CARTILHA

Lei Geral de Proteção de Dados Pessoais

Uma colaboração entre:

Governo Britânico & Felsberg Advogados

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

FELSBERG
ADVOGADOS

Índice

Lei Geral de Proteção de Dados Pessoais - **LGPD**

- A **Lei nº 13.709/18** está em vigência desde 18.09.2020 e objetiva:
  - trazer maior **rigor aos que processam** dados pessoais ou sensíveis
  - proteger os direitos fundamentais de liberdade e privacidade dos indivíduos
  - impor **medidas técnicas e administrativas** às organizações atuantes na cadeia de tratamento dos dados.

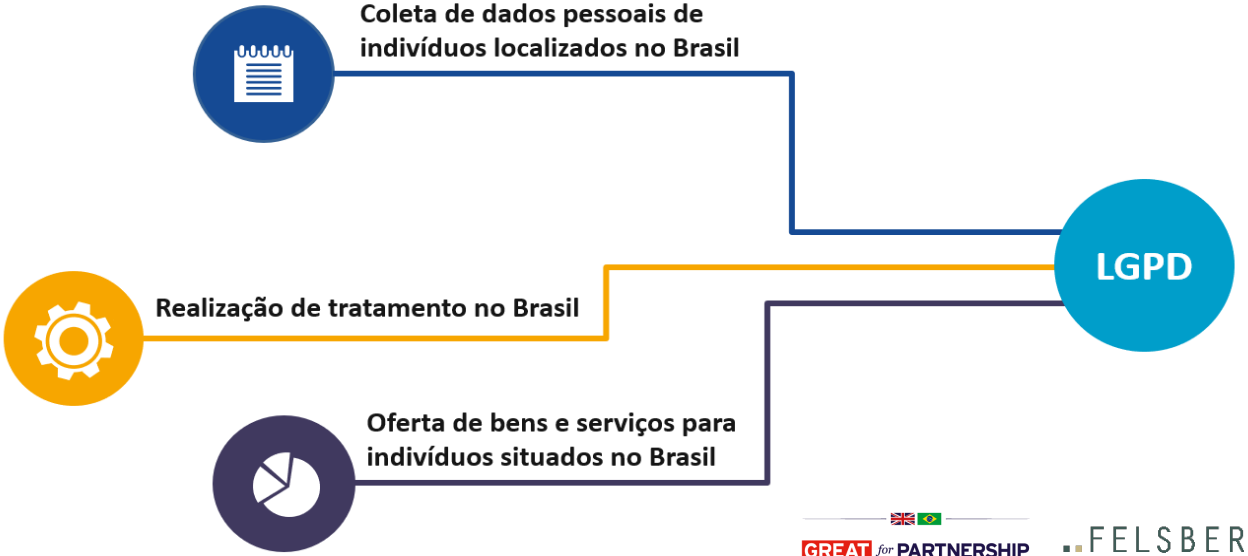
Os **direitos dos titulares** (como exclusão e portabilidade) com curto prazo de cumprimento (15 dias), o provável excesso de judicialização e o dever de prestação de contas (*accountability*), tornam inevitável a **adequação** e planos de governança em organizações públicas e privadas.

Conceitos da **LGPD:**

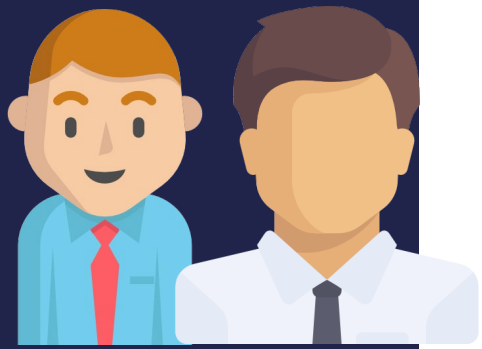
Quem deve se adequar à Lei?

- ✓ pessoas jurídicas de direito público ou privado, de pequeno, médio ou grande porte, **startups, fundações, associações, multinacionais, empresas estrangeiras**

- ✓ que realizem o *tratamento* de dados pessoais ou sensíveis (tratamento inclui um mero acesso a dados, ou coleta, compartilhamento, armazenamento, transferência etc.) em uma das três hipóteses da ilustração abaixo:



Conceitos da **LGPD:**



O que são Dados Pessoais?

Informações que podem vir a identificar uma pessoa física (*titular* dos dados), direta ou indiretamente. Ao contrário do que alguns pressupõe, o consentimento não será um pressuposto para a sua coleta ou utilização. A LGPD prevê 10 bases legais, sem qualquer hierarquia entre elas, como possibilidades a autorizar o processamento dessas informações, de acordo com a hipótese e sua finalidade.

Exemplos de dados pessoais:

- Nome
- Estado civil
- Profissão
- Data de nascimento
- CPF
- Identidade
- Endereço
- Dados bancários e financeiros
- Posts em mídias sociais
- Telefone
- Senhas
- E-mails
- IP
- Placa do carro
- Cookies
- Geolocalização
- Dados para definição de perfil comportamental ou padrões de consumo
- Metadados

Conceitos da **LGPD:**

E no que consistem Dados Sensíveis?

Esta categoria especial de dados pessoais refere-se às informações capazes de gerar maior discriminação aos titulares.

A Lei prevê menos bases legais para o tratamento destes dados (apenas oito) e regras mais rígidas de tratamento, assim como medidas adicionais para a adequação.

O rol dessa categoria é limitado aos dados pessoais referentes a:

- saúde
- vida sexual ou orientação sexual
- informações genéticas ou biométricas
- origens racial ou étnica
- opinião política
- convicção religiosa
- filiação a sindicatos, organização religiosa, filosófica ou política

Dúvidas sobre a legitimidade do tratamento? Observe se os **princípios** estão sendo **respeitados**:

Finalidade, Adequação e Necessidade: propósitos legítimos, específicos e informados, sem alteração posterior; minimização de dados.

Livre acesso e Transparência: consulta facilitada e gratuita sobre a forma e duração do tratamento, com informações claras; respeitado o segredo de negócio.

Qualidade dos dados: exatidão, clareza, relevância e atualização dos dados.

Segurança e prevenção: dever de adoção de medidas técnicas e administrativas para evitar danos, acessos indevidos e vazamentos.

Responsabilização e prestação de contas: devem ser armazenados os registros sobre as atividades de tratamento e as medidas de adequação à norma, comprovando-se sua eficácia.

Não discriminação: tratamento jamais poderá ter fins discriminatórios, ilícitos ou abusivos.

Sobre os Direitos dos Titulares de Dados

– suas solicitações devem ser respondidas, e se necessário atendidas, em até 15 dias:

- Confirmação do tratamento, acesso às informações tratadas e com quais entidades foram compartilhadas.
- Eliminação de dados desnecessários, excessivos, ilícitos ou tratados com base no consentimento.
- Retificação. Correção de dados incompletos, inexatos ou desatualizados.
- Revogação do consentimento – este é um dos motivos que dificulta o gerenciamento de dados processados com base no consentimento.
- Portabilidade dos dados para outro fornecedor de serviço ou produto. Trata-se de direito semelhante à portabilidade de linhas telefônicas.
- Informação ao titular sobre a possibilidade de não fornecer seu consentimento e quais seriam as consequências disso.

Como justificar o uso de dados de acordo com a LGPD?

Bases Legais

- A LGPD não proíbe o acesso a dados
- O consentimento é apenas uma das **10** hipóteses que autorizam o uso de dados pessoais, sem qualquer nível de hierarquia entre elas.
- Qualquer operação realizada com dados pessoais, no entanto, deve estar respaldada em uma das bases legais previstas.

Outras Bases Legais que autorizam o uso de Dados Pessoais:

- Obrigações legais;
- Legítimo interesse;
- Estudos por órgãos de pesquisa;
- Defesa em processos;
- Proteção da vida;
- Tutela da saúde por profissionais do ramo;
- Proteção do crédito (principalmente por instituições financeiras);
- Prevenção à fraude
- Políticas públicas

⚠ Pontos de atenção da LGPD:

Dados Sensíveis e de Menores

Há regras e bases legais específicas para o tratamento dessas informações, portanto deve-se estar atento quando do acesso, coleta ou outro tipo de tratamento destas categorias de dados.

Incidentes de Segurança

O controlador deve comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular sobre incidente de segurança (acesso ou uso indevido) que possa acarretar risco ou dano relevante ao titular.

Multas e penalidades

As sanções administrativas da LGPD incluem multa de até 2% do faturamento anual da empresa, limitada a R$ 50 milhões por infração, advertências, bloqueio ou eliminação da base de dados, e publicização do ilícito. Portanto, danos reputacionais podem ser mais graves do que a multa.

⚠ Pontos de atenção da LGPD:

Mailing, newsletter, marketing, <u>não</u> prescindem, necessariamente, de consentimento:
Em linhas gerais, para fins de marketing, ações promocionais, divulgações de eventos, captação, a base legal poderá ser o legítimo interesse. Afasta-se o consentimento, contanto que se tenha transparência sobre o que é feito com os dados e sejam respeitadas a LGPD e seus princípios. Deve-se incluir meios facilitados de *opt-out* em todas as comunicações (descadastramento).

Prestadores e Fornecedores:
dar preferência a fornecedores adequados à LGPD; incluir acordo com cláusula de proteção aos dados pessoais compartilhados, para limitar responsabilidades, estabelecer padrões de conduta e garantir penalidades por descumprimento

Medidas internas obrigatórias:
colaboradores devem estar aptos e vinculados às medidas de proteção, que incluem governança com políticas corporativas de privacidade e segurança, plano de resposta a incidentes, método para cumprimento aos direitos de titulares no prazo legal.

Setores Público e Privado na LGPD

Principais pontos da LGPD:	Diferenças na aplicação entre Setor Público x Setor Privado
Bases Legais	O Setor Público pode utilizar bases legais adicionais como “execução de políticas públicas”, inclusive para o compartilhamento de dados sensíveis.
Direitos dos Titulares	Mesma aplicação do Setor Privado, exceto quanto ao prazo de atendimento às solicitações dos titulares, que deve observar legislação específica (ex.: Lei do Habeas Data, Lei Geral do Processo Administrativo e Lei de Acesso à Informação).
Transferência Internacional de Dados	Pessoas jurídicas de direito público podem requerer à ANPD a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

LGPD x GDPR | Principais diferenças

Ainda que a empresa já esteja adequada ao GDPR, será necessário ajustar pontos fundamentais para que esteja em conformidade com a legislação brasileira, a começar por treinamentos dos colaboradores tendo em vista as diferenças a seguir:

Principais pontos:	Diferenças entre GDPR e LGPD
Bases Legais **Marketing** **Cookies**	Na LGPD, há 4 hipóteses adicionais para o processamento: órgãos de pesquisa, proteção da saúde, proteção do crédito, defesa em processo e prevenção à fraude. A empresa já adequada ao GDPR deve rever registros de atividades, políticas de privacidade, contratos, DPAs, *intercompany agreements*, para a adequação destes a essa realidade. Apesar de muitos sites atuarem em contrário, o legítimo interesse é menos restritivo que o GDPR, principalmente em ações de marketing. O Brasil não prevê, como na ePrivacy Directive europeia, dever de consentimento ou banners de *cookies*.
Direitos dos Titulares	A empresa adequada ao GDPR deve reorganizar seu plano de resposta a incidentes de segurança e gerenciar o atendimento às solicitações de titulares no prazo, mais curto, da LGPD
Encarregado (DPO)	Ao contrário do GDPR, que caracteriza três situações para indicação do DPO, por enquanto a LGPD determina que operadores e controladores apontem seu Encarregado, sendo provável que a ANPD elabore diretrizes a respeito.
Conclusão	Medidas a serem adotadas por empresas já adequadas ao GDPR: (i) ajuste do registro de atividades de tratamento para adequar bases legais, reanalisar riscos e *gaps*; (ii) revisão de contratos, documentos e políticas de privacidade e segurança, e (iii) nomeação do Encarregado, que pode ser pessoa física ou jurídica, mas fluente na língua portuguesa.

Medidas urgentes de adequação à LGPD:

- Treinamento de conscientização dos colaboradores sobre a LGPD
- Indicação de encarregado (DPO)
- Adequação de contratos de trabalho, prestação de serviços, parcerias
- Políticas de privacidade
- Estrutura para atendimento aos direitos dos titulares em até 15 dias
- Plano de resposta a incidentes de segurança

Uso indevido de dados e incidentes de segurança já motivaram sanções no Brasil:

Banco Inter pagará R$ 1,5 milhão por vazamento de dados em acordo

POR FELIPE PAYÃO | @felipepayao · EM SEGURANÇA · 19 DEZ 2018 – 11H00

MPDFT SOLICITA EXPLICAÇÕES À VIVO SOBRE GUARDA E PROTEÇÃO DE DADOS DE CLIENTES

Publicado em 23 de Abril de 2019, às 16:56

03/12/2018 às 16h07

Marriott: Ministério Público investiga vazamento de dados de clientes

Oi é condenada em R$ 1,5 milhões por compartilhar dados pessoais sem autorização

4 de dezembro de 2017

26/01/2018 - 17H10 - ATUALIZADA ÀS 20H06 - POR ESTADÃO CONTEÚDO

Netshoes deverá avisar 2 milhões de clientes sobre vazamento de dados

Vazamento ocorreu devido à falha de segurança da empresa

Drogaria Araújo é multada em mais de R$ 7 milhões por condicionar descontos a fornecimento de CPF

Empresa foi condenada por condicionar descontos quando consumidor informa o CPF no ato da compra, sem dar informações adequadas sobre a abertura de cadastro.

Por G1 Minas — Belo Horizonte

05/12/2018 17h08 · Atualizado há 3 meses

GREAT for PARTNERSHIP

FELSBERG ADVOGADOS

Uso indevido de dados e incidentes de segurança já motivaram sanções no Brasil:

Justiça impede uso de câmera que coleta dados faciais em metrô em SP

Após ação do Idec, Justiça determina que empresa Via Quatro cesse coleta de dados de emoções de passageiros

18/09/2018 - Atualizado: 12/12/2018

Ministério da Justiça multa Hering por causa de reconhecimento facial

Imagens foram coletadas em loja da marca no Shopping Morumbi, em São Paulo

14.ago.2020 às 16h45

Senacon e Procon-SP notificam Serasa sobre vazamento de 220 milhões de CPFs

Vazamento de dados expôs 223 milhões de CPFs e 40 milhões de CNPJs; Serasa Experian nega ser a fonte das informações

Por Felipe Ventura
26/01/2021 às 17:56

Serasa deve indenizar consumidor por manter seu telefone em cadastro 27/04/2021

Reclame Aqui vira local de queixas sobre proteção de dados

574 reclamações contendo o termo "LGPD" foram feitas em março deste ano

Quinta-feira , 22 de Abril de 2021

STF suspende compartilhamento de dados de usuários de telefônicas com IBGE 7 de maio de 2020

Justiça cita LGPD e manda Mercado Livre suspender anúncio de venda de dados cadastrais

Convergência Digital ... 19/10/2020 ... Convergência Digital

Riscos Cibernéticos
Brasil no top-tier

- A LGPD impõe os deveres de responsabilidade e prestação de contas (accountability), portanto as empresas devem estar aptas a comprovar que adotaram medidas de segurança capazes de proteger os dados tratados, na medida de seus riscos.

Ciberataques: média no Brasil é de 733 ataques por semana por empresa

Convergência Digital ... 19/12/2019 ... Convergência Digital

Brasil é um dos países mais afetados por ransomware na América Latina

POR FELIPE PAYÃO | @felipepayao - EM SEGURANÇA - 14 JAN 2019 — 16H34

Verifique se você já foi vítima de vazamentos de dados internacionais em: **https://haveibeenpwned.com**

Danos reputacionais por vazamentos podem ser mais prejudiciais que penalidades...

ESTUDO IBM | INSTITUTO PONEMON 2020

Perda de Negócios

Do custo médio de um vazamento de dados, 40% correspondem à perda de negócios:

- Perda de receita devido à paralisação do sistema
- Aumento da rotatividade dos clientes
- Aumento de custos para adquirir novos clientes

Brasil – Alto risco de vazamentos

Demora na identificação e contenção: 380 dias
(265 dias para identificar e 115 dias para conter)

Organizado em parceria entre:

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

FELSBERG
ADVOGADOS

CARTILHA

Lei Geral de Proteção de Dados Pessoais - LGPD