# Privacidade e Proteção de Dados LGPD

EY

Building a better working world

# INTRODUÇÃO

# 1 SUMÁRIO EXECUTIVO

Escrevemos hoje para você que já tomou conhecimento da **Lei nº13.709/18**, a **Lei Geral de Proteção de Dados Pessoais (LGPD)**, inspirada na lei Europeia GDPR, mas ainda está confuso sobre o que realmente deve ser feito para cumprir o novo regulamento, uma vez que têm tomado conhecimento de soluções bem distintas oferecidas por escritórios de advocacia, por fornecedores de software e hardware, integradores e consultorias.

A melhor forma que encontramos para tornar esse texto útil para você foi conduzindo-o por um roteiro de estória que o permita responder à pergunta sozinho no final. Para isso, vamos começar pelo começo.

**Tem obrigatoriedade definida.**

- Sendo uma lei Federal sancionada pelo Congresso Nacional, ela precisa ser observada com o rigor de obrigatoriedade relacionada ao escopo, requisitos, direitos e responsabilidades de todos que se enquadrem na definição de pessoa natural ou pessoa jurídica de direito público ou privado que realize tratamento de dados pessoais, inclusive nos meios digitais.

**Tem escopo legal definido.**

- "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."





**Tem prazo de cumprimento definido.**

- A Lei entrou em vigor em 18 de agosto de 2020, fazendo com que todas as organizações atingidas pelo escopo da lei demonstrem conformidade e estejam sujeitas as sanções a partir de 1º. de agosto de 2021.

**Tem sanções administrativas definidas.**

- A lista de penalidades começa com advertência e segue com multa simples de 2% do faturamento limitado a 50 milhões por infração, multa diária e publicação da ocorrência.

**Tem escopo técnico definido, contudo...**

- A grande maioria das empresas não tem maturidade e os alicerces mínimos de governança e gestão de riscos de segurança da informação para tratar a LGPD apenas como uma evolução incremental na direção da privacidade dos dados. Essa condição muda completamente o esforço, a complexidade e a viabilidade técnica para se atingir a conformidade nessas empresas.

  A lei é abrangente demais para que se exija seu cumprimento à empresas de qualquer porte e com qualquer nível de maturidade de governança de dados e segurança da informação, indiscriminadamente.

  As sanções administrativas parecem incompatíveis com temporalidade da lei e desproporcionais à real capacidade do governo de fiscalizar e das empresas de se adequarem em plenitude e eficazmente ao seu escopo técnico.

  Boa parte dos fornecedores, por sua vez, influenciados pelos equívocos descritos nos itens anteriores e ainda assim

motivados a apoiar os clientes oferecendo-lhes soluções, caem na armadilha de suas especificidades. Demonstram só ter olhos para os propósitos e problemas para os quais foram criados, fatiam o desafio da lei que é muito mais amplo, e oferecem pseudo-soluções que só arranham a superfície do problema, gerando uma falsa sensação de conformidade plena.

Não há, de fato, outro culpado pelo que vemos acontecer, senão a falta de educação, maturidade e compreensão do que vem a ser gerir eficientemente a segurança da informação de uma empresa. O problema é multifacetado, deve ser enxergado e gerenciado de forma integrada, ou seja, conectando o negócio aos agentes externos de seu ecossistema; conectando processos de negócio aos ativos físicos, tecnológicos e humanos; conectando diretrizes, normas e procedimentos aos controles; conectando governança, proteção, identificação, detecção e resposta às ameaças, à *frameworks* de gestão de riscos da informação.

> *"Se encarássemos o Sistema de Gestão de Segurança da Informação como um edifício, poderíamos, analogamente, associar o LGPD à exigência de construção de um novo pavimento. Entretanto, para que isso fosse possível, os alicerces estruturais do edifício já deveriam ter sido dimensionados e os fundação bem construída para suportar a nova carga. Quando isso não acontece, será preciso construir ou reconstruir fundação, os primeiros pavimentos, para só então ser capaz de atender os novos requerimentos legais da Lei Geral de Proteção de Dados."*





**Vinte anos em dois.**

- Se observarmos com cuidado e interesse a estrutura da LGPD, veremos se tratar de um embrulho atualizado e mandatório por força de lei - voltado especificamente à proteção de Dados Pessoais Sensíveis[*1] - de um Sistema de Gestão de Segurança da Informação completo, como aquele especificado pelas velhas normas BS7799, ISO17799 e a ISO27001.

Na prática, significa dizer que as empresas terão de avaliar, especificar, implementar e gerenciar um modelo de governança corporativo de riscos de segurança da informação que não conseguiram fazer em vinte anos[*2], em apenas dois.

Obviamente que essa situação crítica e complexa se torna bem diferente para as organizações mais maduras e que já tem governança instalada e um modelo abrangente de gestão de segurança da informação, onde plugar ou aprimorar a abordagem de privacidade por força da nova lei passa a ser apenas mais um passo na evolução incremental do que já tinha sido feito até então.

**1** Dados Pessoais Sensíveis: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

**2** Vinte anos. Tempo médio decorrido desde que Marcos Sêmola, sócio da EY - Cybersecurity, começou a estudar o mercado de segurança da informação, publicou o primeiro livro e, portanto, passou a notar o gap entre as recomendações das normas especialistas e a maturidade do mercado, deixando evidente a dificuldade que é implementar um sistema de gestão de segurança da informação em sua plenitude.

**A lei é clara.**

- **O que:** Tratamento de Dados Pessoais. Toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

- **Atividades de tratamento:**
  **Finalidade:** propósitos legítimos, específicos, explícitos e informados ao titular.

  **Adequação:** compatibilidade do tratamento com finalidades informadas ao titular.

  **Necessidade:** limitação ao mínimo necessário para realização de suas finalidades.

  **Livre Acesso:** garantia, aos titulares, de consulta facilitada e gratuita.

  **Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados.

  **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis.

  **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger dados.

  **Prevenção:** adoção de medidas para prevenir ocorrência de danos face ao tratamento dos dados pessoais.

  **Não discriminação:** impossibilidade de realização do tratamento com fins discriminatórios.

  **Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar observância e cumprimento das normas de proteção de dados pessoais e eficácia dessas medidas.

- **Quando:**
  Mediante fornecimento de consentimento do titular;





Para cumprimento de obrigação legal ou regulatório pelo controlador;

Pela administração pública, para tratamento e uso compartilhado de dados necessários à execução de políticas públicas (sujeito às disposições do Cap. IV);

Para estudos por órgão de pesquisa, garantida, sempre que possível, anonimização dos dados pessoais;

Quando necessário para execução de contrato ou procedimento preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

Para exercício regular de direitos em processo judicial, administrativo ou arbitral;

Para proteção da vida ou da incolumidade física do titular ou terceiro;

Para tutela da saúde, em procedimento realizado por profissionais da área de saúde ou entidades sanitárias;

Quando necessário atender interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam proteção dos dados pessoais;

Para proteção do crédito.

- **Quem:** Pessoas físicas ou jurídicas, de direito público ou privado, que tratem dados pessoais no Brasil ou que coletem dados no Brasil ou, ainda, quando o tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços a titulares localizados no Brasil, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados.

- **Perfis:**
  **Titular:** Pessoa natural (física) a quem se referem os dados pessoais que são objeto de tratamento.

  **Controlador:** Pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais.

**Operador:** Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

- **Direitos do titular:**

Confirmar a existência de tratamento de seus dados pessoais;

Acessar seus dados pessoais;

Corrigir dados pessoais incompletos, inexatos ou desatualizados;

Anonimização, bloqueio ou eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD;

Portabilidade de dados pessoais a outro fornecedor de produto ou serviço;

Eliminação de dados tratados com o seu consentimento;

Obtenção deinformações sobre as entidades públicas e privadas com as quais o controlador realizou o compartilhamento de dados pessoais;

Obtenção de informações sobre a possibilidade de não consentir com o tratamento de dados pessoais e sobre as consequências da negativa;

Revogação do consentimento dado para o tratamento de dados pessoais.

- **Direitos de transferência internacional de dados:**

Para países que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD;

Quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro.

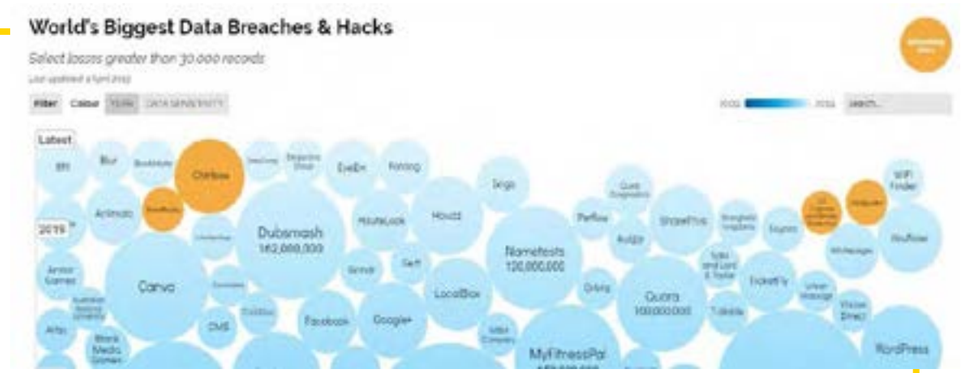
Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência.



# 2 MOTIVADORES PARA A CRIAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

**A sociedade e os negócios são "data driver" e os riscos relacionados ao uso indevido e vazamentos crescem exponencialmente**

**Causando impactos financeiros reais às organizações**





Facebook tem maior perda diária em valor de mercado da história dos EUA


Em dois dias, Facebook perde quase US$ 50 bilhões em valor de mercado

Nos últimos dois pregões, ações da empresa caíram mais de 9%, em meio a escândalo sobre vazamento de dados.


Netshoes paga indenização após vazamento

O Ministério Público do Distrito Federal e Territórios (MPDFT) firmou um termo de ajustamento de conduta (TAC) com a empresa Netshoes. O acordo foi proposto pela Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec) do MPDFT após o vazamento de dados de quase 2 milhões de clientes em 2018.

A empresa deverá pagar indenização de R$ 500 mil, que serão recolhidos mediante depósitos no Fundo de Defesa de Direitos Difusos (FDD). O inquérito civil aberto para investigar o caso ficará suspenso até a quitação do valor integral da indenização.

Segundo o acordo, a Netshoes também se compromete a implantar medidas adicionais ao seu Programa de Proteção de Dados, a realizar esforços de orientação de consumidores, a aumentar o nível de conhecimento sobre os riscos cibernéticos e medidas de proteção de seus dados pessoais, por meio de campanha de conscientização, e a disseminar ao mercado as melhores práticas para privacidade e proteção de dados pessoais.



2. MOTIVADORES PARA A CRIAÇÃO DA
LEI GERAL DE PROTEÇÃO DE DADOS

## Cambridge Analytica

O escândalo envolvendo a empresa Cambridge Analytica escancarou as graves consequências que podem advir do uso não autorizado e indevido de dados pessoais, que extrapolam o plano individual, ao ponto de repercutir nos rumos democráticas de uma nação, como se suspeita que tenha acontecido com a eleição do Presidente Donald Trump nos EUA e com a saída do Reino Unido da União Europeia. Ficou claro o impacto que a ausência de regras claras sobre o uso de dados e de uma autoridade que as aplique e supervisione pode ter. No Brasil, onde a empresa já pretendia atuar no futuro pleito eleitoral para a presidência da república por meio de oferecimento de conteúdos e propagandas direcionadas à eleitores, baseadas nos interesses inferidos dos seus dados pessoais, possivelmente coletados e utilizados de forma indevida, visando influenciar os seus votos, o escândalo teve tal repercussão que uma investigação foi aberta pelo Ministério Público para averiguar se realmente houve coleta e uso não autorizado de dados pessoais. Todavia, na ausência de uma lei geral, uma zona interpretativa cinzenta prevalece quanto à (i)legalidade no uso dos dados, uma vez que inexistiria, em alguns contextos, limitações claras ao tratamento destes. Desta forma, fica evidente a necessidade de uma LGPD.

## Organização para a Cooperação e Desenvolvimento Econômico – OCDE

O Brasil está a pleitear a sua entrada na Organização para a Cooperação e Desenvolvimento Econômico (OCDE, ou OECD, no seu original).
A organização foi uma das primeiras a especialmente lidar com a regulação do uso de dados pessoais, com foco principal nas transferências internacionais inerentes à muitos modelos de negócio. Suas primeiras orientações foram publicadas já em 1980 (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), atualizadas em 2013 para se adequar aos novéis da sociedade da informação, e influenciaram diretamente leis em inúmeros países, até mesmo a antiga diretiva europeia de proteção de dados e o futuro regulamento. Apesar dos seus guideline não terem força de lei, para que o países possam fazer parte da organização, eles devem se obrigar a cumprir com as regras estabelecidos por eles, inclusive às proteção de dados.
Entretanto, o Brasil, por carecer de uma lei geral ou de normas robustas, estava longe de cumprir com tais obrigações. Essa lacuna compeliu o Governo Federal e o Ministério das Relações Exteriores, por meio do seu Chanceler, Senador Aloysio Nunes, que também fora relator do PL de Dados do Senado, o antigo PL 330/2013, a apoiarem a aprovação da LGPD, como forma de facilitar a entrada do Brasil na OCDE.



2. MOTIVADORES PARA A CRIAÇÃO DA
LEI GERAL DE PROTEÇÃO DE DADOS

## Lei do Cadastro Positivo

Um outro ponto que foi essencial para a aprovação da LGPD no Congresso Nacional foi a tentativa de alteração da Lei do Cadastro Positivo, que regulamenta o banco de dados de adimplentes (bom pagadores, em conjunto com o Código de Defesa do Consumidor, que lida com o de mal pagadores), relatórios de crédito e algoritmos de risco de crédito. A lei, como vigente atualmente, determina que os dados de consumidores somente podem ser adicionadas à tais bases com o seu consentimento, prática conhecida como opt-in. A alteração pretendia, entre outros pontos, mudar essa lógica para permitir que os dados pessoais pudessem ser coletados, utilizados e compartilhados sem o consentimento do titular, permitindo a este, apenas, requisitar o cancelamento dos seus dados posteriomente, prática conhecida como opt-out. Essa alteração automaticamente incluiria os dados de mais de 30 milhões de brasileiros em sistemas geridos por empresas, o que poderia, alguns defendiam, alavancar a concessão de crédito no país, pois seria possível, em tese, efetivamente distinguir os bons pagadores dos maus.
Todavia, essa vantagem não viria sem riscos. Numa era de grandes vazamentos de dados e incontáveis casos de usos indevidos destes, permitir a aglomeração de dados pessoais de toda a população brasileira economicamente ativa sem que haja regras claras, transparentes, robustas e harmônicas que regulem tais usos pode ser uma prática indesejada e temerária. Esse cenário deu ensejo a toda uma leva de negociações políticas que culminaram na aprovação de um texto base alterando a Lei do Cadastro Positivo, mas bem diferente do original, com bem mais garantias, e a concordância do Presidente da Câmara dos Deputados, Rodrigo Maia, da necessidade de se ter uma lei geral de proteção de dados antes das alterações pretendidas no cadastro positivo. Esse acordo político foi um dos principais fatores que permitiram a aceleração do trâmite do PL 5276/2016 na Câmara, que recebeu a numeração de PLC 53/2018 após ser aprovado nesta casa e enviado para o Senado.

# 3 TIMELINE



**Visão geral dos principais aspectos da LGPD Brasileira:**

Motivada pela vigência da GDPR (*General Data Protection Regulation*), cujo impacto para as relações de negócios é considerável, o Brasil criou a LGPD (Lei Geral de Proteção de Dados) que tem como objetivo "organizar" a "colcha de retalhos" de regulações setoriais para proteção de dados já vigentes no Brasil.

**LGPD (Lei Geral de Proteção de Dados)**

**2014**
**abril**
Marco civil da Internet

**2016**
Envio de Projeto da LGPD à câmara

**2018**
**junho**
PLC 53/2018 aprovado pelo Senado

**2018**
**junho**
Proposta de Lei da Câmara nº 53/2018 apresentada ao Plenário do Senado Federal

*Vacatio Legis de 24 meses*

**2018**
**agosto**
LGPD sancionada, com vetos

**2019**
**julho**
Sancionada a LGPD com criação da Autoridade Nacional de Proteção de Dados - ANPD com 14 vetos

**2020**
**junho**
LGPD Vigente

## Aplicabilidade da LGPD

Aplica-se a operações de processamento de dados que ocorrem no território brasileiro, mas também a operações de processamento de dados ocorrendo fora do território quando:

- Dados pessoais são coletados no Brasil
- Os dados estão relacionados a indivíduos localizados no território brasileiro
- Os dados são utilizados com o objetivo de oferecer produtos e/ou serviços ao público brasileiro

**Qualquer dado relacionado à uma pessoa identificada ou identificável é um dado pessoal**





## Principais vantagens de uma Lei Geral de Proteção de Dados:

| | |
|---|---|
| **Unificar regras** | Regras únicas e harmônicas sobre o uso de dados pessoais, independente do setor da economia |
| **Maior flexibilidade** | Autorizar formas mais flexíveis para o tratamento de dados pessoais, tais como legítimos interesses, que levam em consideração uma sociedade movida à dados em tempos de Big Data |
| **Redução de custos** | Diminuir custos operacionais causados por incompatibilidades sistêmicas de tratamentos feitos por agentes diversos, além de fomentar uma maior qualidade dos dados em circulação no ecossistema como um todo |
| **Adequar as regras no Brasil** | Tornar o Brasil apto a processar dados oriundos de países que exigem um nível de proteção de dados adequados, o que pode fomentar, principalmente, os setores de tecnologia da informação |
| **Portabilidade** | Indivíduos poderão transferir seus dados de um serviço para outro, aumentando a competitividade no mercado |

Em **09 de Julho de 2019**, a LGPD foi sancionada com 14 vetos, dentre os quais,  destacam-se:

**LGPD sancionada**

**1. Agência Nacional de Proteção de Dados | ANPD**

Sancionada com vetos, a Lei 13.853/19, que cria a Autoridade Nacional de Proteção de Dados e faz outras alterações na Lei 13.709/18 (LGPD) relativas ao encarregado.

**1. ANPD**

**2. Artigo 52**

**2. Decisão automatizada**

Vetada a obrigação de que a revisão solicitada pelo titular dos dados em relação às decisões tomadas de modo unicamente automatizado deverá ser realizada por pessoa natural.

**3. Artigo 52**

**3. Sanções**

Vetados os dispositivos que previam, em caso de infração, a suspensão e até proibição do uso de banco de dados e do exercício das atividades que envolvem o tratamento de dados pessoais.

**4. Artigo 41**

**4. Encarregado**

Vetada a necessidade do encarregado ter conhecimento jurídico-regulatório, e a previsão de que a ANPD regulamentará os casos em que poderá ser indicado um único encarregado por grupo de empresas.

**5. Artigo 55**

**5. Taxas**

Vetada a cobrança de taxas pelos serviços prestados como fonte de recursos da ANPD.

**6. LAI**

**6. Lei de Acesso à Informação**

Vetada a proibição de compartilhamento dos dados pessoais de requerentes de acesso à informação com empresas privadas.





Os próximos passos são, considerando que os vetos ainda podem ser derrubados pelo Congresso:

- Será necessário um decreto para estruturar a ANPD e;
- A indicação dos diretores do Órgão.

# 4 COMO A LGPD IMPACTA SUA ORGANIZAÇÃO

**Nas relações de trabalho.**

A LGPD terá grande impacto nas relações comerciais e de consumo que exigem a coleta de dados, sobretudo diante da crescente tendência de tratamento de dados pessoais de clientes E consumidores com a finalidade de traçar seu perfil, identificando informações e extraindo conhecimento, em especial hábitos de consumo e condições financeiras e de crédito.

> *A utilização dos dados pessoais deve estar relacionada ao negócio jurídico subjacente."*

> *Salvo em caso de comprovado interesse público, fica vedada a troca de informações entre varejistas e empresas especializadas em bancos de dados."*





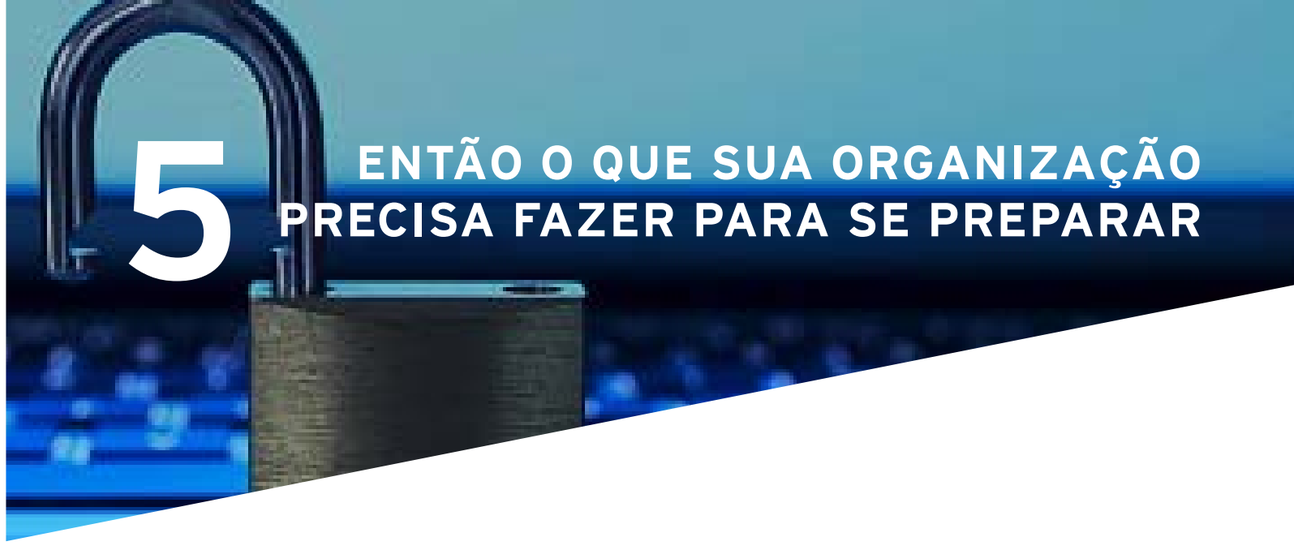
**Nas relações comerciais e de consumo.**

> *Como o empregador é detentor de informações pessoais de seus empregados, ele deve observar a LGPD, sob pena de responsabilidade civil, além de ressarcimento de eventuais prejuízos".*

> *Embora a lei autorize as empresas a usar os dados pessoais dos seus empregados e prestadores de serviços para a legítima execução dos contratos, em benefício do próprio trabalhador, não se pode desconsiderar cautela e observância das regras da LGPD em todas as suas fases, nos atos praticados antes da contratação, durante a vigência do contrato, nas terceirizações e após a rescisão dos contratos".*

Como anunciado logo no início da leitura, há muito a ser feito em termos de volume, natureza, diversidade e profundidade das atividades para se atingir a conformidade com a Lei Geral de Proteção de Dados, especialmente para aquelas organizações sem a fundação ou com uma fundação limitada de governança e gestão de riscos de segurança da informação.
É, de fato, muito mais do que os típicos escritórios de advocacia conseguem enxergar, do que os típicos fornecedores de software e hardware conseguem oferecer, e do que os típicos integradores e consultores de nicho conseguem implementar.
A melhor abordagem requer cooperação, multidisciplinaridade, priorização e coordenação.
Uma vez garantindo os alicerces de gestão de riscos de segurança da informação e realizando esse alinhamento relacionado à privacidades dos dados, é que poderemos sonhar todos juntos com os estados maduros e incorporados à organização de *Privacy by Design* e *Security by Design*.

Em termos de áreas corporativas impactadas pela necessidade de Governança de Privacidade, e Proteção de Dados, podemos mencionar:

# 5 ENTÃO O QUE SUA ORGANIZAÇÃO PRECISA FAZER PARA SE PREPARAR

Mesmo diante desse desafio gigantesco, haja visto sua complexidade também em virtude da perspectiva do tempo, que não é exaustivo, o melhor a ser feito agora é desenvolver uma visão integrada e customizada do seu próprio problema, levando em consideração o grau de preparo e maturidade dos seus processos e controles de governança de dados e proteção à informação, para então desenvolver um roadmap end-to-end priorizado, e que norteará todos os passos da jornada LGPD (que agora podemos chamar também de jornada da gestão corporativa de segurança da informação com requintes de especificidade na proteção de dados pessoais).

A essa altura, deve estar evidente pra você que só é possível endereçar a demanda de conformidade com a Lei Geral de Proteção de Dados com uma abordagem holística, uma equipe e uma oferta multidisciplinar integrada e coordenada para que, a seu tempo, todas as 'peças do quebra-cabeça' que compõem o roadmap tenham perfeito encaixe e cumpram seu papel de subsidiar a gestão eficaz dos riscos relacionados à proteção dos dados pessoais e da privacidade como um todo, onde a conformidade é apenas o end-game.

## 5.1 Compreender

- **Negócio:** o espaço operacional do negócio; sua estratégia comercial, digital e de dados; sua estrutura de gestão e organização; sua cadeia de valor, ativos e processos de negócio; bem como sua cultura de proteção da informação.

- **Estrutura:** a estrutura existente de privacidade e proteção de dados, suas políticas com diretrizes, normas e procedimentos, adquirindo entendimento sobre a postura existente na organização para o tema.

- **Governança:** o modelo de governança atual, incluindo papeis e responsabilidades.

- **Jurídico:** o status e a conformidade da organização em relação às leis relativas ao tema e demais regulamentações aplicáveis.

- **Transferência de dados:** as relações de negócio com fornecedores, parceiros e terceiros em geral.

## 5.2 Avaliar

- **Estratégia e apetite de risco:** o alinhamento estratégico e o apetite de risco, bem como os valores que norteiam a organização.

- **Mapa de fluxo de dados:** o fluxo de dados para gerar o mapeamento que auxiliará na determinação das exigências e na implementação das funções de privacidade de dados.

- **Maturidade LGPD:** a maturidade da privacidade em diferentes domínios como classificação de dados e estratégia de privacidade através da aplicação de ferramentas específicas.

- **Conscientização:** o aspecto cultural do capital humano da organização quanto à privacidade de dados com a aplicação de dinâmicas e artefatos de sensibilização e conscientização.

- **Roadmap:** com base no contexto da organização descoberto pelas atividades predecessoras, as ações processuais, físicas, tecnológicas e humanas necessárias para a aderência aos requisitos da LGPD de proteção e privacidades dos dados.



5. ENTÃO O QUE SUA ORGANIZAÇÃO
PRECISA FAZER PARA SE PREPARAR

## 5.3 Definir

- **Estratégia:** uma estratégia abrangente de proteção de dados e privacidade alinhada com os interesses e o apetite do negócio.

- **Políticas:** diretrizes, normas e procedimentos relacionados à privacidade e proteção de dados; classificação, retenção e perícia forense;

- **Governança:** o modelo de governança de proteção de dados e privacidade, e a diretoria de proteção de dados (DPO), incluindo papeis e responsabilidades na gestão de relacionamentos com agentes reguladores externos.

- **Fluxo de dados:** o roadmap final de atividades priorizadas para modelagem do fluxo de dados ideal para preservação da proteção dos dados sensíveis e da privacidade, considerando inventário de processos, a natureza dos dados pré-avaliados e as avaliações de impacto à privacidade (PIA's).

- **Impacto à privacidade:** os componentes de privacidade a serem inseridos no design de todos os novos produtos e serviços, como sistema de TI, processos e contratos orientados pela mentalidade "*Privacy by Design and by Default*".

- **Uso de dados:** um método de uso de dados sensíveis baseado no consentimento e uso legítimos e registros auditáveis e sustentáveis.

- **Direitos do titular:** direitos de acesso do usuário titular dos dados incluindo acesso lógico a sistemas e aplicativos; direito ao esquecimento e portabilidade de dados.

- **Proteção de dados:** soluções para proteção de dados (confidencialidade, integridade e disponibilidade) em ativos de tecnologia  envolvendo processos e controles de proteção (ex. criptografia, registro de eventos, controles de acesso etc), identificação, detecção e resposta às ameaças; tecnologias de aprimoramento de privacidade (PET); retenção de dados e incorporação técnica do conceito de *Privacy by Design*. (Item G em Atividades de Tratamento)

- **Prestação de contas:** medidas a serem implementadas para garantir que as regras de proteção de dados sejam observadas e possam ser reportadas e evidenciadas junto às autoridades e aos titulares dos dados quando solicitadas para fins de comprovação de conformidade ao LGPD.

- **Gestão de terceiros:** estrutura de orientação dos processos de processamento e troca de dados com terceiros como fornecedores, parceiros e contratados, incluindo gestão de riscos, contratos, monitoramento e relatório de conformidade.

- **Aplicações:** componentes e processos de privacidade para adoção e desenvolvimento de aplicações.

- **Monitoramento e tratamento de incidentes:** estrutura para monitoramento e resposta a incidentes que envolvam quebra de proteção de dados e privacidade, incluindo relatórios legais exigidos pela LGPD.

- **Conscientização e comunicação:** processos e ferramentas de conscientização do capital humano e comunicação interna, que desenvolva a cultura da gestão do risco, da proteção dos dados e da privacidade, enquanto a comunicação externa estabelece um fluxo de comunicação com as autoridades e titulares dos dados para fins de conformidade.

- **Métricas, relatórios e dashboard:** métricas relevantes para o escopo da proteção de dados e privacidade e em apoio ao modelo de governança implementado e comunicado através de um dashboard que conecta negócio a processos críticos, e estes, a ativos de informação.

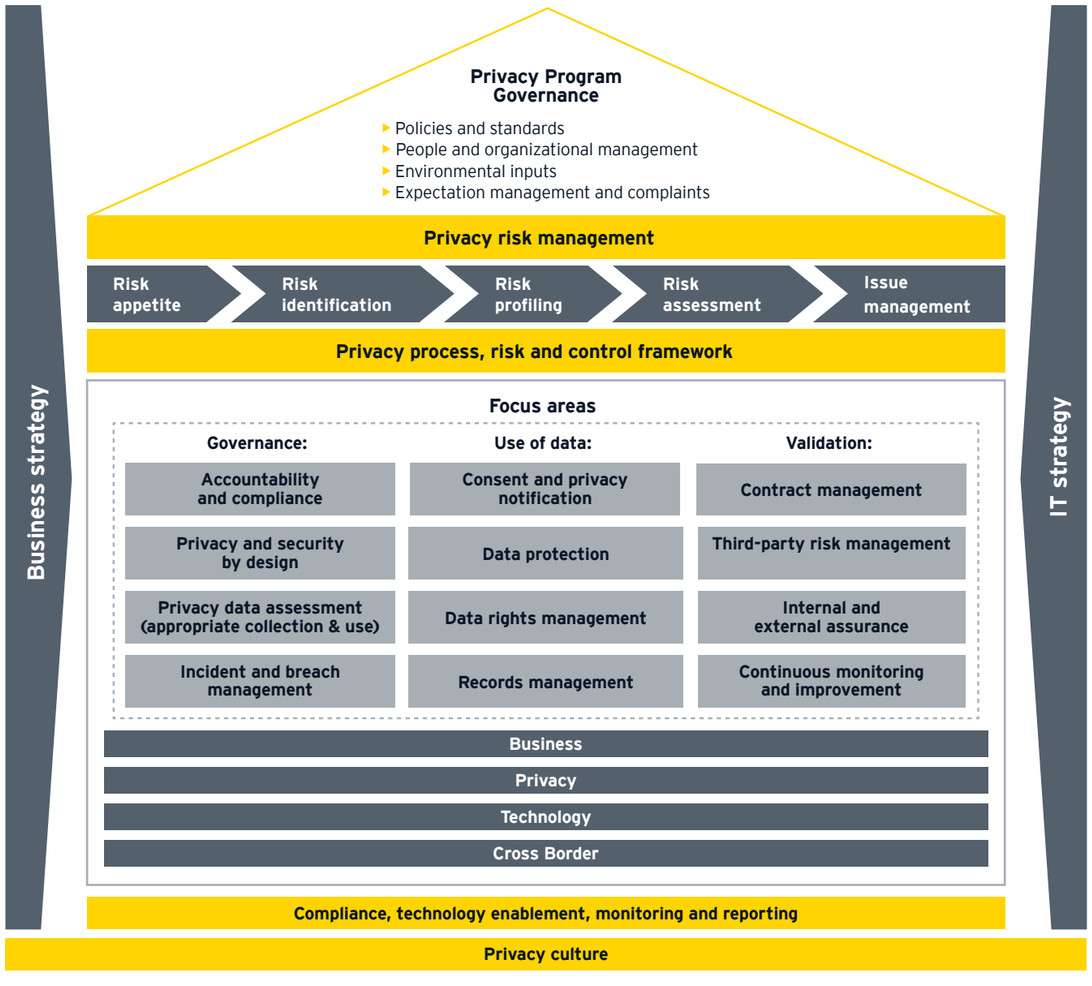


5. ENTÃO O QUE SUA ORGANIZAÇÃO
PRECISA FAZER PARA SE PREPARAR

# 5.4 Implementar

- Os componentes do modelo integrado de governança de proteção de dados e privacidade definidos nas fases anteriores e capturadas no roadmap priorizado de atividades, orientado por um *framework* específico de gestão de riscos.

**_Framework_ de gestão de riscos de privacidade da EY**



# 6 CONCLUSÃO

Independente se sua organização irá realizar a jornada para adequação com o suporte de uma consultoria ou com os recursos e capacidades internas, os passos abaixo são de extrema importância para o sucesso do projeto que, no futuro, se tornará um Sistema de Gestão:

**Estabelecer** um comitê diretor como alicerce para o programa de privacidade

**Construir** uma equipe com formação multidisciplinar

**Obter** apoio do corpo executivo

**Realizar** mapeamento de fluxo de dados seguindo uma abordagem baseada em risco

**Usar** a tecnologia como meio

**Aproveitar** as oportunidades de ganhos rápidos de maturidade



**EY**

Auditoria | Consultoria | Impostos | Transações Corporativas

**Sobre a EY**

A EY é líder global em serviços de Auditoria, Consultoria, Impostos e Transações. Nossos insights e os serviços de qualidade que prestamos ajudam a criar confiança nos mercados de capitais e nas economias ao redor do mundo. Desenvolvemos líderes excepcionais que trabalham em equipe para cumprir nossos compromissos perante todas as partes interessadas. Com isso, desempenhamos papel fundamental na construção de um mundo de negócios melhor para nossas pessoas, nossos clientes e nossas comunidades.

No Brasil, a EY é a mais completa empresa de Auditoria, Consultoria, Impostos e Transações Corporativas, com 5.000 profissionais que dão suporte e atendimento a mais de 3.400 clientes de pequeno, médio e grande portes.

EY refere-se à organização global e pode referir-se também a uma ou mais firmas-membro da Ernst & Young Global Limited (EYG), cada uma das quais é uma entidade legal independente. A Ernst & Young Global Limited, companhia privada constituída no Reino Unido e limitada por garantia, não presta serviços a clientes.

© 2019 EYGM Limited. Todos os direitos reservados.

Esta é uma publicação do Departamento de Marca, Marketing e Comunicação. A reprodução deste conteúdo, na totalidade ou em parte, é permitida desde que citada a fonte.

**www.ey.com.br**

**Facebook | EYBrasil**

**Instagram | eybrasil**

**Twitter | EY_Brasil**

**Linkedin | EY**

**Youtube | EYBrasil**