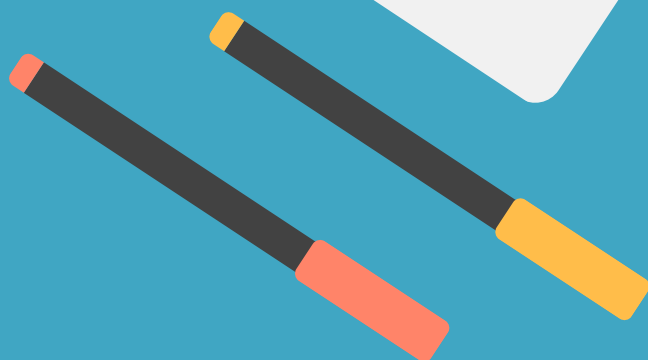
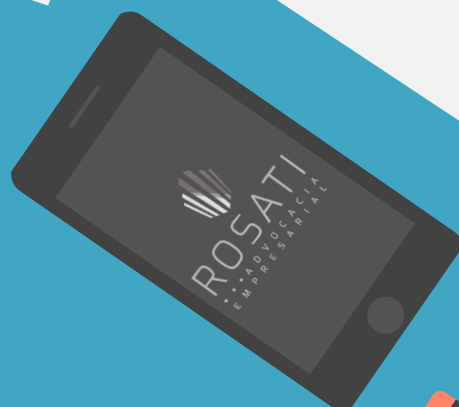




ROSATI

ADVOCACIA  
EMPRESARIAL



# LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

GUIA PRÁTICO DE IMPLEMENTAÇÃO PARA  
STARTUPS, MICRO E PEQUENAS EMPRESAS

LEI 13.709/18 - LGPD

# Índice:

1

**Guia prático para adequação com a Lei**

2

**O que você precisa saber sobre a LGPD**

3

**Quem é e o que faz o DPO (encarregado)**

4

**Como fazer o mapeamento dos dados**

5

**Políticas de Privacidade, Regimento Interno, Conscientização e Gestão de Riscos**

6

**Enquadramento das bases legais**

7

**Princípios, Direitos e Sanções**

8

**Adequação dos Contratos e Política de Segurança das Informações**

9

**E se tiver vazamento de dados**


10

**Sem pânico =)**





# Passos práticos para implementação

**A.** Conheça a Lei e entenda os PRINCÍPIOS, DIREITOS E DEVERES  
Você já está fazendo isso aqui 

**B.** Nomeie um encarregado pela implementação da Lei dentro da empresa. Esse será o seu DPO!

**C.** Identifique quais dados pessoais você tem na sua empresa, por que os tem e como captou  
FAMOSO MAPEAMENTO DE DADOS

**D.** Todos funcionários e parceiros da empresa precisam saber do que se trata a Lei e como será feito o tratamento interno.  
CONSCIENTIZAÇÃO E ADEQUAÇÃO

**E.** Elabore e revise as Políticas de Segurança (PSI), Regimento Interno (RI) e Contratos

**F.** Utilize o mapeamento feito para enquadrar os dados pessoais nas hipóteses de BASES LEGAIS que a Lei dispõe

**G.** Implemente ferramentas que permitam aos titulares de dados pessoais exercerem seus DIREITOS garantidos pela LGPD

**H.** Elabore, revise e adapte CONTRATOS que envolvam tratamento e/ou compartilhamento de dados pessoais, tanto nas relações com usuários e consumidores, quanto nas relações com fornecedores e parceiros comerciais

**I.** Desenvolva as medidas que devem ser tomadas no caso de vazamento de dados juntamente com o RELATÓRIO DE IMPACTO





# O que eu preciso saber sobre a nova Lei

**DEADLINE** 16.08.2020

A LGPD, Lei Geral de Proteção de Dados Pessoais, entrará em vigor no Brasil em **16 de agosto de 2020**

## QUEM PRECISA SE ADEQUAR À LEI?

A nova Lei será aplicada e fiscalizada da mesma forma para todas as empresas que fazem coleta e tratamento de dados pessoais no País. Isso significa que, independente do porte da empresa, todas (sem exceção) deverão apresentar conformidade com a LGPD em Agosto de 2020.

## QUEM É QUEM NA LEI?

**TITULAR** - é a **pessoa física** a quem um dado pessoal se refere

**CONTROLADOR** - é a pessoa que decide como, quando e por que tratar os dados pessoais. Essa pessoa pode ser natural ou jurídica, de direito público ou privado.

**OPERADOR** - é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador.

**ANPD** - Autoridade Nacional de Proteção de Dados - Agência reguladora vinculada ao Ministério da Justiça.



# O que eu preciso saber sobre a nova Lei

## QUAL PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS?

A ANPD terá um papel tríplice de:

- (i) fiscalização - poderá editar normas e procedimentos, deliberar sobre a interpretação da LGPD e requisitar informações relacionadas ao tratamento de dados pessoais;
- (ii) sanção - terá poderes para instaurar processo administrativo quando houver descumprimento à LGPD e terá competência exclusiva para aplicar as sanções previstas na LGPD; e
- (iii) educação - irá difundir o conhecimento sobre a LGPD e medidas de segurança, apresentando diretrizes para interpretação da lei,

## COMO IDENTIFICO E COMO SÃO CLASSIFICADOS OS DADOS PESSOAIS?

**DADO PESSOAL** - É qualquer informação relacionada a uma pessoa natural (pessoa física) que possibilite a sua identificação, incluindo, mas não se limitando a: nome, endereço, perfil online, e-mail, empresa onde trabalha, endereço de IP, CPF, RG, número de telefone, códigos de identificação (Cookies), etc. Esses dados possibilitam individualmente ou em conjunto tornar uma pessoa identificável.

**DADO PESSOAL SENSÍVEL** - Toda informação de uma pessoa natural relacionada à origem racial ou étnica; saúde ou vida sexual; genética e biometria; filiação a sindicato; convicção religiosa; e opinião política.

**DADO ANONIMIZADO** - É todo dado que não permite identificar o titular, impedindo a associação direta ou indireta a uma pessoa natural

**TRATAMENTO** - Tudo que envolve a operação realizada com o dado pessoal, como, por exemplo: coleta, uso, armazenamento, compartilhamento e exclusão







# Como fazer o mapeamento dos dados

- **Quais são os dados coletados?**

- É necessário que sejam dados essenciais à atividade e que sejam obtidos a menor quantidade de dados possível.

- **Onde estão os dados coletados?**

- Segurança, disponibilidade, acesso à pessoa interessada e à ANPD.

- Estamos nos referindo aos dados pessoais de todas as pessoas naturais que disponibilizam essas informações à empresa. São os clientes, os próprios funcionários, dentre outros. Nessa perspectiva, o Data Protection Officer (encarregado) da empresa deverá tratar todas essas informações como a lei determina (produzir relatórios para as pessoas e órgão regulador, atender aos pedidos de exclusão de informações, descartar as informações por meio de um processo controlado, seguro e comprovado).

- **Matriz de tratamento dos dados pessoais?**

- Identifique a matriz de captação e tratamento dos dados pessoais.
- Verifique como é feita a colheita, manutenção e descarte dessas informações

- **Como é feita a gestão do controle de consentimentos?**

- Autorização da pessoa natural para que os dados sejam captados, tratados e mantidos na empresa (em sendo aplicado a base legal do consentimento).

- **Qual é a finalidade de uso dos dados pessoais?**

- Toda e qualquer coleta de dados deve respeitar uma finalidade.



# Políticas de Privacidade, Regimento Interno e Conscientização

No contexto de adequação à LGPD e para garantir o efetivo cumprimento das suas disposições, é altamente recomendável que as empresas adotem políticas e programas de governança em privacidade.

Esses programas devem estabelecer, por exemplo, condições, regimes e procedimentos internos para o tratamento de dados pessoais, normas de segurança da informação, padrões técnicos, alocação de responsabilidades e obrigações aos diversos colaboradores envolvidos nas atividades de tratamento, ações educativas, mecanismos internos de supervisão e mitigação de riscos, procedimentos de resposta a incidentes de segurança, entre outros.

É também muito importante que todos os processos, decisões, esforços e ações relacionados à governança de dados pessoais na empresa sejam documentados e mantidos em arquivo para apresentação à ANPD, se necessário.

A adoção de políticas de boas práticas e governança não apenas auxilia a instituição a cumprir com as obrigações estabelecidas pela LGPD, como evidencia os esforços nesse sentido e será considerada (como um atenuante) na aplicação de penalidades em caso de descumprimento da LGPD.





# Políticas de Privacidade, Regimento Interno e Conscientização

Do ponto de vista prático, um programa de Regimento Interno em Privacidade deve:

- a) demonstrar o comprometimento da empresa em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- b) ser aplicável a todo o conjunto de dados pessoais que estejam sob o controle da empresa, independentemente do modo como se realizou sua coleta;
- c) ser adaptado à estrutura, à escala e ao volume das operações da instituição, bem como à sensibilidade dos dados tratados;
- d) estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- e) ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- f) estar integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
- g) contar com planos de resposta a incidentes e remediação; e
- h) ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.









# Enquadramento das BASES LEGAIS

A Lei prevê 10 possibilidades para o tratamento de dados pessoais, que são:

7. Se o tratamento é necessário para proteger a vida ou segurança física do Titular ou terceiro;
8. Por profissionais da área de saúde, serviços de saúde ou entidades sanitárias, para a proteção da saúde das pessoas (médicos, enfermeiros), serviços de saúde (hospitais, centros de atendimento) ou entidades sanitárias (serviços de vigilância sanitária);
9. Para atender os legítimos interesses do controlador ou terceiros. Essa base se distingue das outras bases legais por não precisar de um motivo particular para sua aplicação; não pode ter outra base mais adequada para a atividade do tratamento; e o interesse legítimo pode ser tanto da empresa controladora dos dados, quanto de terceiros (um terceiro particular ou até mesmo a sociedade como um todo);
10. Para proteção do crédito. Como essa base é completamente nova no cenário legislativo global, ainda não se sabe ao certo qual a amplitude do conceito de Proteção do Crédito, contudo, é correto afirmar que tratamentos realizado para fins de garantir que uma operação de crédito seja executada de forma legítima, segura, e cujos riscos da operação foram analisados poderá ser baseado nesta hipótese.





# Princípios, Direitos e Sanções

**DIREITOS** - O titular poderá solicitar à qualquer tempo:

## Direito ao **ACESSO**

Relatório sobre quais são os dados pessoais que a empresa tem a seu respeito

## Direito à **CORREÇÃO**

A correção e/ou atualização de tais informações

## Direito à **ANONIMIZAÇÃO**

A anonimização de seus dados

## Direito à **PORTABILIDADE**

A portabilidade de tais informações para qualquer outra entidade, de maneira estruturada

## Direito ao **CONHECIMENTO**

As consequências em relação a possível negativa de consentimento por parte do Titular

## Direito à **INFORMAÇÃO**

Informação de que a empresa realizou compartilhamento dos dados

## Direito à **ELIMINAÇÃO**

A eliminação de seus dados

## Direito à **REVOGAÇÃO**

Revogar o consentimento fornecido anteriormente















## **ENTRE EM CONTATO:**

Rosati Advocacia Empresarial  
OAB/RS 5.404 OAB/SP 446.737  
Débora Rosati - (54) 99165-2250  
Instagram @rosatiadvempresarial  
contato@rosatiadvocacia.com.br

## **CONHEÇA O ESCRITÓRIO:**

[www.rosatiadvocacia.com.br](http://www.rosatiadvocacia.com.br)



LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS -  
GUIA PRÁTICO DE IMPLEMENTAÇÃO PARA STARTUPS, MICRO E  
PEQUENAS EMPRESAS

