CARTILHA P&PD

SEUS DADOS
SUAS REGRAS
PRIVACIDADE

suzano
nós plantamos o futuro

CUIDAR DOS DADOS PESSOAIS: FAZ PARTE DO **NOSSO PAPEL.**

Em um mundo hiperconectado, o uso de dados pessoais torna-se cada vez mais relevante para os modelos de negócios das empresas, auxiliando na tomada de decisão e na criação de estratégias assertivas. Com isso, surgem leis e regulamentos voltados à proteção dessas informações, como a Lei Geral de Proteção de Dados (LGPD).

Na Suzano, acreditamos que só é bom para nós se for bom para o mundo. Por isso, temos o compromisso de seguir as legislações vigentes nos países onde atuamos e proteger as informações a que temos acesso, especialmente os dados pessoais de todos que possuem algum relacionamento conosco.

Nossa equipe de Privacidade e Proteção de Dados Pessoais (P&PD) não mede esforços para atender a todas as demandas relacionadas ao assunto, auxiliando na segurança das informações. No entanto, sabemos que o cuidado com os dados pessoais é uma responsabilidade coletiva.

Pensando nisso, desenvolvemos esta cartilha para que você conheça os conceitos básicos e alguns cuidados diários que fazem a diferença quando o assunto é privacidade. ***Afinal, proteger os dados pessoais faz parte do nosso papel.***

ÍNDICE

01. GLOSSÁRIO 05

CONCEITOS BÁSICOS SOBRE PROTEÇÃO DE DADOS PESSOAIS

1.1 DADO PESSOAL 06
1.2 LEIS DE PROTEÇÃO DE DADOS PESSOAIS 06
1.3 AUTORIDADES DE PROTEÇÃO DE DADOS PESSOAIS 07
1.4 CATEGORIAS DE DADOS PESSOAIS 07
1.5 TITULAR DE DADOS PESSOAIS 07
1.6 TRATAMENTO DE DADOS 08
1.7 AGENTE DE TRATAMENTO 09
1.8 ENCARREGADO (DPO) 10
1.9 BASE LEGAL 10
1.10 PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS 11
1.11 DIREITOS DOS TITULARES 12
1.12 SANÇÕES E PENALIDADES 12

02. BOAS PRÁTICAS PARA PESSOAS FÍSICAS 13

COMO CULTIVAR A SUA PRIVACIDADE?

2.1 BOAS PRÁTICAS NO TRABALHO 14
2.2 CUIDADOS COM AS SUAS SENHAS 15
2.3 BOAS PRÁTICAS COM MATERIAIS IMPRESSOS 15
2.4 CONECTE-SE COM SEGURANÇA 16

03. BOAS PRÁTICAS PARA PESSOAS JURÍDICAS 17

ENTENDA O PAPEL DE UMA EMPRESA COM P&PD

3.1 ENTENDENDO AS ATIVIDADES 18
3.2 AVALIAÇÃO DE RISCO 18
3.3 AVISO P&PD NAS PLATAFORMAS 18
3.4 AVISO P&PD INTERNO 19
3.5 PRIVACY BY DESIGN 19
3.6 CONTRATAÇÃO DE FORNECEDORES 20

ÍNDICE

04. F.A.Q: PRINCIPAIS DÚVIDAS 21

O QUE VOCÊ PRECISA SABER SOBRE PROTEÇÃO DE DADOS PESSOAIS

4.1 COMO SEI QUAL LEI DEVE SER APLICADA?.....22
4.2 DADOS DE PESSOAS JURÍDICAS SÃO DADOS PESSOAIS?.....22
4.3 PRECISO TER O CONSENTIMENTO SEMPRE QUE TRATAR DADOS PESSOAIS?.....23
4.4 APÓS A COLETA, POSSO UTILIZAR OS DADOS PESSOAIS DE OUTRAS FORMAS?.....23
4.5 PRECISO ME PREOCUPAR COM A LEI AO TRATAR DADOS PESSOAIS DE BASES PÚBLICAS?.....23
4.6 POSSO UTILIZAR SCRAPING EM SITES PÚBLICOS PARA COLETAR INFORMAÇÕES?.....24
4.7 POSSO CONTRATAR CLOUD FORA DO PAÍS?.....24
4.8 PEQUENAS EMPRESAS PRECISAM SEGUIR AS LEIS DE PROTEÇÃO DE DADOS PESSOAIS?.....25
4.9 COMO FICAM OS SEGREDOS COMERCIAIS E INDUSTRIAIS QUANDO FALAMOS DE P&PD?.....25
4.10 O QUE FAZER EM CASOS DE INCIDENTE DE SEGURANÇA?.....25
4.11 O QUE ACONTECE SE UMA EMPRESA VIOLAR A LEI?.....26

01.

GLOSSÁRIO:

CONCEITOS SOBRE PROTEÇÃO DE DADOS PESSOAIS

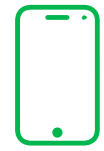
1.1
DADO PESSOAL

Qualquer informação que permita **identificar** uma pessoa, seja de forma **direta ou indireta**.

Biometria

Documentos

Placa de carro

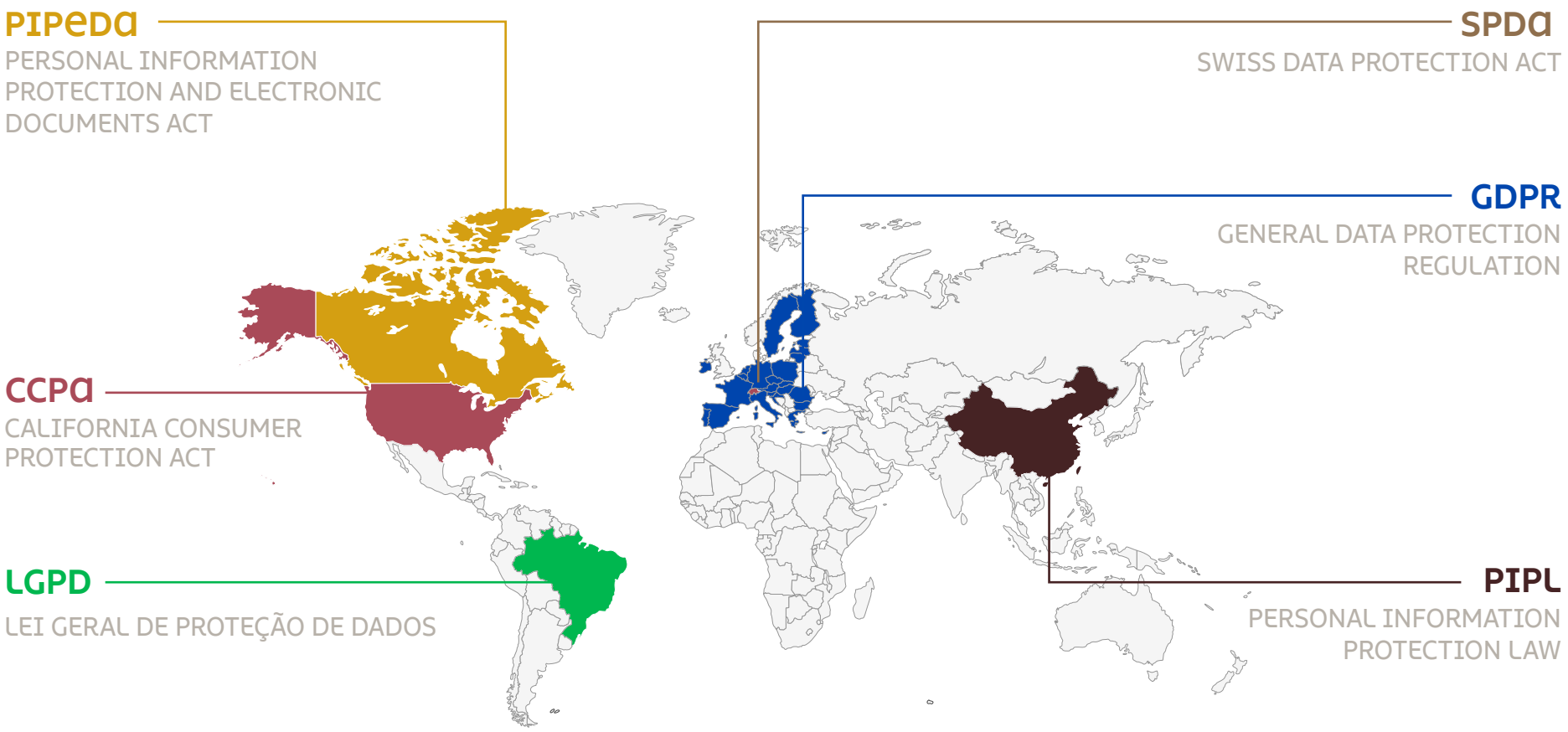


Celular

Endereço

1.2
LEIS DE PROTEÇÃO DE DADOS PESSOAIS

Estabelecem regras, obrigações e princípios a serem seguidos quando lidamos com dados pessoais. Existem diversas legislações ao redor do mundo, entre elas:



Cada lei possui regras específicas e particularidades. O que você precisa saber é que essas legislações trazem benefícios para todos: enquanto pessoas físicas ganham mais **garantias e direitos** sobre as suas informações pessoais, empresas contam com **maior segurança jurídica** para executar suas atividades.

Neste material, abordamos a proteção de dados pessoais de forma ampla, aprofundando alguns conceitos apresentados pela LGPD e pelo GDPR, fique atento a detalhes das leis que se aplicam ao seu país.

1.3 AUTORIDADES DE PROTEÇÃO DE DADOS

Responsáveis pela regulamentação, aplicação e fiscalização das leis de proteção de dados pessoais vigentes em cada país. Entre elas:

BRASIL

ANPD | Autoridade Nacional de Proteção de Dados

FRANÇA

CNIL | Commission nationale de l'informatique et des libertés

REINO UNIDO

ICO | Information Commissioner's Office

ESPANHA

AEPD | Agencia Española de Protección de Datos

1.4 CATEGORIAS DE DADOS PESSOAIS

As legislações de proteção de dados ao redor do mundo estabelecem diferentes categorias de dados pessoais.

1.4.1 Dados pessoais comuns

Identificam uma pessoa de forma direta como nome, RG, CPF ou título de eleitor. Ou indireta, como IMEI, geolocalização, placa de carro e endereço de IP.

1.4.2 Dados pessoais sensíveis

Informações que revelam detalhes íntimos ou com potencial discriminatório. **Na LGPD e no GDPR são:**

- *Dados de Saúde*
- *Vida sexual*
- *Raça e etnia*
- *Dados biométricos e genéticos*
- *Sindicatos, partidos e opinião política*
- *Religião e crenças filosóficas*

1.5 TITULAR DE DADOS

Pessoa física a quem se referem os dados pessoais. Ou seja, **você é o titular dos seus dados pessoais!** Outros exemplos:

USUÁRIOS DE SITES E APPS

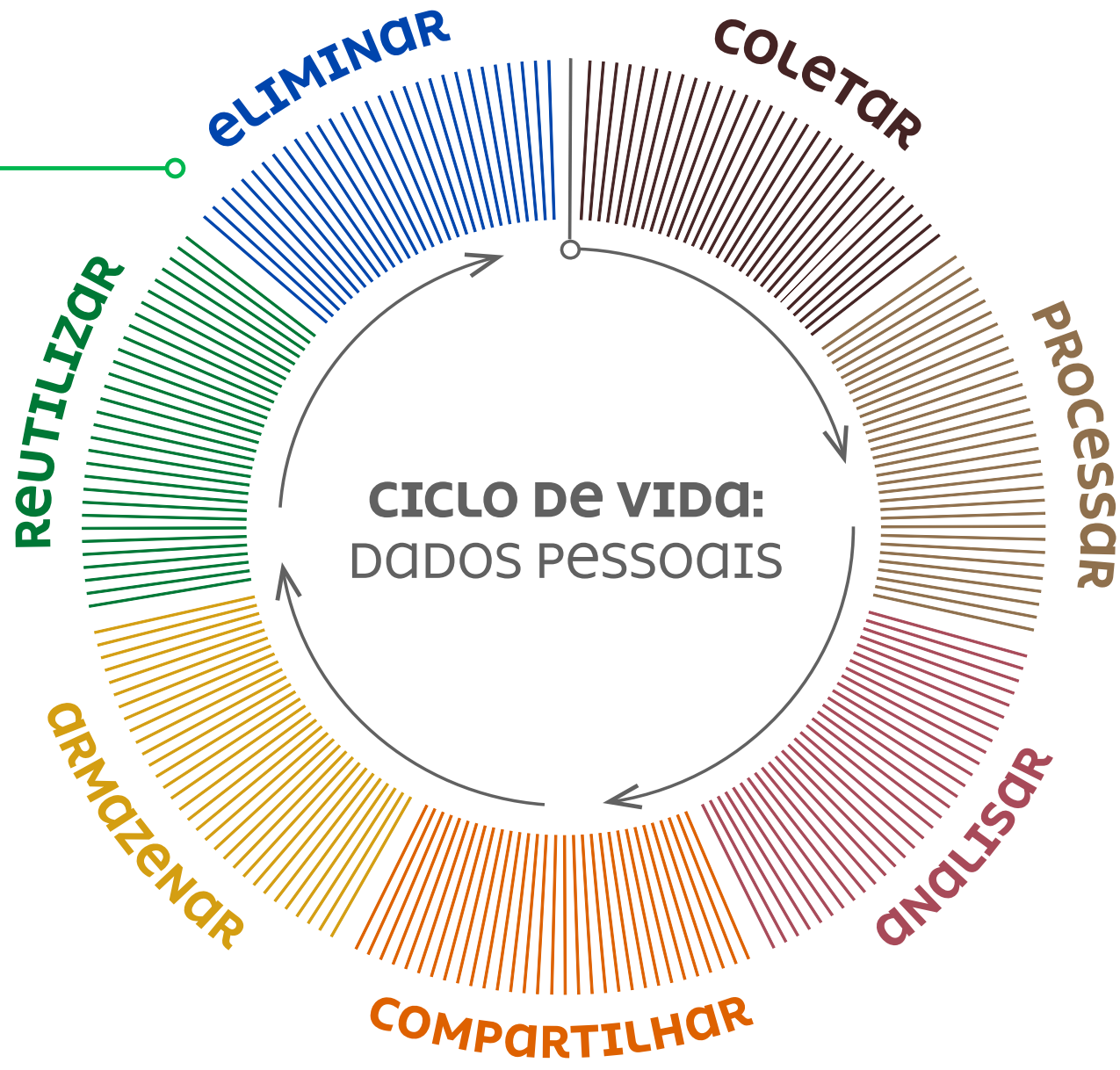
COLABORADORES DE UMA EMPRESA

DEPENDENTES DE COLABORADORES

REPRESENTANTES DE FORNECEDORES

1.6 TRATAMENTO DE DADOS PESSOAIS

O termo se refere a ***qualquer uso que é feito com um dado pessoal***, desde o mero armazenamento, visualização, até análises aprofundadas. Algumas atividades que fazem parte do ciclo de vida das informações são:



O tempo de armazenamento dos dados pessoais antes da exclusão é variável.

1.6.1 Restrições ao tratamento de dados pessoais de crianças e adolescentes

As legislações ao redor do mundo costumam tratar dados pessoais de menores de idade de forma especial, impondo regras para o seu uso, especialmente quando falamos de dados pessoais de crianças. Por exemplo:

NO REINO UNIDO

A autoridade de proteção de dados do país indica que para tratar dados pessoais de crianças (-13 anos), a empresa deverá fornecer avisos de privacidade e proteção de dados acessíveis para esta faixa etária.

NO BRASIL

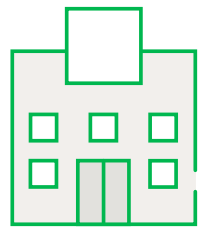
O consentimento do responsável é necessário para tratar dados pessoais de menores de 12 anos. Em alguns casos, prezando pelo melhor interesse da criança, poderá haver tratamento sem o consentimento. Exemplo: autoridades podem tratar os dados pessoais de crianças para garantir sua segurança.

1.7 AGENTE DE TRATAMENTO

Quem realiza as atividades de tratamento de dados pessoais. São pessoas físicas ou jurídicas, que podem ser de direito público ou privado, São exemplos de agentes de tratamento:

UM MÉDICO AUTÔNOMO ANALISANDO EXAMES

Ao tratar dados pessoais de saúde, um médico autônomo atua como agente de tratamento.



UMA EMPRESA GERINDO A FOLHA DE PAGAMENTO

Ao tratar dados pessoais dos seus colaboradores, a empresa atua como agente de tratamento.

O agente de tratamento pode atuar como Controlador ou Operador. Entenda cada um dos papéis:

CONTROLADOR X OPERADOR

É quem define porquê e como dados pessoais serão utilizados. É o responsável por analisar os riscos, desenvolver documentos de conformidade, além de ser o ponto de contato com os titulares de dados.

NA PRÁTICA:

*Uma empresa é **controladora** dos dados pessoais dos seus colaboradores em atividades de RH (ex: contratação, avaliação periódica de performance, etc).*

É quem trata dados em nome do controlador, executando as suas ordens. O operador deve se comprometer a não utilizar os dados para suas próprias finalidades, além de garantir a segurança dos dados tratados.

NA PRÁTICA:

Caso a empresa contrate uma terceira para realizar a gestão da folha de pagamento, a primeira será a controladora e a outra operadora.

NA LGPD

"Controlador" e "Operador" são termos utilizados pela lei brasileira, a LGPD.

NO GDPR

Os termos equivalentes no GDPR são, respectivamente, "controller" e "processor".

NA CCPA

Na lei californiana (CCPA), os respectivos termos são "business" e "service provider".

1.8 ENCARREGADO (DPO)

Pessoa indicada pela empresa para atuar como canal de comunicação entre a própria empresa, os titulares de dados pessoais e as autoridades. Pode ser chamada de encarregado ou Data Protection Officer (DPO).

1.9 BASE LEGAL

É a justificativa jurídica para tratar dados pessoais. Toda atividade de tratamento deve ser justificada com uma base legal.

NO BRASIL

A LGPD prevê 10 bases legais para justificar o tratamento de dados pessoais comuns, e 8 para o tratamento de dados sensíveis. Não existe hierarquia entre as bases legais disponíveis.

BRASIL X UNIÃO EUROPEIA

As bases legais da LGPD são similares às do GPDR, com algumas particularidades. Apenas no Brasil, o tratamento pode ser feito para **proteção ao crédito**. Uma das particularidades do GDPR é a possibilidade de tratar dados pessoais sensíveis que tenham sido tornados públicos pelo próprio titular.

BASE LEGAL	TRATAMENTO DE DADOS PESSOAIS
EXECUÇÃO DE CONTRATO	João compra um livro online e compartilha seu nome completo e endereço para que a empresa possa enviar o produto.
PROTEÇÃO DA VIDA	Uma empresa exige que seus colaboradores apresentem comprovante de vacinação contra COVID para retorno do trabalho presencial.
CUMPRIMENTO DE OBRIGAÇÃO LEGAL	Maria inclui os dados pessoais necessários para preencher a sua declaração de imposto de renda.
LEGÍTIMO INTERESSE	Após a entrega de um produto, a empresa XYZ envia ao cliente uma pesquisa de satisfação por e-mail, buscando aprimorar o serviço prestado.

1.10 PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS

As legislações ao redor do mundo trazem **princípios que devem ser seguidos nas atividades envolvendo dados pessoais**. De modo geral, os três princípios mais recorrentes nas leis de proteção de dados pessoais são:

1.10.1 Transparência

As informações sobre o tratamento dos dados pessoais, ou seja, as regras do jogo, devem ser estar em linguagem simples, didática e objetiva. Por exemplo, o titular deve entender um aviso de privacidade e proteção de dados pessoais.

- **Linguagem acessível:** Fornecer ao titular informações claras, didáticas e transparentes sobre o tratamento.
- **Livre acesso:** o titular poderá acessar de forma gratuita e sem burocracias, quais dados pessoais são tratados, para quê e por quanto tempo.

1.10.2 Finalidade

Ter um objetivo específico e legítimo para o tratamento e informar o titular da finalidade. Por exemplo, uma empresa pode solicitar os dados bancários de um funcionário para remunerá-lo. O funcionário deve estar ciente disso.

- **Adequação:** os dados pessoais devem ser tratados seguindo o que foi informado ao titular.
- **Necessidade:** tratar apenas os dados pessoais que são realmente necessários para cumprir a finalidade.
- **Qualidade das informações:** os dados pessoais tratados devem estar atualizados e corretos.
- **Não-discriminação:** a finalidade do tratamento não pode ser discriminatória ou abusiva.

1.10.3 Prevenção e Segurança

Proteger os dados pessoais contra acesso não-autorizado, tratamento ilícito, roubo, perda, destruição ou danificação, adotando as medidas técnicas adequadas. Por exemplo, utilização de programas e softwares efetivos para barrar o ataque de hackers aos servidores.

- **Prevenção:** adotar medidas para prevenir qualquer dano aos titulares de dados pessoais.
- **Segurança**: adotar medidas técnicas como criptografia e restrição de acesso, para garantir a segurança e integridade dos dados pessoais tratados.
- **Ser responsável e prestar contas:** quem trata os dados pessoais deve comprovar que está de acordo com a lei, apresentando as medidas de prevenção e segurança adotadas.

1.11 DIREITOS DO TITULAR DE DADOS PESSOAIS

Os titulares de dados pessoais possuem direitos, garantidos pelas leis vigentes. É importante que você conheça os principais, afinal, eles ***também são seus direitos.***

Confirmar a existência do tratamento e ter acesso aos seus dados pessoais.

Corrigir os seus dados pessoais caso estejam incorretos, desatualizados ou incompletos.

Solicitar informações sobre o compartilhamento dos seus dados pessoais.

Revogar o consentimento.

Questionar a autoridade os sobre seus direitos como titular de dados pessoais.

1.12 SANÇÕES E PENALIDADES

Incidentes de segurança ou descumprimento da lei podem trazer grandes problemas para a empresa. Além da aplicação de penalidades administrativas pela autoridade ***(incluindo multas de até R$ 50 milhões por infração),*** podem colocar dados confidenciais em risco, trazendo ***consequências judiciais e reputacionais.***

02.

BOAS PRÁTICAS:

COMO CULTIVAR A SUA PRIVACIDADE?

CULTIVE O CUIDADO COM OS SEUS DADOS PESSOAIS

Enviar uma mensagem no grupo da família, comprar um cafezinho na padaria, consultar o saldo da conta bancária, bater o ponto no trabalho: ***a maior parte das nossas atividades diárias envolvem dados pessoais***. Disponibilizamos essas informações de forma tão automática que nem paramos para pensar se estamos seguros e se a nossa privacidade está sendo respeitada.

Para evitar fraudes, golpes e incidentes envolvendo os nossos dados pessoais, é importante adotarmos alguns cuidados no nosso dia a dia. Confira neste capítulo dicas rápidas e boas práticas que não podem ficar de fora da sua rotina!

2.1 BOAS PRÁTICAS NO TRABALHO

Garantir a segurança das informações em uma empresa é papel de todos os colaboradores. Com alguns cuidados, você ajuda a proteger os dados pessoais de clientes, colegas de trabalho, e até mesmo as suas próprias informações!

CONFIRA O DESTINATÁRIO DOS SEUS E-MAILS

Ao enviar e-mails para clientes, fornecedores ou até mesmo internamente, para colegas de trabalho, sempre confira os destinatários da mensagem.

QUESTIONE ANTES DE COMPARTILHAR DADOS PESSOAIS

Se alguém solicitar o compartilhamento de documentos com dados pessoais, questione a finalidade e envie apenas as informações necessárias! *Por exemplo:*

O time de marketing criou uma campanha interna comemorativa de Dia das Mães. Para isso, solicitou ao RH os dados pessoais de todas as colaboradoras da empresa que são mães.

O time de RH **questionou para quê** os dados pessoais seriam utilizados. Ao entender o que o time de marketing precisava, compartilhou a planilha com os dados pessoais necessários.

Neste caso, o time de marketing precisava apenas do nome completo e e-mail de contato dessas funcionárias. Por isso, dados de remuneração, tempo de empresa e aniversário não foram compartilhadas pelo time de RH.

2.2
CUIDADO COM AS SUAS SENHAS

Seja no trabalho ou na vida pessoal, é importante que você adote senhas seguras para seus logins em plataformas digitais. Confira algumas dicas práticas abaixo:

CRIE SENHAS ÚNICAS PARA CADA APLICATIVO E SISTEMA

A mesma senha pra tudo? Jamais! Crie senhas únicas para cada aplicatico e claro, nunca utilize senhas pessoais na hora de proteger dispositivos corporativos.

ESCOLHA SEMPRE SENHAS FORTES

Combine letras maiúsculas, minúsculas, números e caracteres especiais em suas senhas. Além disso, evite utilizar dados pessoais, como seu nome e aniversário.

2.3
DADOS PESSOAIS NÃO ESTÃO APENAS NO MEIO DIGITAL: BOAS PRÁTICAS COM MATERIAIS IMPRESSOS

Muitas vezes relacionamos Privacidade e Proteção de Dados Pessoais com materiais digitais, mas documentos físicos também precisam do nosso cuidado.

EXEMPLO: Uma simples conta de luz revela dados pessoais como: nome completo, endereço de residência, número de documentos, gasto médio de energia e possíveis inadimplências do consumidor!

CUIDADO COM MATERIAIS IMPRESSOS:

- Armazene documentos físicos com dados pessoais em um lugar seguro.
- Ao descartar documentos, risque ou triture dados pessoais como nome e endereço, impossibilitando a leitura dessas informações.
- Se for imprimir algum material no seu trabalho, evite deixar documentos na bandeja da impressora ou em locais com circulação de pessoas.

2.4
CONECTE-SE COM SEGURANÇA

A tecnologia trouxe muitas facilidades para a nossa rotina, mas também novos cuidados que devemos adotar ao nos conectarmos. Confira as dicas abaixo:

SALVAR SENHAS: DESATIVADO

Ao acessar alguma conta, site ou aplicativo em *dispositivos públicos*, não esqueça de fazer logoff. Nesses casos, nunca habilite a conexão automática.

EVITE UTILIZAR REDES WI-FI PÚBLICAS

Sabe aquela rede wi-fi sem senha disponível no shopping ou no aeroporto? Nem sempre ela é uma conexão segura! Acesse apenas redes confiáveis, e entre em aplicativos bancários apenas em redes particulares da sua confiança.

UTILIZE APENAS APLICATIVOS OFICIAIS

Sempre baixe aplicativos diretamente das lojas oficiais, App Store (Apple) ou Play Store (dispositivos Android). Nunca baixe aplicativos de links não oficiais.

GET IT ON Google Play GET IT ON App Store

NÃO VINCULE SUAS CONTAS AO SEU E-MAIL PRINCIPAL

Não vincule o seu e-mail de recuperação de senha a um endereço acessível pelo mesmo dispositivo. ***Por exemplo:*** *caso seu celular seja roubado, e o e-mail para recuperação de senha esteja disponível no dispositivo, outra pessoa poderá se passar por você, trocar as suas senhas e impedir o seu acesso às contas!*

ADOTE MEDIDAS TÉCNICAS DE SEGURANÇA

Algumas funcionalidades podem aumentar a sua privacidade e segunça. Habilite no seus dispositivos um *número máximo de tentativas de desbloqueio*. Outra medida técnica eficiente é ativar a *autenticação de dois fatores* em suas contas.

NÃO CLIQUE EM QUALQUER LINK

Desconfie de links recebidos por aplicativos de mensagens, especialmente de contatos desconhecidos. Se ficar em dúvida, não clique no link recebido!

03.

BOAS PRÁTICAS: PESSOAS JURÍDICAS

QUAL O PAPEL DE UMA EMPRESA NA PROTEÇÃO DOS DADOS PESSOAIS?

As Leis de Proteção de Dados, além de garantirem os direitos das pessoas físicas em relação às suas próprias informações, **trouxeram para empresas maior segurança jurídica** para realizar atividades envolvendo dados pessoais. Assim, empresas de todos os portes e segmentos econômicos devem estar atentas a obrigações e cuidados relacionados à privacidade e proteção de dados pessoais.

3.1 ENTENDENDO AS ATIVIDADES

Antes de mais nada é importante que a empresa tenha conhecimento de quais operações envolvem o tratamento de dados pessoais, quais dados pessoais envolvidos, quem são os titulares, e por qual motivo a empresa realiza o tratamento de dados pessoais.

3.2 AVALIAÇÃO DE RISCO

Após mapear as atividades que envolvem dados pessoais, é necessário entender qual o risco de cada uma em relação aos direitos dos titulares. Atividades de alto risco exigem medidas adicionais, como o registro de documentos conhecidos como RIPD *(Relatório de Impacto à Proteção de Dados Pessoais)* ou DPIA *(Data Protection Impact Assessment).*

3.3 AVISOS P&PD NAS PLATAFORMAS

Buscando a **transparência**, toda empresa deve disponibilizar um Aviso de Privacidade e Proteção Dados Pessoais em suas plataformas, no qual a empresa deve declarar como os dados pessoais são tratados e para quais finalidades. *Esse aviso também é chamado de "Política de Privacidade".*

3.4
AVISOS P&PD INTERNOS

É indicado que as empresas adotem internamente Avisos de Privacidade e Proteção de Dados (também conhecido como Política de Privacidade para Colaboradores), explicando aos funcionários como os seus próprios dados pessoais são tratados dentro da empresa.

3.5
PRIVACY BY DESIGN

A preocupação com a proteção de dados pessoais desde a concepção de produtos e serviços é chamada de "Privacy by Design". Na prática, a metodologia traz para o início dos projetos a preocupação com privacidade. Confira no fluxo abaixo algumas perguntas que podem nortear a aplicação do Privacy by Design nos projetos da sua empresa:

3.6
CONTRATAÇÃO DE FORNECEDORES

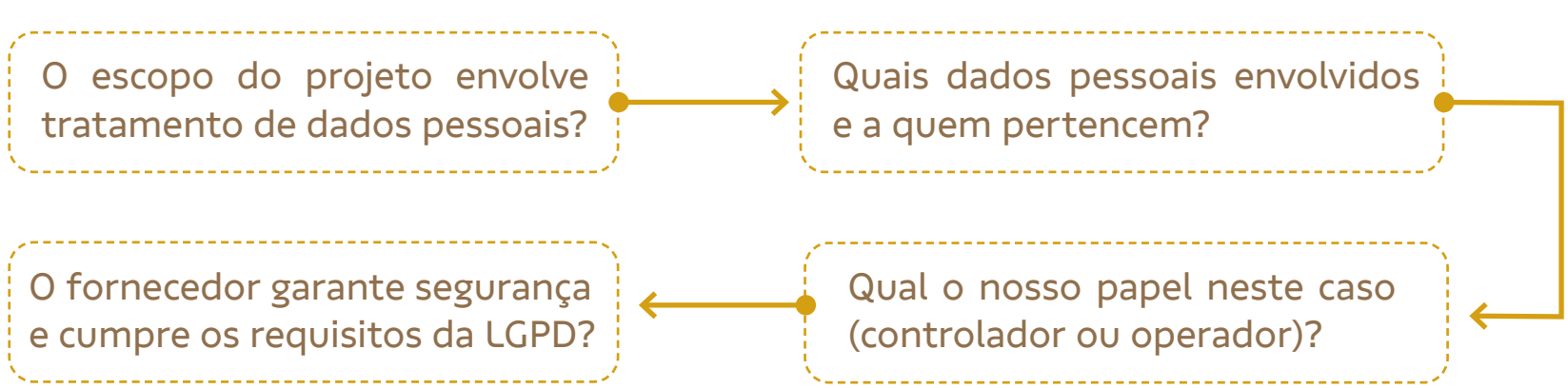
Para que todo o cuidado dentro de casa faça sentido, a empresa deve ter requisitos e normas internas para a contratação de fornecedores. Confira abaixo alguns pontos que devem ser levados em consideração:

01 AVALIE O FORNECEDOR

É importante que a empresa contrate fornecedores que estejam adequados às leis de proteção de dados pessoais e que adotem boas práticas relacionadas a privacidade e segurança da informação. **A empresa deverá definir os requisitos mínimos para a contratação de fornecedores.**

02 ENTENDA OS DETALHES DO PROJETO

Ao contratar um fornecedor para um projeto, é necessário entender:



03 ADOTE CLÁUSULAS CONTRATUAIS DE P&PD

Quando o escopo do projeto envolver tratamento de dados pessoais, é necessário que o contrato entre a empresa e o fornecedor traga cláusulas de privacidade e proteção de dados pessoais (P&PD). A existência de cláusulas específicas garantem a proteção dessas informações, o tratamento de dados pessoais de acordo com a lei, além de alocar a responsabilidade de cada parte em relação às atividades de tratamento.

A adequação dos contratos é feita pelo time responsável da empresa, a partir do detalhamento das operações e do papel de cada uma das partes nas atividades de tratamento de dados pessoais.

04.

F.A.Q:
O QUE VOCÊ PRECISA SABER SOBRE PROTEÇÃO DE DADOS PESSOAIS

4.1
COMO SEI QUAL LEI DEVE SER APLICADA?

RESPOSTA: Em geral, o que determina qual a lei de proteção de dados pessoais aplicável é a **localização** dos titulares desses dados. Por exemplo:

SE...	A LEI APLICÁVEL É:
Uma empresa brasileira com filial na Alemanha tratar dados de funcionários que residem na Europa	**GDPR** Não importa o país sede da empresa, o que deve ser observado é a localização dos titulares.
Sou mexicano, durante uma viagem fiz check-in em um hotel em São Paulo e forneci meus dados pessoais	**LGPD** Não importa a nacionalidade do titular, mas a sua localização.
Minha empresa é norte-americana e presta serviços para italianos de forma remota, coletando dados pessoais	**GDPR** Não importa onde os dados pessoais são armazenados, mas a localização do titular.
No Brasil, um médico digitalizou os prontuários físicos dos seus pacientes	**LGPD** O meio de operação de tratamento de dados pessoais não é relevante.

4.2
DADOS DE PESSOAS JURÍDICAS SÃO DADOS PESSOAIS?

RESPOSTA: De modo geral, dados de pessoas jurídicas não são considerados dados pessoais. Porém, em alguns casos, dados empresariais podem levar à identificação de pessoas físicas. Confira alguns exemplos abaixo:

É um dado pessoal	Não é um dado pessoal
mariasilva@empresa.com.br	contato@empresa.com.br
CPF de um fornecedor	CNPJ de uma empresa
O nome da empresa contém o nome completo do dono. Ex: João Silva LTDA	O nome da empresa é formado pelas iniciais dos sócios. Exemplo: ABC LTDA
Número de contato da empresa é o celular pessoal do sócio fundador	Número de contato da empresa é um telefone corporativo

4.3
PRECISO TER O CONSENTIMENTO DOS TITULARES SEMPRE QUE TRATAR DADOS?

RESPOSTA: Um dos principais mitos relacionados ao tratamento de dados pessoais é a falsa ideia de que sempre é necessário pedir o consentimento. Na maior parte das legislações, o consentimento é apenas **UMA** das bases legais disponíveis para justificar o tratamento de dados pessoais.

4.4
APÓS COLETARMOS OS DADOS PESSOAIS, PODEMOS UTILIZÁ-LOS PARA OUTRAS FINALIDADES?

RESPOSTA: Sim, empresas podem utilizar dados pessoais para uma finalidade distinta para a qual foram coletados, desde que a nova finalidade seja **legítima e cumpra com a lei aplicável.** Por exemplo, no Brasil:

Uma empresa de e-commerce coleta dados pessoais para que um cliente possa comprar online e receber o produto. → Após a entrega, a empresa envia ofertas relacionadas por SMS ao cliente, com base no **LEGÍTIMO INTERESSE.** → "Digite **SAIR** para deixar de receber ofertas": a empresa deve disponibilizar ferramenta de opt-out aos seus clientes.

4.5
PRECISO ME PREOCUPAR COM LEIS DE PROTEÇÃO DE DADOS AO TRATAR DADOS PESSOAIS DISPONÍVEIS EM BASES PÚBLICAS?

RESPOSTA: Depende da legislação vigente em cada país. Por exemplo:

NA LGPD E NO GDPR

No Brasil (LGPD) e na União Europeia (GDPR) a resposta é SIM, você precisa se preocupar! Ainda que as bases de dados sejam públicas, os princípios, direitos e obrigações previstos nas leis de proteção aos dados pessoais devem ser observados integralmente.

NA CCPA (CALIFÓRNIA)

Algumas leis são mais flexíveis em relação ao tratamento de dados pessoais disponibilizados em bases públicas. No CCPA, vigente na Califórnia (EUA), dados pessoais tornados públicos pelo próprio titular (por exemplo, em perfis abertos de redes sociais) **podem ser utilizados de forma menos restritiva.**

4.6
PODEMOS COLETAR INFORMAÇÕES, INCLUINDO DADOS PESSOAIS, DE SITES PÚBLICOS POR MEIO DE SCRAPING?

RESPOSTA: Nem sempre! Para coleta de dados em grande escala, muitas vezes empresas utilizam robôs, sistemas de varredura e armazenamento de dados, e outros métodos que extraem dados de forma automatizada, prática conhecida como scraping. Apesar de ser amplamente utilizada, nem todos os websites permitem que você realize essas atividades nas suas plataformas. Para saber se você pode realizar scraping em um site público, **antes de mais nada, você deve consultar os Termos de Uso do site ou plataforma, e a legislação aplicável no seu país. Por exemplo:**

RECEITA FEDERAL DO BRASIL

A Receita Federal do Brasil atualizou os termos de uso do seu site, proibindo que seja utilizado qualquer tipo de sistemas de varredura de dados na plataforma.

REDES SOCIAIS

As redes sociais mais conhecidas, entre elas Twitter, Facebook, Instagram e TikTok, proíbem em seus Termos de Uso a utilização de ferramentas de scraping nas plataformas.

4.7
PODEMOS CONTRATAR CLOUD FORA DO PAÍS?

RESPOSTA: Além dos cuidados para a contratação de fornecedores, como a comprometimento da empresa com a segurança e qualidade dos serviços (+ item 3.6), ao contratar serviços de cloud fora do país, sempre observe:

01 **PAÍS-ORIGEM:** Em qual país a empresa está localizada?

02 **PAÍS-DESTINO:** Onde estão localizados os servidores? Ou seja, onde são armazenados os dados pela empresa de cloud?

03 **NA LEI APLICÁVEL, HÁ REQUISITOS OU IMPEDIMENTOS PARA QUE A TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS OCORRA?**

Em geral, a transferência internacional poderá ocorrer se o país-destino garantir o mesmo nível de proteção do país-origem. Por exemplo:

UNIÃO EUROPEIA considerou que os EUA não ofereçam proteção suficiente aos dados pessoais. Por isso, indica-se a contratação de serviços de CLOUD em países europeus ou em países considerados adequados pela Autoridade Europeia, como Uruguai e Israel.

4.8
START UP'S E PEQUENAS EMPRESAS PRECISAM SEGUIR AS LEIS DE PROTEÇÃO DE DADOS PESSOAIS?

RESPOSTA: Todas as empresas, independentemente do tamanho, devem respeitar a legislação sobre proteção de dados. Contudo, alguns países possuem regras mais flexíveis para empresas de pequeno e médio porte.

NO BRASIL

Empresas de pequeno porte que não realizam tratamento de dados pessoais de alto risco, não precisam nomear um DPO e podem realizar o relatório de impacto simplificado.

NA CALIFÓRNIA

A lei se aplica a empresas que lucrem +U$25 mil por ano; ou que tratem dados pessoais de mais de 50 mil titulares; ou com 50% da receita resultante da venda de dados pessoais.

NO REINO UNIDO

Empresas de todos os portes devem seguir a lei e pagar uma taxa à autoridade por ano. Enquanto grandes empresas devem pagar £2,900, a maior parte dos pequenos negócios pagam menos de £100 por ano.

4.9
O QUE FAZER EM CASOS DE INCIDENTES DE SEGURANÇA?

RESPOSTA: Qualquer evento adverso relacionado à violação na segurança de dados pessoais, como acesso não autorizado, perda, roubo ou qualquer forma de tratamento inadequada ou ilícita é considerada um **incidente de segurança.**

Caso seja identificado um incidente de segurança, é necessário que as áreas responsáveis pela cibersegurança e privacidade sejam imediatamente informadas. Essa comunicação deve ser detalhada, contendo:

- descrição do ocorrido;
- causa;
- quais os dados pessoais envolvidos;
- quais os titulares afetados

É importante que haja o registro de todas as medidas tomadas pela empresa em resposta ao incidente de segurança.

Em alguns países, como no Brasil, os incidentes de segurança que possam causar prejuízo aos titulares de dados pessoais devem ser informados às Autoridades de Proteção de Dados e aos próprios titulares. **Confira sempre a legislação aplicável no seu país.**

4.10
O QUE ACONTECE SE UMA EMPRESA VIOLAR A LEI?

RESPOSTA: Existem penalidades previstas às empresas que descumprirem com as Leis de Proteção de Dados Pessoais. As penalidades variam de acordo com cada legislação. Existem diversos tipos de penalidades, como:

- **Advertências e imposições técnicas:** advertência com prazo para correção, bloqueio e/ou eliminação dos dados pessoais.
- **Multas:** a maior parte das legislações estabelecem multas com base no faturamento da empresa ou no tipo de infração.
- **Operacionais:** como a suspensão do funcionamento do banco de Dados, e a proibição parcial ou total do exercício da atividade.
- **Reputacional:** algumas leis trazem a publicização da infração, que pode afetar a imagem e a reputação da empresa no mercado.

NO BRASIL

A LGPD traz diferentes sanções em caso de descumprimento da lei, entre elas a **multa de até 2% do faturamento** anual da empresa no país (multa limitada a 50 milhões).

NA CALIFÓRNIA

A lei traz penalidades de até US$7.500 por violação. Além disso, garante que os consumidores o direito de processar as empresas que violem a lei.

UNIÃO EUROPEIA

De acordo com o GDPR, as autoridades de supervisão de cada país podem impor multas de **até 4% do faturamento anual global** ou de 20 milhões de euros (o que for maior).

4.11
COMO FICAM OS SEGREDOS COMERCIAIS E INDUSTRIAIS QUANDO FALAMOS DE PROTEÇÃO DOS DADOS PESSOAIS?

RESPOSTA: Nem todos os dados da empresa podem ser compartilhados em nome da transparência. Informações que revelem segredos industriais e comerciais são regulados por outros tipos de lei. A sua empresa deve estar preparada para orientar os colaboradores sobre este assunto.

seus dados, suas regras.

Nós plantamos o futuro.
Suzano - Time P&PD

ppd.suzano.com.br

suzano
nós plantamos o futuro