



**OS EFEITOS DA LEI GERAL DE
PROTEÇÃO DE DADOS NAS
STARTUPS**

OBJETIVO DO E-BOOK

Com o auxílio de um **advogado especializado** em proteção de dados, a startup deve **mapear todos os dados** objeto de tratamento, **analisar** como são utilizados e **medir a exposição da empresa** de acordo com a natureza das informações que são coletadas, bem como se atentar para coletar e capturar somente os **dados essenciais para a atividade** exercida pela empresa.

Neste e-book, **trazemos de forma simples** alguns **conceitos**, bem como os principais **pontos de atenção** que uma startup deve focar para adequar suas atividades à Lei Geral de Proteção de Dados que logo entrará em vigor.



Luciana Bortolozo é especialista em Direito em Startups pelo Insper. Especialista em Direito Civil e Processo Civil pela Escola Paulista de Direito. Certificada em Propriedade Intelectual pela Universidade de Genebra em parceria com a Organização Mundial de Propriedade Intelectual (WIPO). Atuação consultiva e contenciosa com ênfase em Direito Digital, Proteção de Dados, Propriedade Intelectual e Direito das Startups.

STARTUP

CONCEITO

O que é uma startup?

Existem vários conceitos para “**startup**”, e Eric Ries define como “**uma instituição humana projetada para criar novos produtos e serviços sob condições de extrema incerteza**”.

Toda empresa deve começar com uma **base sólida**, mesmo uma startup, cheia de incertezas, inseguranças e poucos recursos.

A **Lei Geral de Proteção de Dados (LGPD)** em pouco tempo estará vigente e as startups também precisam se adequar, especialmente no que tange à segurança dos dados, a criação de produtos e serviços que protejam as informações dos usuários desde o início (privacy by design e by default), a revisão de contratos com parceiros comerciais e criação de regras de boas práticas para funcionários, práticas de RH, etc.

LEMA: startup, dê aos usuários o **controle** de seus dados pessoais e **use** seu ativo econômico de forma **legal, ética e transparente**.

O QUE É A LGPD?

A legislação sobre privacidade e proteção de Dados Pessoais entrou em vigor no Brasil no dia 18 de setembro de 2020, com a Lei Geral de Proteção de Dados Pessoais (“LGPD” - Lei 13.709/2018).

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), popularmente conhecida como “LGPD”, é uma norma que dispõe sobre o tratamento de dados pessoais por pessoas físicas ou por empresas públicas ou privadas, através de qualquer meio (físico ou eletrônico).

Essa lei se aplica a empresas de todos os segmentos e não somente às empresas de tecnologia. Assim, empresas de todos os setores da economia, que de qualquer maneira realizem o tratamento de dados pessoais (clientes, funcionários, parceiros, etc.), deverão se adequar às disposições da LGPD.

A LGPD entrou em vigor em 18 de setembro de 2020, data em que as empresas já deverão estar adequadas às novas regras, garantindo o exercício dos direitos dos titulares de dados pessoais e podendo passar por processos de fiscalização por parte das autoridades.

Qual a importância da adequação da sua empresa?

- Diferencial competitivo frente aos concorrentes, demonstrando ao público consumidor que a empresa se preocupa com o tratamento de dados pessoais de forma ética;
- Diferencial competitivo frente aos investidores, aumentando o valor da marca;
- Melhorar a cultura de proteção de dados dentro da empresa;
- Evitar advertência à empresa em caso de descumprimento da legislação;
- Evitar a ordem de divulgar o incidente ao público;
- Evitar o bloqueio ou eliminação dos dados pessoais;
- Evitar multas de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, e limitada ao montante de R\$50 milhões por infração.

A photograph of a group of people in a meeting, with hands pointing at a laptop screen. The image is overlaid with a semi-transparent purple and blue gradient. The text "ENTENDENDO OS TERMOS" is centered in white, bold, uppercase letters.

ENTENDENDO OS TERMOS

DADOS PESSOAIS

CONCEITO

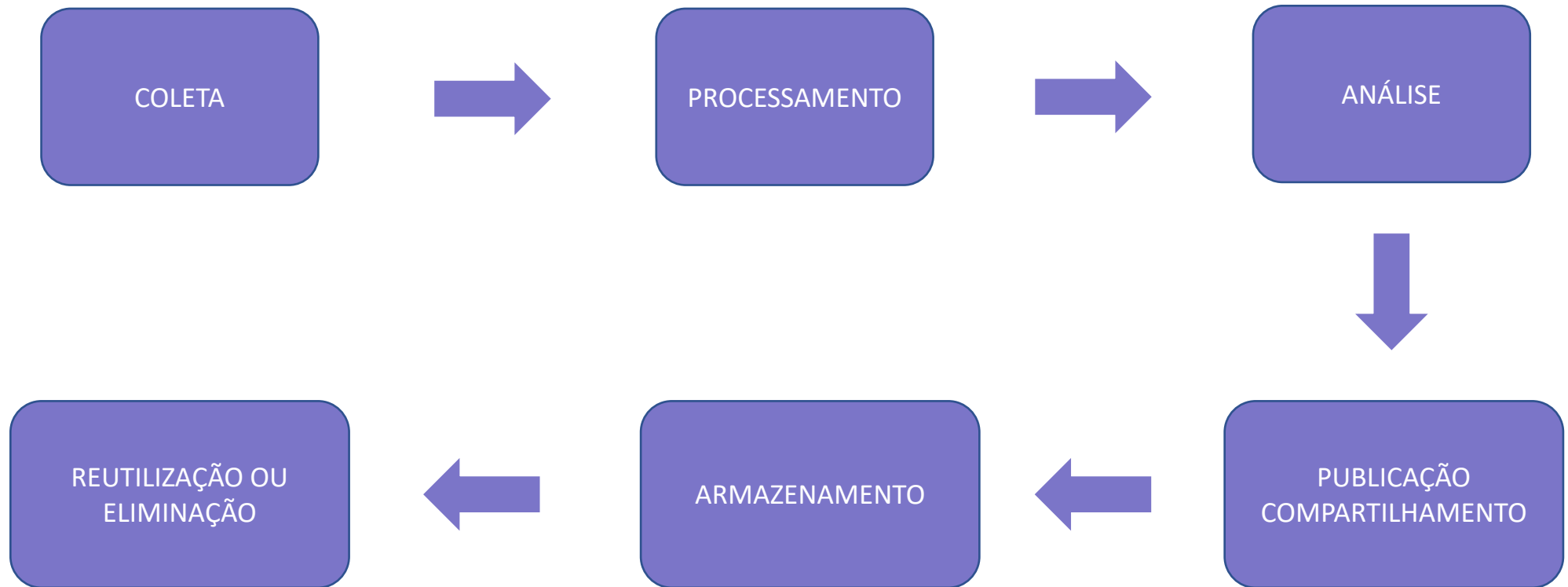
O que são dados pessoais?


É toda e qualquer informação relacionada a pessoa natural identificada ou identificável.

Quando esses dados são considerados 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.

CICLO DE VIDA DOS DADOS PESSOAIS





dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram a desvinculação dele a essa pessoa

banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico

titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento

tratamento: é toda e qualquer operação que é realizada com os dados pessoais. Por exemplo: coleta, utilização, distribuição, armazenamento, eliminação, transferência;

agentes de tratamento: o controlador e o operador

controlador: pessoa natural ou jurídica, de direito público ou privado que possui **competência e autonomia para tomar as decisões** referentes ao tratamento de dados pessoais

operador: pessoa natural ou jurídica, de direito público ou privado, que **realiza o tratamento** de dados pessoais em nome do controlador

encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados

PRINCÍPIOS

NORTEADORES DA LGPD

finalidade
adequação
necessidade

livre acesso

qualidade
dos dados

transparência

segurança

prevenção

não
discriminação

responsabilização
prestação de
contas

A QUEM SE APLICA A LEI

- ❖ a qualquer **operação de tratamento de dados pessoais coletados no Brasil**, realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio (*online ou off-line*)
- ❖ se o tratamento for realizado fora do território nacional, mas a atividade de tratamento for executada com o **objetivo de oferta ou de fornecimento de bens ou serviços no Brasil**, a Lei se aplica

A QUEM NÃO SE APLICA A LEI

A LGPD **não** se aplica ao tratamento de dados pessoais de **pessoas jurídicas ou pessoas falecidas**, bem como não se aplica ao tratamento:

- ❖ realizado por pessoa natural para **fins exclusivamente particulares e não econômicos**
- ❖ realizado para fins exclusivamente:
 - ❖ **jornalístico e artísticos**
 - ❖ **acadêmicos**
- ❖ realizado para fins exclusivos de:
 - ❖ **segurança pública**
 - ❖ **defesa nacional e segurança do Estado**
 - ❖ **atividades de investigação e repressão de infrações penais**
- ❖ Não se aplica a dados que **somente transitem pelo Brasil**, sem ser realizada operação de tratamento

A person wearing a light blue button-down shirt is shown from the chest down, sitting at a desk. They are holding a silver and black pen in their right hand and are in the process of signing a document. Their left hand is resting on the paper. The background is softly blurred, showing what appears to be an office setting. A semi-transparent purple horizontal band is overlaid across the middle of the image, containing the text.

DIREITOS

DOS TITULARES DE DADOS PESSOAIS

- ✓ confirmação da **existência** de tratamento
- ✓ **acesso** aos dados
- ✓ **correção** de dados incompletos, inexatos ou desatualizados
- ✓ **anonimização, bloqueio ou eliminação** de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na lei
- ✓ **portabilidade** dos dados a outro fornecedor de serviço ou produto
- ✓ **eliminação** dos dados pessoais tratados com o consentimento do titular
- ✓ **informação** das entidades públicas e privadas com as quais o controlador realizou **uso compartilhado** de dados
- ✓ informação sobre a possibilidade de não fornecer **consentimento** e sobre as **consequências da negativa**
- ✓ **revogação** do consentimento, por **procedimento gratuito e facilitado**

Os direitos dos titulares **não são absolutos**. Por exemplo, uma empresa pode manter certos dados pessoais para cumprir com obrigação regulatória.

De qualquer forma, a empresa precisa estar **preparada** para atender as requisições dos titulares dos dados pessoais e ter **procedimentos definidos** para cada hipótese.

É responsabilidade da empresa informar de maneira imediata aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento.



A top-down view of a meeting table. Several people's hands and arms are visible, engaged in discussion. One person points at a tablet displaying a pie chart. Another person writes in a notebook. The table is covered with various documents, including one with a bar chart and the word 'FINANCIAL' visible. A pair of glasses lies on the table in the bottom right corner. The entire scene is overlaid with a semi-transparent purple and blue gradient.

BASES LEGAIS

PARA TRATAMENTO DE DADOS PESSOAIS

De acordo com o artigo 7º da Lei, o tratamento de dados pessoais somente poderá ser realizado nas seguintes **hipóteses**:

I - mediante o fornecimento de **consentimento** pelo titular;

O que é consentimento? → é a manifestação **livre, informada** (deve ser clara) e **inequívoca** (demonstrável) pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Em alguns casos, além de respeitar todas as características elencadas acima, a LGPD exige que o **consentimento seja obtido de forma específica e destacada**. São eles:

- Dados pessoais sensíveis: quando a base legal for o consentimento, o tratamento de dados pessoais sensíveis somente poderá ocorrer quando o titular ou seu responsável legal autorizar, de forma específica e destacada, para finalidades determinadas.
- Dados pessoais de crianças e de adolescentes: o consentimento deve ser específico e em destaque, fornecido por pelo menos um dos pais ou pelo responsável legal.
- Transferência internacional de dados pessoais: quando também for baseada em consentimento, este deve ser específico e em destaque, com informação prévia sobre o caráter internacional da operação, distinguindo claramente de outras finalidades.

II - para o **cumprimento de obrigação legal ou regulatória** pelo controlador;

Sua empresa/instituição é do setor bancário? A Lei Anti Lavagem de Dinheiro e a Instrução 617 da CVM a obriga armazenar os dados pelo prazo 5 anos, a contar do encerramento da conta ou conclusão da transação.

A vantagem de utilizar essa hipótese para o tratamento dos dados? É fácil justificar o tratamento. No entanto, a empresa/instituição está limitada a possuir os dados pessoais somente para cumprir a obrigação legal e não os utilizar para fazer marketing, por exemplo.

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;

Exemplo: A utilização de dados pessoais por um hotel, quando o consumidor firmou contrato com uma empresa de turismo (online ou off-line). O hotel pode utilizar essa base legal para tratar os dados do consumidor que foram fornecidos para a empresa de turismo.

VI - para o **exercício regular de direitos em processo judicial, administrativo ou arbitral**;

Por exemplo, a empresa pode armazenar dados pessoais de funcionários para defesa em eventual futura ação judicial trabalhista.

VII - para a **proteção da vida ou da incolumidade física** do titular ou de terceiro;

Por exemplo, uma instituição financeira que quer garantir a segurança das pessoas em agência bancária com a instalação de cameras.

VIII - para a **tutela da saúde**, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

Por exemplo, dados armazenados por hospitais, médicos e enfermeiros.

IX - para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente;

Por exemplo, a automática negativação (opt-out) do nome da pessoa, com a inclusão do cadastro nos órgãos de proteção ao crédito. * Lei do Cadastro Positivo (análise de risco de crédito e dar subsídios para concessão ou extensão de crédito).

X - 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 dos dados pessoais;

O tratamento de dados pessoais pela hipótese do interesse legítimo do controlador ou de terceiro **somente é possível se houver uma finalidade legítima** (art. 10 da Lei), consideradas a partir de **situações concretas** (o legítimo interesse não pode justificar o tratamento de dados pessoais em situações futuras e hipotéticas) **que incluem, mas não se limitam a:**

I - **apoio e promoção** de atividades do controlador; e

II - **proteção**, em relação ao titular, **do exercício regular de seus direitos ou prestação de serviços** que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais;

Quando o tratamento for baseado no legítimo interesse do controlador, **somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.**

INTERESSE LEGÍTIMO

TESTE DE PROPORCIONALIDADE

Um ótimo exercício que deve ser feito para se chegar à conclusão de que há interesse legítimo é o seguinte:

#1

Em primeiro lugar, deve existir uma situação concreta para aplicar o interesse legítimo como base para o tratamento de dados. **Tendo uma situação concreta, pergunte-se: tenho de fato um interesse legítimo? É justificável capturar esse dado?**

#2

Esses dados são realmente necessários para atingir o objetivo que quero? **É bom e conveniente** ter esse dado **ou é mesmo imprescindível?** Deve ser imprescindível. Existem outras bases legais aplicáveis para este caso em concreto?

#3

Quando analiso os direitos, liberdades e expectativas do titular de dados, o coloco em uma situação injusta ou **violo algum direito?**

#importante

A hipótese do legítimo interesse não se aplica a:

dados sensíveis (de saúde, por exemplo)

dados de crianças (é necessário consentimento específico e em destaque dados por pelo menos um dos pais ou pelo responsável legal)

RELATÓRIO DE IMPACTO



Quando o tratamento de dados pessoais tiver como fundamento o interesse legítimo, a Autoridade Nacional poderá solicitar ao **controlador** o **RELATÓRIO DE IMPACTO**, observados os segredos comercial e industrial.

O **Relatório** deverá conter, no mínimo:

- ❖ a descrição dos tipos de dados coletados
- ❖ a metodologia utilizada para a coleta e para a garantia da segurança das informações
- ❖ a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados

O raciocínio jurídico que deve existir no Relatório de Impacto é:

- ❖ elencar os direitos que estão em jogo e porque há legítimo interesse

O relatório deve estar pronto, caso a Autoridade Nacional o solicite. *#importante*

A woman with blonde hair, wearing a white button-down shirt, is sitting at a white desk. She is using a white mouse with her right hand. In front of her is a silver laptop. To the left of the laptop is a smartphone. The background is a blurred office setting. A semi-transparent purple banner is overlaid across the middle of the image, containing the text.

DADOS SENSÍVEIS

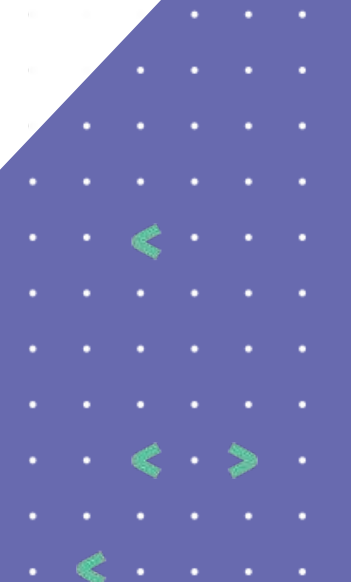
TRATAMENTO

DADOS SENSÍVEIS PODEM SER TRATADOS NAS SEGUINTE HIPÓTESES

I - quando o titular ou seu responsável legal **consentir**, de forma **específica e destacada**, para finalidades específicas;

II - **sem fornecimento de consentimento** do titular, nas **hipóteses em que for indispensável** para:

- ❖ cumprimento de **obrigação legal ou regulatória** pelo controlador;
- ❖ tratamento compartilhado de dados **necessários à execução, pela administração pública, de políticas públicas** previstas em leis ou regulamentos;
- ❖ realização de **estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- ❖ o **exercício regular de direitos**, inclusive em contrato e em processo judicial, administrativo e arbitral;
- ❖ a **proteção da vida** ou da incolumidade física do titular ou de terceiro;
- ❖ a **tutela da saúde**, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
- ❖ garantia da **prevenção à fraude e à segurança do titular**, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.





DADOS DE CRIANÇAS E ADOLESCENTES TRATAMENTO

TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

O tratamento de dados pessoais de crianças requer o **consentimento específico** e em **destaque** dado **por pelo menos um dos pais ou pelo responsável legal**.

No entanto, quando a coleta for necessária para contatar os pais ou o responsável legal, ou para a proteção da criança, poderá ser realizada sem o consentimento. Neste caso, os dados podem ser utilizados uma única vez e sem armazenamento.

Em nenhum caso os dados poderão ser repassados a terceiro sem consentimento dos pais ou responsável legal.

Se seu negócio é uma plataforma online de jogos ou outras aplicações na internet, não poderá condicionar a participação das crianças e adolescentes ao fornecimento de informações pessoais além das estritamente necessárias à atividade. Ainda, você deve proporcionar à criança um entendimento claro, simples e acessível às informação sobre a privacidade.

Com as tecnologias disponíveis no mercado, a startup deve realizar todos os **esforços** razoáveis para **verificar** que o **consentimento** foi dado pelo responsável pela criança.



PENALIDADES

Quais as penalidades que a Lei traz?

1. advertência, com indicação de prazo para adoção de medidas corretivas
2. multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos
3. multa diária
4. publicização da infração
5. bloqueio dos dados pessoais
6. eliminação dos dados pessoais

As **sanções** serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa e considerados os seguintes **parâmetros e critérios**, dentre outros:

- I. a gravidade e a natureza das infrações e dos direitos pessoais afetados
- II. boa-fé do infrator
- III. grau do dano
- IV. cooperação do infrator
- V. existência de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados
- VI. adoção de política de boas práticas e governança



**PRIVACY BY DESIGN
PRIVACY BY DEFAULT**

Se você é uma startup, provavelmente você cria e recria produtos com certa frequência. Com a introdução das regras da LGPD, qualquer **sistema ou solução** deve ser pensada observando a **proteção dos dados pessoais** dos usuários/clientes, desde o início, ou seja, desde a **concepção do produto**.

O conceito do **Privacy by Design** possui **7 princípios**:

1. Proatividade e não reatividade

Prevenção é o lema. Tudo o que pode ser feito para proteger dados pessoais deve ser adotado. Antecipar/prevenir situações de invasão de privacidade é melhor a remediar. Proteja antes que aconteça o pior com os dados de seus clientes.

2. Privacidade como padrão

O sistema/produto/serviço deve trazer a privacidade dos usuários/clientes, garantindo que eles não precisem ajustar nenhuma configuração para seus dados estarem seguros. Esse princípio pode ser chamado de **Privacy by Default**

Privacy by Default possui 4 princípios: especificação do propósito, limitação da coleta, minimização dos dados, limitação no uso, retenção e divulgação.



3. Privacidade incorporada ao projeto

A privacidade e proteção dos dados pessoais deve ser incorporada à elaboração do design do projeto. Cada arquitetura de sistemas deve ser pensada com viés da proteção de dados, desde a concepção.

4. Funcionalidade total

A funcionalidade de um sistema ou plataforma não pode ser prejudicada ou comprometida pela incorporação da privacidade dos dados.

Não é um jogo de quem ganha ou quem perde. O objetivo é ter ambos: funcionalidade e proteção.

5. Segurança durante todo o ciclo de vida dos dados

Medidas fortes de segurança, desde a coleta do dado até seu compartilhamento com terceiros ou eliminação.

6. Visibilidade e transparência

Importante para criar a confiança dos usuários/clientes. A transparência e visibilidade podem ser passadas através de uma Política de Privacidade bem elaborada, que mostrará como a sua startup vai conduzir a gestão de dados pessoais dos seus clientes.

7. Respeito pela privacidade do usuário

A startup deve respeitar a privacidade do usuário, com medidas fortes na proteção dos dados pessoais. Todo sistema/plataforma ou prática de negócio deve respeitar a privacidade dos usuários. Processos internos, procedimentos e políticas adequadas devem demonstrar as soluções centradas no usuário.



BOAS PRÁTICAS DE GOVERNANÇA

O que deve conter em um Programa de Governança em Proteção de Dados?

- ❖ as condições de organização dos dados
- ❖ o regime de funcionamento e os procedimentos adotados
- ❖ as normas de segurança e os padrões técnicos
- ❖ as obrigações específicas para os diversos envolvidos no tratamento dos dados pessoais
- ❖ as ações educativas
- ❖ os mecanismos internos de supervisão e de mitigação de riscos

As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente, assim como poderão ser reconhecidas e divulgadas pela Autoridade Nacional.



AS ETAPAS DO PROJETO DE ADEQUAÇÃO

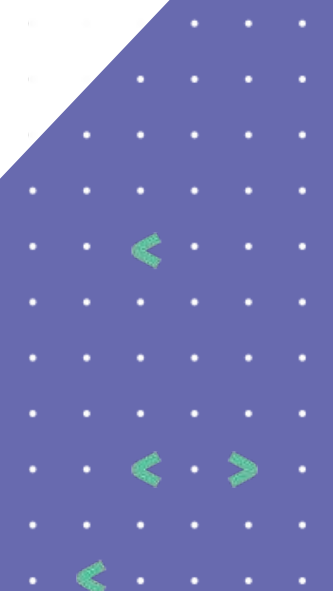
O Projeto de Adequação envolverá todas as áreas da startup e contará com o envolvimento dos principais funcionários de cada área, tal como o líder do RH, do administrativo, do TI e assim por diante.

Não existe um “passo a passo” definido e cada Projeto será adaptado de acordo com o modelo de negócio da empresa. Contudo, existem algumas **fases essenciais para o sucesso do Projeto**, são elas:

1) Consultoria

2) Implementação

3) Operação



1) Consultoria

- ▶ Nessa fase, é feito o **planejamento do projeto**, com a entrega de um cronograma.
- ▶ À partir de reuniões com o time da startup, os principais *stakeholders* são identificados e o negócio do contratante é entendido a fundo.
- ▶ Serão conduzidas sessões de **workshop** com as áreas responsáveis pelo levantamento dos dados tratados. Através de entrevistas com o time da startup, será feito o **mapeamento do fluxo de dados** e sistemas da empresa.
- ▶ Normas e políticas internas relativas à proteção de dados serão avaliadas, com a identificação de **gaps de conformidade**.
- ▶ Serão fornecidas **recomendações jurídicas** para procedimento, contratos, estrutura de governança de dados, comunicação de incidentes, etc.

2) Implementação

- ▶ Nessa fase, serão **elaborados os materiais/documentos** necessários para que a startup esteja *compliant* com a LGPD. Alguns exemplos:
 - ▶ Elaboração/revisão de programa de governança em proteção de dados
 - ▶ Elaboração/revisão de política de segurança da informação
 - ▶ Condução de treinamentos para funcionários
 - ▶ Elaboração/revisão de termos de uso e política de privacidade
 - ▶ Elaboração e revisão de contratos
 - ▶ Elaboração de relatório de impacto

3) Operação

- ▶ Nessa fase, serão realizados **testes** a fim de verificar a segurança das operações de tratamento de dados, assim como para verificar **se a startup está preparada para receber solicitações de titulares de dados**.

bortolozo ▶

Serviços jurídicos em direito
digital e proteção de dados

Entre em contato

Tel. 11 98218 6525

luciana@bortolozoadv.com.br



[/bortolozo.adv](https://www.bortolozo.adv.br)