

# Guia LGPD

O melhor caminho  
para a conformidade

Julho de 2021

# Apresentação

A sociedade contemporânea é marcada pelo rápido desenvolvimento e transformação da tecnologia da informação. A capacidade de processamento de um grande volume de dados (*big data*) é um dos principais ativos empresariais, de onde se extrai perfis de consumo, possíveis mercados, tendências, análises de risco, dentre outras infinitas variáveis. Segundo o jornal *The New York Times*<sup>1</sup> e as revistas *The Economist*<sup>2</sup> e *Wired*<sup>3</sup>, vivemos a era em que os dados valem mais que o petróleo.

Essa evolução tecnológica trouxe também políticas corporativas agressivas em relação ao uso de dados pessoais. Tais excessos fizeram surgir uma necessidade de regulação. A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), fundamentada no direito à privacidade<sup>4</sup> e criada à semelhança da *General Data Protection Regulation* europeia, é um resultado disso, e traz regras sobre o tratamento de dados no Brasil, como hipóteses que autorizam o tratamento dos dados, princípios, direitos e obrigações. A lei entrou em vigor no dia 18 de setembro de 2020. As sanções previstas, por sua vez, poderão ser aplicadas a partir do dia 1º de agosto de 2021<sup>5</sup>.

O presente material traz os principais aspectos, recomendações e informações sobre a lei. A sua leitura é essencial para aqueles que desejam não apenas se adequar à LGPD, mas também tornar esse *compliance* uma vantagem competitiva.

---

1 <https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>

2 <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

3 <https://www.wired.com/story/wired-guide-personal-data-collection/>

4 O primeiro ensaio sobre privacidade foi publicado na Revista de Direito da Universidade de Harvard por Samuel Warren e Louis Brandeis, no ano de 1890, e enfrentava o “direito de ser deixado só”. Há várias teorias sobre a origem do artigo. Uma delas é a de que, já naquela época, os avanços tecnológicos causavam grande preocupação com relação à privacidade. Uma dessas preocupações surgiu em 1884, quando a Eastman Kodak Company introduziu a “snap camera”, uma câmera fotográfica pequena e barata e, portanto, disponível ao público em geral, e que poderia registrar desautorizadamente momentos de privacidade, principalmente pela imprensa sensacionalista (SOLOVE, Daniel J. SCHWARTZ, Paul M. Information Privacy Law. 6th Edition. New York: Wolters Kluwer Law & Business, 2018. p. 49).

5 Até o fechamento desta edição do e-book, estava pendente de votação o PL nº 500/2021. Caso aprovado, poderá haver a postergação da aplicação das multas para o dia 1º de janeiro de 2022.

# /// Sumário

|  |    |  |    |
|--|----|--|----|
| / O que é a LGPD?                          | 4  | / Agentes de tratamento  | 12 |
| / O que são dados pessoais?                | 5  | / Sanções  | 15 |
| / A quem a lei se aplica?                  | 6  | / 7 motivos pelos quais<br>você deve se adequar                              | 16 |
| / O que é tratamento de<br>dados pessoais? | 7  | / Como se adequar  | 19 |
| / Princípios gerais                        | 8  | / A importância de um<br><i>compliance</i> adequado<br>ao perfil empresarial | 20 |
| / Bases legais                             | 9  |  |    |
| / Direitos dos titulares                   | 10 |  |    |

# / O que é a LGPD?

A Lei Geral de Proteção de Dados (Lei 13.709/2018) inaugura um regime geral de proteção de dados pessoais e complementa um conjunto de normas relacionadas ao tratamento da informação no país, ao lado da Lei de Acesso à Informação (Lei 12.527/2011), do Marco Civil da Internet (Lei 13.709/2018) e do Código de Defesa do Consumidor (Lei 8.078/1990).

A sua finalidade é a de tutelar o tratamento de dados pessoais no Brasil, a fim de “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (art. 1º, LGPD).

A sua principal inspiração é a GDPR (*General Data Protection Regulation* - EU 2016/679), regulamentação europeia sobre a proteção de dados, que está em vigor desde maio de 2018 e que estabelece regras aos estados membros da União Europeia para a coleta, armazenamento e compartilhamento de dados pessoais.

O propósito da LGPD, assim como o da GDPR e de outras legislações que tratam do assunto, é o de basicamente proporcionar a proteção dos dados pessoais das pessoas físicas, de forma a garantir seus direitos e impor obrigações às corporações que realizam o tratamento de seus dados.

# / O que são dados pessoais?

Para a LGPD, são considerados dados pessoais e protegidos pela lei as informações que identificam ou possam identificar uma pessoa natural, como, por exemplo: **RG**, **CPF**, **endereço** (físico e eletrônico), **IP** e **imagens**.

São também considerados pessoais e denominados sensíveis, ou seja, com uma proteção ainda mais rigorosa da lei, os dados relacionados à origem racial ou étnica, à convicção religiosa, à opinião política, à filiação a sindicato, à organização de caráter religioso, filosófico ou político e os referentes à saúde ou vida sexual, genéticos ou biométricos.

# / A quem a lei se aplica?

A lei se aplica a qualquer pessoa (natural ou jurídica de direito público ou privado) que realize o tratamento de dados pessoais e que preencha, ao menos, uma das seguintes hipóteses:

- a. possuir estabelecimento no Brasil;
- b. oferecer serviços ao mercado brasileiro;
- c. coletar e tratar dados de pessoas localizadas no Brasil.

Para a LGPD, pouco importa o meio pelo qual é realizado o tratamento de dados, o país onde se situa a sede da empresa, a localização dos dados e a nacionalidade dos titulares dos dados. Se a empresa se enquadrar em uma das hipóteses antes mencionadas e realizar o tratamento de dados pessoais, deverá respeitar as suas regras.

A lei também não se restringe a dados coletados por meios eletrônicos. Aqueles constantes em documentos físicos também são protegidos pela LGPD.

# / O que é tratamento de dados pessoais?

É toda e qualquer operação realizada com dados pessoais. A LGPD faz questão de exemplificar algumas modalidades de operação (art. 5º, Inciso X).

São elas:

- Coleta;
- Produção;
- Recepção;
- Classificação;
- Utilização;
- Acesso;
- Reprodução;
- Transmissão;
- Distribuição;
- Processamento;
- Arquivamento;
- Armazenamento;
- Eliminação;
- avaliação ou controle da informação;
- Modificação;
- Comunicação;
- Transferência;
- Difusão ou extração.



# / Princípios gerais

Além da boa-fé, a LGPD identificou, em seu art. 6º, os demais princípios que devem nortear toda e qualquer atividade de tratamento de dados. São eles:

- **(i) finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular.
- **(ii) adequação:** compatibilidade do tratamento com as finalidades informadas ao titular.
- **(iii) necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades.
- **(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, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
- **(vi) transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
- **(vii) segurança:** utilização de medidas 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.
- **(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.



# / Bases legais

De acordo com a LGPD, o tratamento de dados deverá, obrigatoriamente, estar enquadrado em uma das dez hipóteses previstas em seu art. 7º, denominadas bases legais. Ou seja, o tratamento somente será considerado legítimo se estiver em harmonia com referidas bases legais e ocorrer:

- (i) mediante o fornecimento de **consentimento** pelo titular.
- (ii) para o **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** previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.
- (iv) para a realização de estudos por **órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais.
- (v) quando necessário para a **execução de contrato** ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.
- (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 procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária.
- (ix) quando necessário para atender aos **interesses legítimos** do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção.
- (x) para a **proteção do crédito**.

# / Direitos dos titulares

Um dos principais propósitos da lei é o de proteger o titular e garantir com que ele tenha maior autonomia sobre os seus dados, além de transparência e clareza em relação ao tratamento.



São direitos do titular, previstos no art. 18 da LGPD:

- **(i)** a confirmação da existência de tratamento do seu dado.
- **(ii)** o acesso aos seus dados.
- **(iii)** a correção de dados incompletos, inexatos ou desatualizados.
- **(iv)** a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei.
- **(v)** a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.
- **(vi)** a eliminação dos dados pessoais tratados com o seu consentimento, exceto nas hipóteses previstas no art. 16 da LGPD.
- **(vii)** a informação sobre o uso compartilhado de seus dados com entidades públicas e/ou privadas.
- **(viii)** a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
- **(ix)** a revogação do consentimento.

Em síntese, as principais provisões com relação aos titulares do dado são:

- a.** o direito de saber que tipo de informação foi coletada, e qual o uso da referida informação;
- b.** o direito de saber se a sua informação está sendo compartilhada com outras pessoas;
- c.** o direito de acessar o dado e levá-lo para outro lugar (“portabilidade”);
- d.** o direito, em algumas situações, de ter o seu dado eliminado.

Além disso, na eventualidade de sofrer algum tipo de prejuízo patrimonial ou moral em razão do tratamento inadequado de seus dados, o titular terá direito à reparação civil, conforme estabelece o art. 42 da lei.

# / Agentes de tratamento

A Lei Geral de Proteção de Dados caracterizou como agentes de tratamento duas pessoas específicas: o controlador e o operador (art. 5º, inciso IX, da LGPD).

O controlador é o responsável pela tomada de decisões sobre o tratamento de dados pessoais<sup>6</sup>. O operador, por sua vez, realiza o tratamento dos dados pessoais a pedido do controlador (art. 5º, inciso VII, da LGPD) ou por força de lei. Ambos podem ser pessoas naturais ou jurídicas, de direito público ou privado (art. 5º, incisos VI e VII, da LGPD).

<sup>6</sup> VAINZOF, Rony. Disposições preliminares. *LGPD – Lei Geral de Proteção de Dados Comentada* / Viviane Nóbrega Maldonado, Renato Ópice Blum, coordenadores – São Paulo: Thomson Reuters Brasil, 2019. p. 105.

O quadro abaixo traz o detalhamento das atribuições e obrigações de cada um dos agentes, segundo a LGPD:

## CONTROLADOR

- Deve observar o enquadramento de ao menos uma das bases legais para cada tratamento de dados (arts. 7º e 11, da LGPD).
- Acompanha o ciclo de vida dos dados, determinando o descarte quando do término do tratamento.
- Indica o encarregado (arts. 5º, inciso VIII e 41, da LGPD).
- Elabora o relatório de impacto à proteção de dados pessoais (art. 5º, inciso XVII, da LGPD).
- Suporta o ônus da prova sobre o consentimento do titular (art. 8º, §2º, da LGPD).
- Deve cumprir os direitos dos titulares (art. 18, da LGPD).
- Adota as medidas aptas a demonstrar a observância às normas de proteção de dados (art. 6º, inciso X, da LGPD).
- Comunica à ANPD e o titular dos dados em caso de incidente que possa gerar risco ou dano relevante aos titulares (art. 48, caput, da LGPD).

## OPERADOR

- Trata dados pessoais, a pedido/em nome do controlador (art. 5º, inciso VII).
- Adota as medidas aptas a demonstrar a observância às normas de proteção de dados (art. 6º, inciso X, da LGPD).
- Responde solidariamente pelos danos causados a terceiros, na hipótese de descumprimento das normas de proteção de dados ou não atendimento às instruções lícitas do controlador (art. 42, §1º, inciso I, da LGPD).
- Presta informações, quando solicitadas pela ANPD (art. 55-J, inciso IV, da LGPD).

Aos agentes de tratamento é também atribuído o dever de adotar todas as medidas necessárias a proteger os dados pessoais que lhe forem conferidos de acessos não autorizados, de situação acidental ou ilegal, de perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito dos dados pessoais (art. 46, da LGPD).

Como já visto, a LGPD previu, ainda, a responsabilização civil dos agentes de tratamento, quando a atividade ocasionar prejuízos materiais ou morais aos titulares (art. 42).



# / Sanções

As infrações à Lei Geral de Proteção de Dados poderão ensejar as seguintes sanções administrativas (art. 52): multa (que pode chegar a 2% do faturamento, limitada a 50 milhões de reais, por infração), multa diária, publicização da infração cometida e bloqueio do uso ou eliminação dos dados relacionados à infração.

As sanções não estão diretamente relacionadas a um vazamento de dados ou a um incidente de segurança da informação, podendo resultar de qualquer infração aos regramentos previstos na LGPD, como o tratamento irregular dos dados.

O órgão responsável pela fiscalização e aplicação de sanções aos agentes de tratamento de dados é a Autoridade Nacional de Proteção de Dados, criada pela Lei 13.853/19. Este órgão também poderá exigir a apresentação de relatórios e informações, como também aplicar eventuais penalidades. É possível afirmar, ainda, que em situações envolvendo o direito de consumidor, órgãos de defesa do consumidor, como o PROCON, também terão legitimidade para fiscalizar o cumprimento da lei.

# / 7 motivos pelos quais você deve se adequar

Arrolamos abaixo sete motivos pelos quais entendemos que as empresas devem se adequar às normas de proteção de dados, em especial à LGPD:

1. A legislação impõe uma série de direitos aos titulares dos dados, os quais irão requerer, cada vez mais, produtos, sistemas e serviços adequados, sob pena de optarem por empresas que priorizam e são transparentes com relação ao uso de seus dados e à privacidade<sup>7</sup>.
2. A adequação é uma boa oportunidade para rever a política de governança de dados e, mais do que isso, promover um sistema de valores e princípios morais relacionados à coleta, uso e compartilhamento responsável de dados, a denominada “ética digital”. Ou seja, dá ensejo a uma verdadeira mudança cultural corporativa, que permitirá com que as empresas sobrevivam a essa (re)evolução social brasileira em relação à cultura da privacidade.

<sup>7</sup> Estudo realizado pela *Accenture Creative* em 2019 com 8 mil consumidores no Canadá, França, Alemanha, Itália, Espanha, Suécia, Reino Unido e EUA identificou que “73% dos consumidores dispõem-se a compartilhar mais informações pessoais, desde que as marcas sejam mais transparentes quanto ao modo de uso” - *Consumer Pulse Survey 2019*. Disponível em: <http://https://www.accenture.com/br-pt/insights/digital/see-people-not-patterns>. Acesso em 9 de Março de 2020.

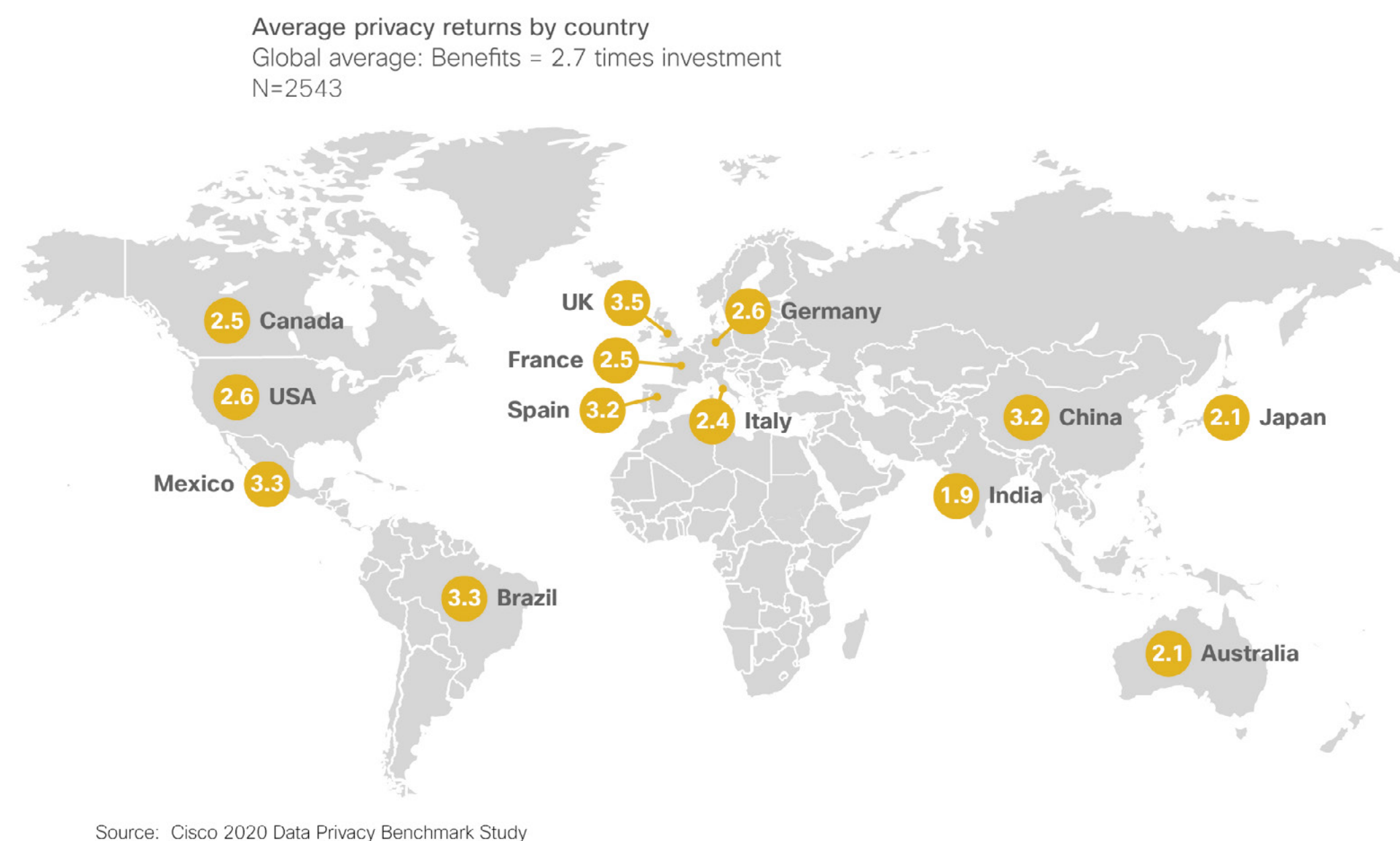
**3.** O processo de conformidade permite a revisão da segurança digital da empresa, aspecto fundamental em um mundo em que o vazamento de dados se tornou tão corriqueiro. A adoção de precauções (em consonância com o estado atual da técnica) possibilita minimizar e até mesmo isentar eventuais responsabilidades e sanções.

**4.** Além de prevenir a multa pecuniária prevista na LGPD (que pode chegar a 2% do faturamento, limitada a 50 milhões de reais, por infração) e eventual responsabilização civil, a conformidade busca evitar, também, a imposição das demais sanções previstas, como a publicização da infração, o bloqueio e, inclusive, a eliminação dos dados pessoais a que se refere a infração. São medidas que, além de esfacelar determinados modelos de negócios, podem arruinar reputações.

**5.** Portanto, o *compliance* com a LGPD possibilita a proteção da reputação da empresa, na medida em que a publicização de um eventual vazamento ou tratamento indevido de dados gera prejuízos imensuráveis à imagem.

**6.** Para as empresas de tecnologia, especialmente as em estágio inicial (*startups*), que buscam a atração de investidores e competitividade, estar em conformidade com a lei é um grande atrativo e um ótimo posicionamento frente ao mercado.

7. Pode-se afirmar que a conformidade com as normas de proteção de dados, em especial a LGPD, é um importante diferencial competitivo, que impulsiona novos negócios ao garantir transparência e respeito em relação ao titular do dado. O estudo *2020 Data Privacy Benchmark*, realizado pela CISCO, destaca que, a cada dólar investido em privacidade, as empresas que participaram da referida pesquisa receberam, em média US\$ 2,70 de retorno, considerando benefícios diretos e indiretos (principalmente, o aumento da vantagem competitiva, o maior envolvimento dos investidores e a confiança dos clientes). O estudo destaca, ainda, que o segundo melhor ROI ficou com as empresas brasileiras (US\$ 3,3). Veja o desempenho geral no mapa abaixo<sup>8</sup>:



8 2020 *Data Privacy Benchmark*. CISCO. Disponível em: [http://https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf?utm\\_source=The+Shift+Newsletter&utm\\_campaign=e1d0a751b0-THESHIFT\\_IA\\_2019\\_11\\_27\\_COPY\\_01&utm\\_medium=email&utm\\_term=0\\_7f93052ef8-e1d0a751b0-49045267](http://https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf?utm_source=The+Shift+Newsletter&utm_campaign=e1d0a751b0-THESHIFT_IA_2019_11_27_COPY_01&utm_medium=email&utm_term=0_7f93052ef8-e1d0a751b0-49045267). Acesso em 9 de Março de 2020.



# / Como se adequar

A adequação às normas de proteção de dados dependerá do modelo de negócio e do grau de maturidade da empresa em relação à privacidade e à segurança da informação. De todo modo, dois pontos são comuns para os que pretendem se adequar:

- a.** é fundamental o envolvimento de todos os setores da empresa, principalmente o engajamento do corpo diretivo;
- b.** a aplicação de uma metodologia própria, desenhada para atender as necessidades específicas da empresa, é fundamental para uma efetiva adequação.

A seguir, faremos uma breve análise dos principais passos para a adequação:

- **Data Mapping;**
- **Implementação;**
- **Relatório de impacto;**
- **Monitoramento.**

# / A importância de um *compliance* adequado ao perfil empresarial

A experiência prática vem nos mostrando que a aplicação de uma metodologia adequada ao perfil e modelo de cada empresa torna o programa de *compliance* à LGPD muito mais eficaz.



Portanto, ao realizar o seu projeto, considere os seguintes passos:

- a.** *workshop*, para alinhar e sensibilizar a equipe e formar um grupo que estará na linha de frente dos trabalhos de adequação;
- b.** diagnóstico, mediante uma análise técnica e jurídica, através de um levantamento de todo o ambiente organizacional e entrevistas com os setores (*data mapping*);
- c.** auditoria contínua, através do acompanhamento da evolução do ambiente organizacional e da avaliação de não conformidades e ações sugeridas;
- d.** a realização periódica de treinamentos relacionados à adequação e a entrega de “pílulas” de conscientização, o que pode ser feito em infinitos formatos;
- e.** a realização constante de análises de vulnerabilidades, a fim de identificar gargalos técnicos que evidenciem riscos aos dados;
- f.** a nomeação de um encarregado de dados;
- g.** a adoção da certificação ISO 27001 e extensões.

Por último, **confie sempre a um especialista sobre o universo da privacidade e proteção de dados a liderança do seu projeto de adequação**. A presença de um *expert* possibilita um olhar estratégico, que vai além dos aspectos básicos da legislação, passando pela compreensão do negócio, pelo mapeamento dos riscos e oportunidades ligados ao *compliance*, para, finalmente, converter essa transformação organizacional em verdadeira vantagem competitiva.

# Equipe / Privacidade e Proteção de Dados



**Rodrigo de Assis Horn**  
Sócio CAO Mosimann-Horn

[rodrigo@mh.adv.br](mailto:rodrigo@mh.adv.br)

[Bio](#)



**Thays Joana Tumelero**  
Sócia Mosimann-Horn

[thays.tumelero@mh.adv.br](mailto:thays.tumelero@mh.adv.br)

[Bio](#)

Conhecimento  
em **evolução** por  
relações completas

MOSIMANN-HORN  
A D V O G A D O S

SEDE

**FLORIANÓPOLIS**  
Praça Pereira Oliveira, 64 - 3º Andar  
88010-540 | Santa Catarina - SC

CONTATO

E-mail: [contato@mh.adv.br](mailto:contato@mh.adv.br)  
Fone: +55 48 32223738  
[www.mh.adv.br](http://www.mh.adv.br)

[www.mh.adv.br](http://www.mh.adv.br)