

The background of the top half of the page is a dark blue field filled with abstract, glowing blue lines and concentric circles, suggesting a digital or technological theme. A semi-transparent shield icon is visible on the left side of the upper half.

Lei Geral de Proteção de dados

*// Tudo que você precisa saber para
adequar sua empresa à LGPD*

Compliance
for **Business**

Autores



> **Tiago Alegretti**

Executivo com mais de 10 anos de experiência, Tiago integrou e liderou departamentos jurídicos e de compliance de empresas como Vipal, Hyundai e Grupo A Educação. Em 2020, foi eleito como um dos executivos jurídicos mais admirados do Rio Grande do Sul pela Intelijur. É coordenador e professor de cursos de compliance, especialista e mestrando em Direito empresarial pela PUC e Unisinos. Ocupa também o cargo de Diretor Acadêmico da Associação Brasileira de Direito e Administração (ABD&A), além de ser fundador do GEPACE (Grupo de Estudos e Práticas Avançadas em Compliance Empresarial).



> **Lucas Froehlich**

Advogado com mais de 10 anos de atuação na área jurídica, sendo membro da ICA – International Compliance Association. Pós-Graduando em Direito Empresarial pela PUC-MG e com Pós-Graduação concluída, também na área empresarial, pelo Centro Universitário Leonardo da Vinci, área em que detém ampla experiência, principalmente em análise e negociações com jurídicos corporativos de multinacionais. Com experiência em processos judiciais e administrativos em diversos Estados, principalmente Rio Grande do Sul e São Paulo.

Índice

- 04.** O que é a LGPD?
- 05.** A dificuldade de começar
- 06.** Quais são os fundamentos da Lei?
- 07.** O que é dado pessoal?
- 07.** E os dados pessoais Sensíveis e Anonimizados?
- 08.** O tratamento de dados pessoais
- 08.** Quando se aplica a LGPD?
- 08.** Quando não se aplica a LGPD?
- 09.** ANDP
- 10.** Incidentes e procedimentos relacionados
- 11.** Treinamentos
- 12.** Requisitos básicos da adequação à LGPD
- 13.** Etapas de uma adequação à LGPD
- 13.** Etapas comuns
- 14.** Mapeamento de riscos, medidas mitigadoras e monitoramento
- 15.** Mapeamento de fluxos de dados pessoais
- 16.** Tecnologia e segurança da informação
- 16.** Relatório de maturidade e proteção de dados
- 17.** Planos de ação
- 17.** Redesenho de processos internos
- 17.** Política de proteção de dados e segurança da informação
- 17.** Contratos e termos de consentimento
- 18.** Portal do titular
- 18.** Cultura

O que é a LGPD?

A Lei Geral de proteção de dados (Lei nº 13.709, de 14 de agosto de 2018) tem o objetivo de regular o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica. Implica dizer que, salvo raras exceções detalhadas adiante, empresas e pessoas físicas que coletam, guardam, processam ou utilizam dados pessoais para fins de atividades remuneradas tem o dever de zelar por estes nos termos estabelecidos na LGPD.

Estas legislações que objetivam proteger dados pessoais foram motivadas, principalmente, pela necessidade de se evitar monopólios detentores de dados e proteger a privacidade das pessoas.

A partir do momento em que países americanos e europeus iniciaram suas legislações, verificou-se a necessidade de que outros países, como o Brasil, embarcassem na mesma jornada, eis que não ter uma legislação protetiva poderia resultar em uma perda importante de competitividade internacional. Isto ocorre porque empresas que se preocupam com a proteção e correta utilização de dados pessoais tendem a evitar a realização de negócios com empresas que não o fazem, criando assim um efeito cascata de

adequação.

Assim, para todas estas pessoas e empresas que de alguma forma tratam dados pessoais, a legislação criou algumas obrigações com a

finalidade de resguardar os dados pessoais e proteger os direitos fundamentais de liberdade, de privacidade, e o livre desenvolvimento da personalidade, que veremos nos capítulos a seguir.



A dificuldade de começar

As alterações propostas pela Lei Geral de Proteção de Dados mudaram a forma como as empresas e pessoas se relacionavam com dados pessoais. Esta mudança implicou em uma

necessidade de adequação de negócios e ambientes tecnológicos, causando naturalmente dificuldades de adaptação.

As antigas modalidades de captação de dados pessoais em troca de produtos ou serviços, compra e venda de listas de e-mail ou telefones, e formas agressivas de abordagem a potenciais clientes devem ser imediatamente cessadas.

Além disso, a simples guarda de documentos de funcionários e prestadores de serviço ou fornecedores implicam em necessidades adicionais de segurança, dever de sigilo e, principalmente, ciência e consentimento dos titulares destes dados para suas formas de utilização.

Afora estes cuidados, a LGPD criou outras obrigações, como a necessidade de disponibilizar um local para os titulares realizarem solicitações, a

eleição de um encarregado pela proteção de dados da empresa (DPO), a criação de políticas de dados e de privacidade, entre outras adiante detalhadas.

O objetivo deste e-book é demonstrar como a LGPD impacta as empresas, trazer a teoria à prática, e servir como um guia básico dos passos de uma adequação à LGPD para empresas de todos os portes.

Quais são os fundamentos da Lei?

Os fundamentos da LGPD são as premissas que basearam sua criação nos âmbitos econômicos e sociais. Estes fundamentos são:

-
- > Respeito à privacidade
- > Autodeterminação informativa
- > Liberdade de expressão, de informação, de comunicação e de opinião
- > Inviolabilidade da intimidade, da honra e da imagem
- > Desenvolvimento econômico e tecnológico e a inovação
- > Livre iniciativa, a livre concorrência e a defesa do consumidor
- > Direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais
-

O que é dado pessoal?

Dado pessoal é qualquer Informação relacionada a pessoa natural.

Ao nos depararmos com a expressão dados pessoais, imediatamente pensamos em dados como nome, CPF, telefone e endereço. Entretanto, há muito mais dados pessoais do que os citados.

Podemos citar outros exemplos, como hábitos e características físicas. Assim, este conceito deve ser entendido de maneira literal, eis que, efetivamente, toda e qualquer informação relacionada a uma pessoa natural é um dado pessoal para fins da LGPD.

E os dados pessoais Sensíveis e Anonimizados?

Dados pessoais sensíveis são aqueles que tratam sobre questões delicadas, que podem causar graves prejuízos ao titular quando reveladas sem sua anuência. Estamos tratando de dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, sobre saúde ou vida sexual, genética ou biometria.

Já os dados anonimizados são aquelas informações relativas a um titular que não pode ser identificado. Estes não são abrangidos pelas obrigações estabelecidas na LGPD.

O Tratamento de Dados Pessoais

Tratamento é toda e qualquer 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.

Quando se aplica a LGPD?

Aplica-se a Lei Geral de Proteção de Dados a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I. a operação de tratamento seja realizada no território nacional;

II. a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

III. os dados pessoais objeto do tratamento tenham sido coletados no território nacional (Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta).

Quando não se aplica a LGPD?

Não aplica-se a Lei Geral de Proteção de Dados ao tratamento de dados pessoais:

I. realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II. realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos;

III. realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

- c)** segurança do Estado; ou
- d)** atividades de investigação e repressão de infrações penais; ou
- IV.** provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de

dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

ANPD

Assim como outras agências reguladoras, a ANPD (Autoridade Nacional de Proteção de Dados) é um órgão da administração pública federal e tem assegurada sua autonomia técnica e decisória.

A ANPD é composta de:

- I** Conselho Diretor, órgão máximo de direção;
- II** Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;
- III** Corregedoria;
- IV** Ouvidoria;

V Órgão de assessoramento jurídico próprio; e

VI Unidades administrativas e unidades especializadas necessárias à aplicação da Lei

Sua atuação consiste em zelar pela proteção de dados pessoais, gerar diretrizes, fiscalizar a aplicação da Lei, inclusive aplicando sanções, compartilhar conhecimento, entre outras obrigações estabelecidas na LGPD.

Incidentes e procedimentos relacionados

A violação de dados ocorre quando do descumprimento, por parte da controladora, dos deveres e obrigações referentes ao processamento, armazenamento e/ou utilização dos dados por ela controlados.

> Penalidades

Sem prejuízo de outras ações cíveis ou penais, o descumprimento da LGPD pode gerar à empresa:

- a)** Multas de até 2% do faturamento até o limite de R\$ 50.000.000,00 (cinquenta milhões de reais) por infração
- b)** Publicização da Infração, gerando prejuízos à imagem da empresa
- c)** Bloqueio de acesso aos dados
- d)** Suspensão da atividade de tratamento de dados
- e)** Proibição de atividades relacionadas

Estas penalidades podem ocorrer após procedimento administrativo com possibilidade de ampla defesa e levarão em conta fatores como

gravidade, vantagem econômica percebida pelo infrator, reincidência, capacidade econômica do infrator e a cooperação do infrator.



Treinamentos

Mais do que estar adequado, é de fundamental importância que a empresa treine seus colaboradores e terceiros sobre os direitos e deveres estabelecidos na Lei Geral de Proteção de Dados, bem como sobre a sua política de proteção de dados.

Para as empresas, é importante que todas as pessoas treinadas informem expressamente que compreenderam e concordam com as regras contidas na Lei e nos documentos da empresa, incluindo a Política de Proteção de Dados.

Além de estar adequado à legislação, é importante que as empresas consigam atestar esta adequação, comprovando etapas realizadas, mapeamento de dados, decisões tomadas, treinamentos efetuados, entre outros.

Requisitos básicos da adequação à LGPD

Consentimento



É importante que a empresa tenha consentimento de todas as pessoas sobre os dados que estiver em sua posse, bem como que as formas de utilização estejam autorizadas.

Cuidados



A nova lei de dados também tem regras específicas para tratar de dados sensíveis, como informações de crianças e adolescentes, e, ainda, transferência internacional de dados.

Prevenção



A lei determina punições para infrações envolvendo incidentes de segurança de dados, que vão de advertência a multa de até 2% do faturamento anual da empresa, limitado a R\$ 50 milhões por infração.

Acesso



Os titulares dos dados têm direito ao acesso, informação, cancelamento, retificação, oposição e portabilidade de seus dados.



DPO/Encarregado



Todas as empresas deverão ter um encarregado, ou seja, uma pessoa responsável pelo cumprimento da LGPD da empresa. Esta pessoa pode ser física, como por exemplo um funcionário, ou um terceiro (até mesmo uma pessoa jurídica).

Relatório de Impacto



É necessário também que a empresa tenha um relatório de impacto, no qual serão descritos todos os riscos de eventuais descumprimentos da Lei e formas de amenização de danos.

Etapas de uma adequação à LGPD

Não há uma fórmula exata para estar adequado à LGPD, cada empresa deve verificar suas rotinas, seu mapeamento de dados, processos internos, ambiente tecnológico e jurídico, a fim de cumprir integralmente a legislação.

Entretanto, algumas etapas são comuns na grande maioria das adequações, passemos a elas.



Etapas comuns

- 1 Definição do Encarregado (DPO)
- 2 Diagnóstico Inicial
- 3 Mapeamento de Riscos
- 4 Mapeamento de Dados
- 5 Análise de vulnerabilidades tecnológicas e reforço em segurança da informação
- 6 Revisão do site e redes sociais
- 7 Criação do Portal do Titular
- 8 Redesenho de Processos Internos
- 9 Revisão Contratual e de termos de consentimento
- 10 Criação de Políticas
- 11 Treinamentos
- 12 Fortalecimento de Cultura em Proteção de Dados

Mapeamento de riscos, medidas mitigadoras e monitoramento

Esta etapa consiste na identificação de riscos das atividades da empresa em relação à LGPD. Pode ser baseada em uma matriz probabilidade x impacto, considerando fatores como a forma de utilização de dados e a regulamentação específica do setor.

		Impacto					
		← + — →					
		1. Extremo	2. Alto	3. Moderado	4. Baixo	5. Irrelevante	
Probabilidade	+	Quase Certo	Muito Crítico	Muito Crítico	Crítico	Pouco Crítico	Significante
		Muito Provável	Muito Crítico	Crítico	Pouco Crítico	Muito Significante	Significante
		Pouco Provável	Crítico	Pouco Crítico	Muito Significante	Significante	Pouco Significante
		Improvável	Pouco Crítico	Muito Significante	Significante	Pouco Significante	Insignificante
	-	Raro	Muito Significante	Significante	Pouco Significante	Insignificante	Insignificante

É importante realizar um desenho de implementação progressiva de

medidas de mitigação dos riscos identificados, conforme prioridades estabelecidas, gerando alternativas seguras e sustentáveis sem prejudicar o andamento dos negócios.

Para iniciar, a empresa pode criar um comitê de LGPD, com eleição dos integrantes, distribuição de funções, treinamento e monitoramento de atividades, tendo como principal atribuição garantir o cumprimento da política de proteção de dados da companhia.

vazamento/má-utilização de dados pessoais, é preciso definir restrições de acesso e aprimorando a segurança do trânsito das informações.

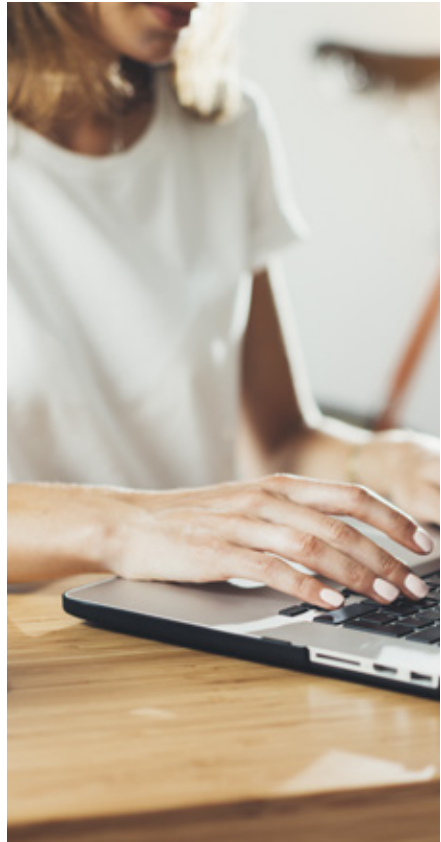
Neste momento, a empresa deve estabelecer as funções e realizar os treinamentos necessários para que o Comitê de LGPD propicie governança adequada de dados na empresa, promovendo a segurança e o cumprimento da política de dados pela companhia, seus colaboradores e terceiros.

Mapeamento de fluxos de dados pessoais

Nesta etapa, a empresa deve mapear todas as entradas de dados pessoais e qual seu fluxo de tratamento interno e externo.

Em todas as entradas, devem ser criados os termos de consentimento necessários. Lembrando que o consentimento pode ser dispensado sempre que o tratamento do dado for motivado pelo cumprimento de obrigações contratuais ou legais.

Após identificar os principais riscos a que a empresa está exposta e adequar o fluxo visando a redução de riscos de



Tecnologia e segurança da informação

// Após o mapeamento dos fluxos de dados e entendimento dos riscos a qual a empresa está exposta, mapear os dados de forma adequada para o controle, inventário e ciclo de vida dos dados.

Esta etapa consiste em identificar riscos, inteligência de ameaças, identificação de vulnerabilidades e gap analysis, para que a empresa tenha maior tranquilidade quanto à segurança dos dados por ela processados.

Ao final deste trabalho, deve ser possível elaborar um relatório de vulnerabilidade de sistemas, riscos de vazamentos de dados e principais vetores de ataques e roubo de dados.

Após, a empresa deve continuar monitorando melhorias nos sistemas ou substituições, conforme necessidade, dentre eles antivírus, segmentação de rede, melhoria na análise de gestão dos incidentes de segurança, sugestão de ferramentas contra vazamento de dados, definição de itens para construção de RFP de segurança.

Relatório de maturidade e proteção de dados

Este processo de monitoramento e adequação continua prevê a elaboração de relatórios contendo o nível de maturidade da empresa com relação aos dados pessoais tratados, finalidades indicadas conforme enquadramento pela LGPD, regulamentação complementar, consentimentos,

riscos por ordem de grandeza, priorizações conforme grau de gravidade e área de atuação, implementação das medidas de mitigação sugeridas, resultados, efeitos e planos de ação.

Planos de ação

O projeto de adequação contempla, ainda, a identificação, execução, monitoramento e aprimoramento de planos de ação com o objetivo de melhoria contínua da empresa em matéria de adequação à LGPD, segurança da informação e privacidade, considerando o planejamento estratégico da companhia, os riscos envolvidos e a priorização das ações para o enquadramento da empresa.

Redesenho de processos internos

Nesta etapa, a empresa já tem conhecimento sobre os riscos e a segurança de seus sistemas, o que permite redesenhar seus processos internos, com o objetivo de evitar o trânsito inadequado de dados, propondo modificações que criem segurança e sustentabilidade na empresa com o menor impacto possível em suas

atividades. Esta etapa contempla, ainda, a criação de processos internos para avaliação de riscos de privacidade.

Política de proteção de dados e segurança da informação

O projeto deve englobar a criação da política de dados da empresa contendo todas as orientações acerca da LGPD, formas de tratamento de dados, restrições, incentivos, visando o fortalecimento da cultura de proteção a dados da empresa.

Contratos e termos de consentimento

Nesta etapa ocorre a revisão e adequação dos contratos modelo da empresa, visando a alteração ou inclusão de cláusulas necessárias para o correto enquadramento da LGPD,

considerando as atividades e trocas de dados ocorridas caso a caso.

É nesta fase também que deve ocorrer a criação dos termos de consentimentos necessários para o correto tratamento dos dados nos limites estabelecidos em lei, bem como preparação do ambiente para que estes termos sejam aceitos ou não pelo titular, com o correto direcionamento dos dados na empresa conforme decisão tomada pelo usuário.

Portal do titular

Uma etapa imprescindível no projeto é a abertura de um canal de comunicação entre a empresa e os titulares de dados, com o objetivo de proporcionar a estes a possibilidade de questionar quais dados a empresa detém, forma de tratamento e utilização, bem como solicitar alterações/remoções.

Para estar preparada, a empresa pode elaborar um plano de resposta a incidentes, minutas padrão para respostas de titulares de dados e autoridades. É recomendável a realização de workshops que contemplem, dentre outras questões, treinamentos para o DPO da empresa, interno ou externo, quanto à forma de resposta destas solicitações.

Cultura

Prestadores de Serviços e demais terceiros

Por fim, considerando-se que o fortalecimento da cultura se dá por meio do princípio “Tone From the Top”, no qual a transformação cultural inicia-se na liderança, irradiando para o restante da empresa por meio do exemplo e incentivo ao cumprimento da legislação externa e políticas da Companhia, a empresa deve buscar no mercado ou internamente, a realização de treinamentos que contemplem:

- > O que é LGPD
- > A Importância da Proteção de Dados e Privacidade
- > O papel dos colaboradores no processo de adequação à LGPD
- > DPO – Atribuições e Respostas a titulares
- > Conscientização sobre riscos tecnológicos em relação à LGPD
- > Mitigando riscos práticos sobre vazamento de informações
- > Como tratar dados pessoais na empresa e na vida privada

// Esperamos que este e-book possa servir como um guia de noções gerais para a adequação de sua empresa à LGPD.

-

Contem conosco para o que precisarem nessa jornada.

(51) 2117-1877 | contato@complianceforbusiness.com.br

Compliance
for **Business**