainda que seja somente dos colaboradores - todos devem se adequar à LGPD.

Por que preciso adequar a minha PME à LGPD?

Primeiramente, para **demonstrar o compromisso com a privacidade dos seus clientes, consumidores, usuários, fornecedores e colaboradores**, é de extrema importância a adequação à LGPD, de forma a contribuir para uma cultura de proteção de dados essencial em nossa sociedade cada vez mais digital.

Além disso, a empresa que atende políticas de *compliance* com a LGPD, por exemplo, guarda para si um **diferencial competitivo** em seu nicho de mercado: potenciais clientes, ao perceberem que a sua empresa está em conformidade legal - ao contrário dos demais concorrentes -, tendem a valorizar a iniciativa e postura e esse fator poderá ser decisivo no momento da contratação.

Outro ponto de destaque: desde a concepção de um novo modelo de negócio, novos produtos ou serviços, é a constante busca por soluções que harmonizem às boas práticas de privacidade dos clientes em potencial, consumidores ou usuários. Isso certamente abrilhanta e inova o cotidiano. Afinal, é preciso estabelecer parâmetros construtivos para atender novas demandas de privacidade daqueles que buscam pelos produtos e serviços dispostos no mercado.

Existem outras motivações para a chamada conformidade legal com a LGPD:

1. Minimizar riscos e incidentes;
2. Evitar sanções judiciais ou regulatórias;
3. Padronização de processos, procedimentos e atividades;
4. Incrementar a Segurança da Informação na empresa;
5. Aumentar a credibilidade.

Uma empresa mais segura (tanto jurídica, quanto técnica e administrativamente), tem maior valor e confiança perante o mercado e público-alvo.

Por que é importante ter respaldo jurídico na adequação à LGPD?

A LGPD é uma legislação dividida por 2 visões: **jurídica** e **técnica**. Portanto, ao se adequar à Lei Geral de Proteção de Dados Pessoais é de extrema importância que profissionais responsáveis pelo projeto de compliance tenham expertise jurídica e técnica, focada em Segurança da Informação.

O respaldo jurídico é essencial para a plena implantação da LGPD: advogados especializados no tema, com prática em Direito Digital, Segurança da Informação, Compliance, Proteção de Dados e Privacidade da Pessoa Natural terão maior segurança na interpretação dessa Lei e implementação ao correspondente negócio, sabendo distinguir quais níveis de sigilo devem ser empregados a toda documentação, fluxos de dados, processos de negócios e ciclo de vida dos dados pessoais que trafegam por sua empresa.

Esses profissionais também atuam na:

- Revisão da documentação jurídica essencial à sua empresa nas principais relações do dia a dia: contratos com clientes, fornecedores, prestadores de serviços e colaboradores; elaboração de termos de conformidade; redação de cláusulas específicas para contratos, aditivos contratuais, termos e outros documentos jurídicos, visando plena adequação da empresa à legislação vigente;

- Elaboração dos pareceres jurídicos específicos sobre a melhor aplicação da LGPD à sua empresa, de acordo com os tipos de dados pessoais tratados de seus titulares;

- Orientação sobre criação do cargo de Encarregado do Tratamento de Dados Pessoais;

- Revisão das seções específicas do site ou app da empresa, com foco nas demandas e questionamentos recepcionados via site ou app, que tenham relação com tratamento de dados pessoais;

- Elaboração ou revisão dos Termos de Uso, Políticas de Privacidade, entre outros documentos específicos para o site ou app da empresa ou desenvolvido sob encomenda;

- Treinamento para todos os colaboradores e diretoria da empresa, nivelando o grau de conscientização sobre a LGPD e criação da cultura de proteção de dados de excelência.

Por que é importante ter o apoio técnico em Segurança da Informação na adequação da minha empresa à LGPD?

Dos princípios que regem a própria LGPD vale a pena enfatizar o da Segurança da Informação.

Não é demais relembrar que no texto da LGPD é obrigatório às empresas que implementem mecanismos no controle de Segurança da Informação.

Veja essa simplificação:

Adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais (art. 46)

Garantir a segurança da informação em relação aos dados pessoais (art. 47)

Comunicar à Autoridade Nacional e ao Titular de Dados Pessoais, a ocorrência de incidentes de segurança (art.48)

Estabelecer sistemas estruturados de tratamento de dados pessoais de forma a atender os requisitos de segurança (art. 49)

Formular normas de segurança (art. 50)

Dessa maneira, ter uma estrutura de Segurança da Informação passível de atender às exigências e modelos de fiscalização impostos pela Lei depende de um controle de implementação operacional compatível com o porte e abrangência do negócio da empresa.

A colaboração de um apoio técnico nessa seara é fundamental para entender a lógica dos passos de uma implementação de Segurança da Informação bem feita. Pequenas e médias empresas normalmente não contratam para o quadro interno profissional com experiência em Segurança da Informação e precisam de apoio externo.

O detalhamento de como devem ser os controles de Segurança da Informação que a LGPD cita estão descritos na Família de Normas ISO 27000, já aprovadas e disponíveis pela Associação Brasileira de Normas Técnicas (ABNT).

Considerando as Pequenas e Médias Empresas, destacamos alguns **controles básicos de Segurança da Informação que a sua empresa deve adotar o quanto antes**:

Controle de Acesso Lógico

1

Os acessos às informações dos sistemas existentes e serviços em uma empresa tipo Internet Banking devem ser monitorados em tempo real. Dessa forma, somente usuários devidamente autorizados e que mantenham vínculo profissional podem preencher tais requisitos. O desligamento desse profissional descarta automaticamente o seu perfil de acessos.

Regulamentos

2

Os controles que a empresa segue devem ser melhor definidos nos regulamentos internos ou códigos de conduta. A estrutura desses regulamentos ou códigos são desenhados de acordo com o tamanho e complexidade do negócio. Para uma pequena empresa apenas o regulamento talvez seja suficiente. A depender de uma avaliação profissional.

Cópias de Segurança

3

Devem existir cópias de segurança dos dados, sistemas e outros elementos necessários para a operacionalização do negócio. A guarda dessas cópias pode ser em serviço de nuvem de tecnologia ou em um disco removível guardado em local diferente do ambiente principal de informação.

Proteção Técnica

4

Os recursos de tecnologia devem ser protegidos tecnicamente contra erros, falhas e invasão por criminosos. Muitas vezes o desenvolvimento ou contratação de programas que protejam o ambiente é mandatório. Nesses casos, o apoio de um especialista para sanar dúvidas, fixar rotinas de triagem e proteção de dados sensíveis economiza dinheiro, tempo e transtornos atuais ou futuros.

Gestão de Riscos: combate a ameaças

5

Faça um exercício do "**E se..?**": E se o link de Internet estiver indisponível? E se o computador parar de funcionar? E se os dados dos clientes forem manipulados? Coloque os impactos se estas situações acontecerem e trate de implementar controles preventivos.

Treine seus colaboradores

6

Todos os colaboradores, funcionários ou prestadores de serviço diretos ou indiretos devem ser treinados em Segurança da Informação e Proteção de Dados Pessoais. Isso evita uma série de constrangimentos, identifica responsáveis e minimiza a ação de criminosos, principalmente.

As normas ABNT NBR/ISO definem outros controles, mas esses citados acima são essenciais.

Portanto, a Segurança da Informação é base essencial para a implementação de um bom projeto de adequação à LGPD.

O que a LGPD considera como PME?

De acordo com a Resolução da Agência Nacional de Proteção de Dados (ANPD), que visa a aplicação da LGPD para agentes de tratamento de pequeno porte, são consideradas como PMEs as seguintes classes empresariais:

Microempresas e empresas de pequeno porte:

Sociedade empresária, sociedade simples, empresa individual de responsabilidade limitada e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual.

Startups

Organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados.

Pessoas jurídicas sem fins lucrativos

Associações, fundações, organizações religiosas e partidos políticos.

Agentes de tratamento de pequeno porte

Microempresas, empresas de pequeno porte, startups e pessoas jurídicas sem fins lucrativos, que tratam dados pessoais, e pessoas naturais e entes despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador.

Zonas acessíveis ao público

Espaços abertos ao público, como praças, centros comerciais, vias públicas, estações de ônibus e de trem, aeroportos, portos, bibliotecas públicas, dentre outros.

Além dessas classificações empresariais, há outros fatores que devem ser levados em consideração. Veja:

Condições:

- Limitação de receita bruta máxima conforme prevê o art. 4º, Lei Complementar nº 182, de 1º de junho de 2021 (Marco Legal das Startups);

- Não realizar tratamento de dados de “alto risco” ou de “larga escala”.*

*dados sensíveis ou de grupos vulneráveis; vigilância ou controle de zonas acessíveis ao público; uso de tecnologias emergentes; tratamento automatizado de dados pessoais que afetem interesses dos titulares ou abranger nº significativo de titulares

Facilidades:

- Atendimento às requisições por meio eletrônico ou impresso;

- Dispensa de apresentação de algumas documentações detalhadas;

- Dispensa de cumprir com o direito à “portabilidade”;

- Documentos simplificados.

Assim, se a sua empresa se enquadra no conceito de PME ou *Startup* terá respaldo especial à luz da LGPD.

Quais são os principais processos para a implantação da LGPD na minha empresa, considerando que é uma PME?

Uma vez identificada se a sua empresa se encaixa como PME ou *Startup*, alguns procedimentos são essenciais para implementar com segurança as normas da LGPD.

De acordo com a nossa experiência aqui estão os principais processos para o sucesso de um projeto de adequação à LGPD voltado às PMEs e Startups:

Governança dos Dados

- Revisão de políticas de privacidade e de termos de uso;
- Rastreabilidade dos processos de tratamento de dados;
- Identificação dos dados pessoais e dos tipos de titulares de dados.

Segurança da Informação

Criação de mecanismos para assegurar a proteção dos dados e minimizar incidentes.

Jurídico

- Análise das bases legais da LGPD;
- Revisão dos principais contratos;
- Elaboração de Termo de Conformidade;
- Revisão do site ou app e canais de contato.

Atendimento aos titulares de dados

Criação de mecanismos e fluxos para atender aos titulares de dados e também à ANPD.

Qual a importância das dez bases legais previstas na LGPD?

Podemos dizer que as bases legais previstas na LGPD são os “motivos” pelos quais sua empresa deve seguir para validação e justificativa no tratamento dos dados pessoais.

Se, ao menos, uma ou duas das bases legais à luz da LGPD encaixarem com as finalidades das operações realizadas pela empresa, sua empresa está segura de penalidades ou riscos de ataque cibernético.

Vale lembrar que o termo “tratamento” é toda operação realizada com os dados pessoais, como por exemplo mero armazenamento ou simples acesso visual.

Para elucidar esse tema exemplificamos 10 bases legais da LGPD. Confira aqui:

1

Consentimento

É a única base legal na qual se necessita de autorização do titular.

2

Cumprimento de obrigação legal

Muitas vezes a pessoa ou a empresa solicitam dados pessoais não porque querem, mas sim porque a lei os obriga a ter ou informar esses dados.

3

Execução de política pública

O Estado pode tratar dados para segurança pública, saúde, etc.

4

Execução de contrato

Quando é necessário tratar o dado para execução de um contrato, respeitando-se o princípio da finalidade.

5

Exercício regular do Direito

Sempre que for necessário exercer um direito do Controlador. Exemplo: apresentação de documentação em juízo.

6

Proteção da vida

Sempre que for necessário tratar o dado para proteger a vida ou incolumidade física do titular.

7

Tutela da saúde

Não é necessário consentimento do ponto de vista público.

8

Atividade acadêmica

Não é necessário consentimento para finalidades de estudos e pesquisas estatísticas.

9

Proteção ao crédito

Não é necessário consentimento no sentido regulado, para fins de proteção ao crédito (Ex:SERASA).

10

Legítimo interesse

Permite que a empresa faça o tratamento dos dados de que ela dispõe para o desenvolvimento de suas atividades.

Quais são as imposições da LGPD para as PMEs?

O tratamento de dados sensíveis não pode ser o *Core Business* ou atividade principal de uma PME, tais como: armazenamento, gravação sob qualquer suporte, transcrição das informações pessoais de potenciais clientes, clientela fixa, consumidores em geral ou simples usuários (não habituais). Todo cuidado se faz necessário para manter a segurança e prevenir incidentes com os dados tratados mesmo aqueles básicos coletados e consentidos para garantir obrigações contratuais, entregas etc.

Agir com a máxima transparência perante os titulares de dados e atuar proativamente esclarecendo dúvidas sobre os procedimentos implementados pela empresa somados à indicação rápida e simples dos responsáveis pelo acompanhamento desses dados reforça a boa política de aderência à LGPD, dá mais tranquilidade a todos os envolvidos e demonstra, acima de tudo, respeito às normas de proteção dos dados pessoais de terceiros.

Quais são as sanções e multas da LGPD para as PMEs?

Durante a apuração de indícios de irregularidades por descumprimento de quaisquer normas elencadas na LGPD, as PMEs podem sofrer sanções (penalidades) por cada infração cometida, respondendo ainda processo administrativo de fiscalização para conferir se houve má-fé da empresa ou dos representantes legais por omissão (negligência), imprudência ou imperícia.

Entre as hipóteses de incidência dessas sanções podemos enumerar além da restrição de atividades a advertência, multa simples de até 2% do faturamento, multa diária e/ou publicização da infração após devidamente confirmada em deliberação colegiada a sua ocorrência, e até mesmo eliminação da base de dados, conforme apontam os artigos 52 a 54 da Lei.

Os valores serão calculados quanto a intensidade do dano causado e capacidade financeira das PMEs. De toda sorte, evitar processos burocráticos e custosos que influenciam negativamente na imagem das empresas investigadas como dito anteriormente é a alternativa mais condizente com as técnicas de *Compliance*.

Como iniciar um processo de adequação da minha empresa à LGPD?

O processo de adequação de uma empresa à LGPD não precisa ser excessivamente caro ou complexo, pois deve ser adaptado à realidade organizacional e financeira de cada PME.

O profissional interno ou a consultoria contratada deverá analisar o perfil de sua empresa e elaborar um plano de ação que seja adequado à realidade da empresa e conforme o tratamento de dados pessoais efetuado.

Para iniciar a conformidade legal com a LGPD desenvolvemos um infográfico de medidas emergenciais que poderão ser adotadas por sua empresa:

Sete sugestões de ações emergenciais para cumprimento da LGPD pelas empresas:

Nomeação do Encarregado

Revisão do Consentimento

Elaboração ou Revisão dos Termos de Uso e Política de Privacidade

Plano de Ação

Revisão da Documentação Jurídica

Garantia dos Direitos dos Titulares de dados

Conscientização dos colaboradores sobre a LGPD

Perguntas Frequentes

- **Minha empresa é pequena. Preciso me adequar à LGPD?**

Sim, a LGPD se aplica a todas as empresas (bem como órgãos públicos e pessoas físicas) que tratam dados pessoais, independentemente do porte. Contudo, a ANPD criou regras mais flexíveis para PMEs.

- **O que acontece se minha PME não seguir a LGPD?**

Você pode sofrer sanções, tais como advertências, multas de até 2% do faturamento e até a proibição do tratamento de dados, o que pode impactar suas operações, e até mesmo fechar seu negócio.

- **Minha empresa só coleta nome e e-mail dos clientes. Ainda assim, preciso seguir a LGPD?**

Sim, qualquer dado que possa identificar uma pessoa está sujeito à LGPD. É necessário garantir transparência e segurança no tratamento dessas informações.

- **Preciso contratar um DPO (*Data Protection Officer* - Encarregado de Dados)?**

PMEs estão dispensadas dessa obrigatoriedade, mas é recomendado nomear um responsável interno ou terceirizar o serviço para evitar problemas de conformidade.

- **Como minha empresa pode obter consentimento válido dos clientes?**

O consentimento deve ser claro, específico e livre de coerção. Você pode usar formulários, caixas de seleção no site ou contratos que explicitem como os dados serão usados.

- **Como minha PME pode comprovar que está em conformidade com a LGPD?**

Manter registros dos processos, criar políticas de privacidade, revisar contratos e garantir a segurança dos dados são formas de demonstrar conformidade.

Sobre os autores:

Gisele Truzzi

CEO e Sócia Fundadora de *Gisele Truzzi Tech Legal Advisory*.
Advogada especialista em Direito Digital, Segurança da Informação, Privacidade e Proteção de Dados, com prática de 20 anos na área; dos quais 15 são à frente de seu escritório, assessorando empresas a alavancarem e organizarem seus negócios no mundo digital.

Iasmin Palotta

Advogada e sócia em *Gisele Truzzi Tech Legal Advisory*.
Atuante nas esferas consultiva e contenciosa em Direito Digital, Segurança da Informação, Inovação, Privacidade e Proteção de Dados.

Beatriz Junque

Advogada e gestora de projetos de *Compliance* em *Gisele Truzzi Tech Legal Advisory.*
Especialista em Direito Digital e Compliance. Atuante nas áreas do Direito Digital, Privacidade e Proteção de Dados e Direito do Entretenimento.

Flora Santiago

Advogada em *Gisele Truzzi Tech Legal Advisory.*
Especialista em Direito Digital e Proteção de Dados. Encarregada de Dados.

Marcelo Nogueira Mallen

Advogado especialista em Direito Digital, Direito Societário e Direitos Autorais.

Beatriz Pistarini

Advogada especialista em Direito Digital e *Compliance.*

Edison Fontes

Consultor e Gestor de Segurança da Informação e Proteção de Dados Pessoais.

GISELE TRUZZI

TECH LEGAL ADVISORY

www.truzzi.com.br

Acesse nossas redes:

Avenida Paulista, nº 1.765 - 7º andar - Conj. 72 - CV 8828
Bela Vista - São Paulo/SP - CEP 01311-200

Telefones: +55 11 3075-2843 e 98584-9279

E-mail: contato@truzzi.com.br

ISBN: 978-65-986496-0-9