PACTO DE PROMOÇÃO
DA EQUIDADE RACIAL

# POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

PACTO DE PROMOÇÃO DA EQUIDADE RACIAL

# POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

| Histórico | |
|---|---|
| Área | Proteção de Dados pessoais |
| Data \| Versão | Setembro 2022\| v1 |

## Escopo da Política

Nós quantificamos e apoiamos a equidade na prática.

Esta é a nossa Política de Proteção de Dados Pessoais.

Aqui estabelecemos a estrutura de governança e os procedimentos que seguimos para garantir que o direito à privacidade e à proteção de dados pessoais seja realidade em todas as nossas atividades.

As regras desta Política existem para que os dados pessoais utilizados no dia a dia e as novas atividades sejam pautadas pelos princípios da lei e pelas melhores práticas de proteção de dados disponíveis atualmente.

Esta Política se aplicará a qualquer pessoa que faça parte dos quadros de colaboradores do Pacto pela Equidade Racial e se você for um "Participante", "Homologador" ou "certificador", prestador de serviço se, em algum momento, você teve acesso a dados pessoais.

## Referência Normativa

As regras desta Política foram elaboradas para que estejamos em conformidade com a legislação de proteção de dados pessoais aplicável no Brasil, onde atuamos.

Para tanto, utilizamos como referências as legislações e padrões estabelecidos no Brasil, ou seja, o Código de Defesa do Consumidor, o Marco Civil da Internet e o seu Decreto Regulamentador, a Lei Geral de Proteção de Dados Pessoais, a Lei de Acesso à informação, normas setoriais e regulatórias aplicáveis e a ISO/IEC 27701 *(Diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um sistema de Gestão de Privacidade da Informação (SGPI)*.

## Definições

- Certificadoras: Entidades responsáveis (i) pelo cálculo do IEER dos Participantes; (ii) pela emissão do Laudo de Certificação; e (iii) a partir do segundo ano da emissão de um Laudo de Certificação, pela verificação da efetiva implantação e observâncias das ações afirmativas e realização dos investimentos em equidade racial, observados os termos deste Regimento e as orientações emitidas pelo Conselho Deliberativo, nos termos do artigo 17 do Regimento interno do Pacto.

- Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

- Controlador: pessoa a quem competem as decisões referentes ao tratamento de dados pessoais.

- Dado pessoal sensível: 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. Algumas jurisdições podem incluir outros dados ou circunstâncias da vida privada, como hábitos pessoais, condição socioeconômica, ou quaisquer dados que possam dar origem à discriminação ou implicar risco grave ao titular.

- Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

- Encarregado: pessoa indicada para atuar como ponto focal sobre questões de proteção de dados, inclusive comunicação com os titulares e as autoridades de proteção de dados pessoais.

- Homologadoras: entidades responsáveis pela capacitação e habilitação das instituições certificadoras de auditoria e consultoria que desejarem obter o credenciamento e autorização necessários para atuação como entidade, conforme os requisitos do artigo 12 do Regimento Interno do Pacto.

- Índice ESG de Equilíbrio Racial ("IEER"): medirá a representatividade negra em três níveis hierárquicos das empresas e entidades integrantes do Pacto (direção, gerência, não liderança) e será calculado por uma certificadora.

- Incidente de Segurança: evento em que há perda da confidencialidade, integridade ou disponibilidade de informação.

- Operador: pessoa que realiza o tratamento de dados pessoais em nome do controlador.

- Relatório de impacto à proteção de dados pessoais: análise de risco sobre atividades de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação.

- Segurança da informação: preservação da segurança da confidencialidade, integridade e disponibilidade.

- Titular de dados: pessoa natural a quem se referem os dados pessoais que são tratados.

- Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

- Tratamento: toda operação realizada com dados pessoais.

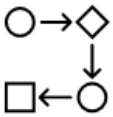
- Participantes: empresas e entidades que aderem aos compromissos do Pacto submetendo-se ao cálculo do IEE e à certificação da organização.

## Princípios para o tratamento dos dados

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) contém uma série de princípios que precisam ser efetivados no dia a dia das atividades que envolvam dados pessoais.

**Princípio da Finalidade:** Coletar apenas os dados necessários para uma finalidade específica de tratamento – a atividade para a qual os dados serão tratados deve estar muito clara para a nossa organização.

Por exemplo: se você deseja realizar um evento, pode ser necessário coletar dados pessoais para viabilizar a entrada das pessoas no evento. Como os dados foram coletados para realização da do evento (finalidade), não é possível inserir os respondentes no *mailing* do Pacto automaticamente, isso significaria um desvio de finalidade de uso dos dados pessoais. Os dados sempre têm que estar atrelados a uma finalidade que justifique a sua coleta.



**Princípio da Adequação:** Sempre garantir que os dados estão sendo usados para as mesmas finalidades que, inicialmente, justificaram a sua coleta e que foram informadas aos titulares.

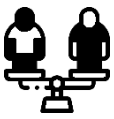
Por exemplo: Para realização de uma pesquisa a respeito das posições que pessoas não-brancas ocupam na empresa, não devem ser coletados dados relacionados à orientação sexual do participante, caso isto não faça parte dos propósitos declarados da pesquisa.

**Princípio da Necessidade:** o Pacto limita o tratamento de dados pessoais ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Por exemplo: se para participar de determinado evento via Zoom a pessoa precisa fornecer nome, e-mail, telefone, raça, cargo e gênero, podem estar sendo coletados mais dados do que o que é necessário, uma vez que para se conectar ao *zoom* só é necessário coletar nome e e-mail do participante. A análise da necessidade deve ser feita caso a caso.

**Princípio da Transparência:** O Pacto deve garantir aos titulares dos dados pessoais informações claras, precisas e facilmente acessíveis sobre a realização do tratamento de seus dados, e possibilitar que todas as dúvidas sobre o tratamento sejam enviadas para o(a) encarregado(a).

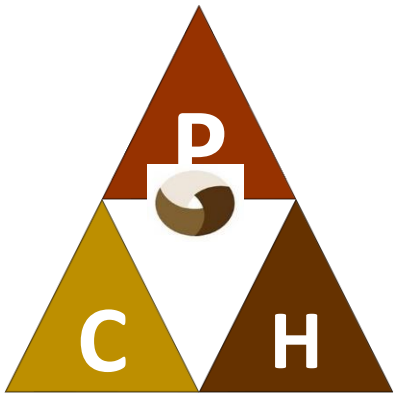
**Princípio da Segurança e prevenção:** Utilizar sempre medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação o u difusão indevidas ou inadequadas.



**Princípio da Não Discriminação:** A nossa organização atua para reduzir a discriminação ligada à raça e origem ética e isso também é um dos objetivos da LGPD! A lei proíbe que os dados pessoais sejam utilizados de forma a

## Contexto da organização

O Pacto pela Democracia Racial atua como controlador de dados pessoais dos titulares, sejam clientes, colaboradores ou representantes legais das homologadoras, colaboradoras e participantes. Para nós é importante estar em conformidade com a legislação do Brasil como um de todos os países nos quais estamos presentes.




Temos o compromisso de atuar para reduzir a discriminação racial e étnica e fazemos isso por meio do fomento ao processo de cálculo do Índice ESG de Equilíbrio Racial (“IEER”). Para isso, viabilizamos o contato entre os participantes (“P”), as certificadoras (“C”) e as homologadoras (“H”).

**No geral não tratamos os dados pessoais e pessoais sensíveis dos colaboradores dos nossos participantes, utilizados para criar o IEER, só atuamos para viabilizar o contato dos participantes com as Certificadoras selecionadas para fazer isso.**

Na eventualidade de isso acontecer, o motivo deverá ser registrado e os titulares dos dados deverão ser informados.

De toda forma, podemos acessar os dados pessoais sensíveis dos líderes das organizações Homologadoras, para garantir que suas diretorias ou coordenações são compostas por 51% ou mais de pessoas autodeclaradas negras, conforme exposto no artigo 12 do Regimento interno do Pacto.

## Governança Corporativa

O encarregado pela proteção de dados é uma pessoa física ou jurídica que assume a função de ponto de contato entre os titulares de dados, a Autoridade Nacional de Proteção de Dados (ANPD) e a empresa.

De forma mais específica, são suas funções:

- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- receber comunicações da autoridade nacional e adotar providências;
- orientar os funcionários e os contratados da empresa a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, quando julgar necessário ou quando receber solicitação dos colaboradores nesse sentido;
- executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;
- identificar riscos ligados a determinadas atividades de tratamento e requerer ou produzir um Relatório de PACTO à Proteção de Dados Pessoais (art. 38).

### Órgão Encarregado de Proteção de Dados

No Pacto, as funções do Encarregado de proteção de dados são exercidas de forma colegiada, por um comitê, devido ao reduzido quadro de profissionais da organização. Esse comitê é apoiado tecnicamente, quando necessário por escritório de advocacia especializado.

No caso do Pacto, o encarregado de proteção de dados pode ser contatado por meio do seguinte endereço eletrônico: contato@pactopelaequidaderacial.org.br .

## Condições de coleta e tratamento

Por meio da presente Política, o PACTO estabelece um fluxo padrão para o respeito à LGPD, conforme as etapas abaixo destacadas:

O primeiro passo ao ver que determinadas atividades envolvem dados pessoais é entender que tipos de dados serão utilizados. Lembre-se que os dados podem ser pessoais (ex.: nome, cpf, endereço, telefone) ou pessoais sensíveis (ex.: raça, origem étnica, orientação sexual, biometria, dados de saúde, opiniões políticas etc).

**1. Identificação dos dados pessoais tratados nas suas atividades/projetos - são pessoais ou pessoais sensíveis?**

Também é importante considerar se há tratamento de dados pessoais de crianças (menores de 12 anos) na atividade que você está realizando, pois é necessário obter o consentimento específico dos pais para o tratamento destes dados.

Após entender que tipos de dados podem ser tratados durante uma atividade, é importante registrar o percurso dos dados pela nossa organização. O registro dos tipos de tratamento de dados vai desde as atividades de gestão de pessoas, até atividades de marketing, pesquisa e etc. Toda atividade que envolva o tratamento de dados pessoais deve ser registrada, e esse registro deve ser atualizado conforme novas atividades e projetos surgem.

**2. Registro da atividade no formulário de mapeamento.**

Cada atividade que envolve o tratamento de dados pessoais deve ser suportada por uma justificativa adequada, à qual chamamos de “base legal”. Essa justificativa também deve constar no registro de tratamentos de dados feito pela organização. Lembre-se: nem todo tratamento necessita de consentimento do titular pois a lei traz justificativas próprias para cada situação e o consentimento é só mais uma delas.

**3. Identificação da base legal que justifica o tratamento dos dados.**

Em respeito ao princípio da boa-fé, aconselha-se a definição de apenas uma base legal ("justificativa") para cada atividade de tratamento de dados pessoais. Para identificar a base legal adequada deve-se refletir nos seguintes elementos:

**(ORIGEM DO DADO + TIPO DO DADO + FINALIDADE) x PRINCÍPIOS = BASE LEGAL**

A importância de definir a base legal é não só verificar se há fundamento para o tratamento, mas também definir como se efetivará a transparência do tratamento. Se a base legal for o consentimento, a forma como o aviso de transparência será construída é diferente daquela para uma atividade realizada sob a justificativa de realização de pesquisa, por exemplo.

As dez justificativas para o tratamento de dados pessoais presentes na Lei Geral de Proteção de Dados (LGPD) são:

- consentimento
- obrigação legal (ou regulatória)
- execução de políticas públicas
- realização de estudos (por órgão de pesquisa)
- execução de contratos ou procedimentos preliminares relacionados ao instrumento contratual
- exercício regular de direitos
- proteção da vida
- tutela da saúde (por profissionais, serviços de saúde e autoridade sanitária
- legítimo interesse
- proteção ao crédito

Para os dados pessoais sensíveis há outras bases legais que autorizam o seu tratamento. Para dados sensíveis, estão excluídas as bases de (i) legítimo interesse, (ii) proteção ao crédito e (iii) cumprimento do contrato.

## 4. Elaboração de medidas de transparência ou de coleta válida de consentimento para o titular de dados, conforme o caso.

O consentimento só deve ser usado como justificativa quando isso for necessário e adequado à situação. Para isso é preciso garantir as seguintes condições:

### 1) O consentimento deve ser específico.

Não se pode consentir com uma lista de finalidades diversas de modo genérico, em um aceite único. O consentimento deve ser para uma ou outra finalidade específica, uma vez que autorizações genéricas são consideradas nulas (art. 8º, da LGPD). Se for identificada a necessidade de tratar os dados para atender a mais de uma finalidade devemos identificar se o consentimento é necessário para ambas, e, se sim, obter um aceite para cada uma delas.

### 2) O consentimento precisa ser livre.

O titular de dados pessoais não pode ser obrigado a fornecer os dados pessoais para continuar a relação com o PACTO. Se entendemos que, sem os dados da pessoa não poderemos oferecer nossos serviços. Outra justificativa deve ser escolhida para garantir a conformidade do tratamento dos dados pessoais.

O consentimento só é válido se as pessoas puderem fornecê-lo de forma livre, ou seja, continuar na relação, sem fornecer os dados pessoais.

*Por exemplo: para baixar determinados conteúdos, os usuários do site não precisam necessariamente fornecer dados pessoais. Normalmente as organizações requerem os dados pessoais antes de liberar o conteúdo para identificar um possível público interessado naquele conteúdo. Nesse caso, se o fornecimento de dados for opcional, ou seja, se houver a possibilidade de o usuário baixar o arquivo sem fornecer os dados pessoais, falaremos de um consentimento livre. Se o fornecimento de dados for obrigatório, então o consentimento não será livre.*

### 3) O consentimento precisa ser informado.

As pessoas só podem consentir com atividades de tratamento de dados pessoais que elas entendem totalmente como acontecerão. Por isso, espera-se que as organizações sejam transparentes em relação à forma como tratam os dados pessoais.

### 4) O consentimento precisa ser inequívoco:

Isso quer dizer que não pode existir dúvida quanto à manifestação de vontade dos titulares de dados e essa vontade também não pode ser presumida.

*Por exemplo: a criação de uma caixa de seleção pré-selecionada ou de buscar o consentimento no meio de um texto muito grande, com várias outras informações, torna a coleta incorreta e inválida. Para obter o consentimento inequívoco é preciso que seja feita uma pergunta clara sobre o consentimento, com a indicação de todas as finalidades pretendidas, com uma caixa de seleção para cada uma dessas finalidades em que o titular tenha que assinalá-las ativamente.*

**5)** Gerir os direitos relativos aos dados tratados com base no consentimento.

Conforme explicado na descrição do princípio da "finalidade" é preciso que haja muita compreensão sobre os motivos que justificam a coleta dos dados pessoais. Isso porque os titulares dos dados podem desejar exercer os direitos específicos em relação às informações que foram coletadas com base no consentimento:

a) Obtenção da informação quanto à consequência de não fornecer o consentimento;
b) Solicitação de eliminação dos dados da base de dados a qualquer tempo;
c) Revogação do consentimento para aquela determinada finalidade de uso dos dados.

Assim, o consentimento só pode ser utilizado quando for possível efetivar todos esses direitos e quando ele for LIVRE, ESPECÍFICO, INFORMADO E INFORMADO. **No caso dos dados pessoais sensíveis ele ainda deverá ser DESTACADO, ou seja, em frase específica para a finalidade de uso dos dados pessoais sensíveis.**

## 4. Elaboração de medidas de transparência ou de coleta válida de consentimento para o titular de dados, conforme o caso.

<u>Sempre elaborar um aviso de transparência</u>

Sempre é necessário elaborar um aviso de transparência sobre a finalidade e compatibilidade dos dados utilizados para tal finalidade, em consonância com os princípios da LGPD.

É importante que o aviso seja informativo (de fácil compreensão) e específico, na medida do possível. Isso porque, de acordo com o art. 9º da LGPD, o titular tem direito ao **acesso facilitado às informações** sobre o tratamento de seus dados, que deverão ser disponibilizadas de **forma clara, adequada e ostensiva** acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso.

## A adoção de medidas de Segurança Técnicas e Administrativas

O tratamento de dados pessoais sempre deve sempre conter medidas técnicas e administrativas para garantir a segurança dos dados pessoais tratadas pelo Pacto:

| Exemplos de medidas técnicas | Exemplos de medidas administrativas |
|---|---|
| a) Adote a confidencialidade para o envio de *e-mails* contendo informações pessoais;<br>b) Adote técnicas de pseudonimização: ou seja, delete os dados que identificam | c) Apague da base de dados compartilhada qualquer dado que não seja extremamente necessário para a realização da atividade que demanda o compartilhamento.<br>d) Se o repasse dos dados é para a mídia, verifique sempre se se trata de um veículo de informação confiável antes do compartilhamento e se a matéria que será produzida pode vir |

diretamente os sujeitos referidos (como nome, CPF, e-mail) e substitua-os por um pseudônimo (confira o Anexo III, com técnicas de anonimização e pseudonimização dos dados pessoais);

a prejudicar a imagem do PACTO. Lembre-se, a LGPD não se aplica para finalidades jornalísticas desde que a reportagem seja feita por um veículo de comunicação reconhecido como tal.

e) Sempre busque fechar acordos sobre a proteção de dados antes de enviá-los a terceiros – as cláusulas dos contratos que envolvam o compartilhamento de dados pessoais devem ser robustas e apresentar medidas técnicas e administrativas para as informações transferidas;

f) Sempre verifique o grau de conformidade do parceiro comercial antes de efetivar a contratação, conforme o Anexo I – Checklist de avaliação de terceiros.

## O compartilhamento de dados pessoais:

Dentro das nossas atividades diárias é natural que haja necessidade de compartilhar os dados pessoais que tratamos. Isso não é proibido, mas deve ser feito com cuidado, se não a chance de um incidente envolvendo dados pessoais pode aumentar.

Assim, o cuidado com o compartilhamento de dados pessoais está atrelado aos princípios da finalidade, adequação, segurança e prevenção.

Lembre-se: Existem vários tipos de incidente:

(a) acesso indevido aos dados pessoais;
(b) utilização dos dados para finalidade diversa daquela informada inicialmente ao titular;
(c) alteração dos dados com prejuízo aos titulares etc.

Por isso, sempre que for compartilhar os dados pessoais dentro da organização ou com pessoais e empresas de fora do PACTO, quem for responsável pelo procedimento deve responder às seguintes questões:

| | |
|---|---|
| 1. Os dados que precisamos compartilhar são pessoais ou pessoais sensíveis? | Ao responder essa primeira pergunta, conseguimos identificar o tipo de risco envolvido no compartilhamento de dados. Isso porque o compartilhamento de dados pessoais sensíveis pode impor maior risco de discriminação abusiva dos titulares de dados a quem eles se referem. |
| 2. Os dados que precisamos compartilhar já são acessados pelas pessoas ou organizações a quem irá receber as informações em nosso poder?<br><br>3. Podemos ver risco de que a pessoa ou empresa irá utilizar os utilizar os dados pessoais compartilhados por nós para objetivos diferentes daqueles para os quais nós usamos os dados? | Por outro lado, ao responder às perguntas 2 e 3 conseguimos identificar a possibilidade de acesso indevido ou de desvio de finalidade por parte da pessoa ou empresa para a qual os dados pessoais estão sendo transferidos.<br><br>Isso é importante para evitar que os dados sejam utilizados de forma diferente do que foi informado para os titulares de dados pessoais. |

Se a resposta para as perguntas em vermelho for positiva, contate o comitê encarregado para que ele possa analisar a relação e definir quais mecanismos de proteção podem ser aplicados a ela, para garantir a conformidade com a lei. Sugerimos que o e-mail de comunicação contenha as informações ao lado.

1. Com quem os dados serão compartilhados (pessoa, consultor, outra organização ou empresa).
2. Por qual motivo os dados pessoais serão compartilhados (por exemplo: execução de parte do projeto comandado pelo PACTO, análise conjunta de uma mesma base de dados pessoais, prestação de contas sobre um projeto etc.)
3. Quais são as finalidades para as quais a pessoa/organização, com quem os dados serão compartilhados, podem utilizar tais dados pessoais?
4. Existência de cláusula contratual prevendo os cuidados que a pessoa ou organização deve ter com os dados pessoais transferidos pelo PACTO.

## A adoção de padrões de Privacidade desde o começo dos projetos

Sempre que um novo projeto ou atividade for criada, é importante que ela seja estruturada para garantir a privacidade e a proteção dos dados pessoais desde o princípio da captação dos dados pessoais para essa atividade. Para isso existem alguns princípios de uma prática denominada como "Privacidade desde o Princípio" ("*Privacy by design")* que podem ser úteis:

| Princípio | Na prática |
|---|---|
| **Atuação preventiva e não reativa**<br>As atividades que envolvem o tratamento de dados devem ser organizadas de forma a evitar práticas de desvio de finalidade, compartilhamento inseguro e outros tipos de conduta que podem colocar em risco os titulares de dados pessoais. | Orientamos constantemente os colaboradores que estão trabalhando no projeto, sobre como os dados pessoais devem ser tratados, em acordo com esta política e a política externa de proteção de dados pessoais |
| **Privacidade como padrão**<br>Significa efetivar princípios da LGPD garantindo que apenas o mínimo de aspectos dos titulares de dados será utilizado para atingir o resultado do projeto. | • Tornar os critérios de coleta de dados o mais restrito possível.<br>• Evitar perguntas que possam revelar dados pessoais sensíveis a menos que isso seja essencial para a atividade (raça, orientação sexual, concepção política etc).<br>• Limitar o uso de dados pessoais às finalidades para as quais eles foram coletados e garantir que haja uma base legítima para o tratamento.<br>• Restringir o acesso aos dados pessoais às partes envolvidas no tratamento de acordo com o princípio da "necessidade de conhecer" e de acordo com a função por trás da criação de perfis de acesso diferenciados.<br>• Definir prazos para a retenção dos dados.<br>• Proibir a vinculação não autorizada de fontes independentes de dados (cruzamento de dados). |

| | |
|---|---|
| | ● Definir o ciclo de vida dos dados desde o início do projeto.<br>● Analisar seriamente os riscos que o tratamento de dados pode trazer para os titulares, que fornecerão os dados ao PACTO, e contatar o DPO em caso de uso de inteligência artificial ou outro tipo de tecnologia que possa ocasionar impactos relevantes para os titulares de dados.<br>● Documentar as decisões tomadas no mapeamento de dados do PACTO, para atualização constante do documento. |
| Privacidade incorporada ao design do projeto<br>Considere a privacidade e os princípios de proteção de dados como um requisito essencial dentro do projeto. | |

| | |
|---|---|
| Funcionalidade total<br><br>Normalmente a ideia de garantia de privacidade é atrelada à ideia de perda de algum tipo de funcionalidade, de possibilidade de pesquisa, ou de benefício que pode ser entregue para os titulares de dados. A ideia atrelada à aplicação deste princípio é balancear a privacidade do beneficiário das atividades ou dos projetos sem perda em razão da garantia deste direito. | ● na construção do projeto buscar a harmonia dos interesses do PACTO e dos direitos do beneficiário;<br>● gerenciar de forma responsável a possibilidade de impacto que as escolhas do projeto podem trazer para os titulares de dados. |

| | |
|---|---|
| Segurança de ponta a ponta durante o ciclo de vida dos dados<br><br>Deve haver uma análise prévia, considerando o trajeto dos dados pessoais, a respeito de quais medidas técnicas (TI) e administrativas podem ser adotadas para garantir a segurança dos dados pessoais dentro das atividades do projeto, em cada fase do ciclo de tratamento dos dados. | ● adoção de técnicas de pseudonimização ou anonimização desde o início do projeto;<br>● classificação e organização das operações de tratamento e dados com base em perfis de acesso;<br>● adotar criptografia no armazenamento dos dados;<br>● garantir a destruição segura e garantida das informações no final de seu ciclo de vida. |

**Visibilidade e transparência**

A adoção de medidas de transparência pode ser muito importante para a mitigação de riscos regulatórios atrelados à proteção de dados pessoais.

- Garantir o uso dos dados para finalidades determinadas e que sejam claramente expostas para os titulares de dados;
- Informar os titulares de dados quanto a eventuais compartilhamentos de dados pessoais;
- Entender se parceiros dos projetos podem fazer outros usos para os dados pessoais e como isso pode impactar a PACTO e quem deverá informar os titulares de dados a respeito;
- Se for o caso estabelecer canais claros para o exercício de direito, definir quem deverá ser contato para isso, se o parceiro do PACTO ou ele próprio.

---

**Manter o usuário no centro da preocupação do desenvolvimento do projeto**

Tenha em mente sempre que os dados pessoais são uma parte da personalidade do usuário e, por isso, desenvolver um projeto ou atividade que efetive a proteção desse direito é muito importante.

- garantir mecanismos de efetivar o consentimento livre, específico e informado;
- permitir o acesso livre dos titulares aos seus dados pessoais

## O fim do tratamento dos dados pessoais – Períodos de retenção dos dados

**dados pessoais coletados e utilizados pelos controladores devem ser descartados**

Art. 15º

.

- Verificação de que a finalidade de uso dos dados foi alcançada e que eles não são mais necessários;
- o fim de um período predeterminado de tratamento (por exemplo, prazo máximo estabelecido em disposição contratual);
- a comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento;
- a determinação da Autoridade Nacional de Proteção de Dado (“ANPD”).

**os dados podem ser conservados pelo controlador mesmo após o término do tratamento**

Art. 16º

- Caso a retenção dos dados seja necessária para cumprir uma obrigação legal/regulatória de armazenamento, auditoria, fornecimento dos dados, resposta a eventuais questionamentos judiciais e administrativos;
- Se os dados estiverem em uso para pesquisa conduzida por órgão de pesquisa, garantida a sua anonimização;
- Caso eles devam ser transferidos a terceiros;
- Em caso de uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. Nestes casos, o titular de dados não necessita ser notificado.

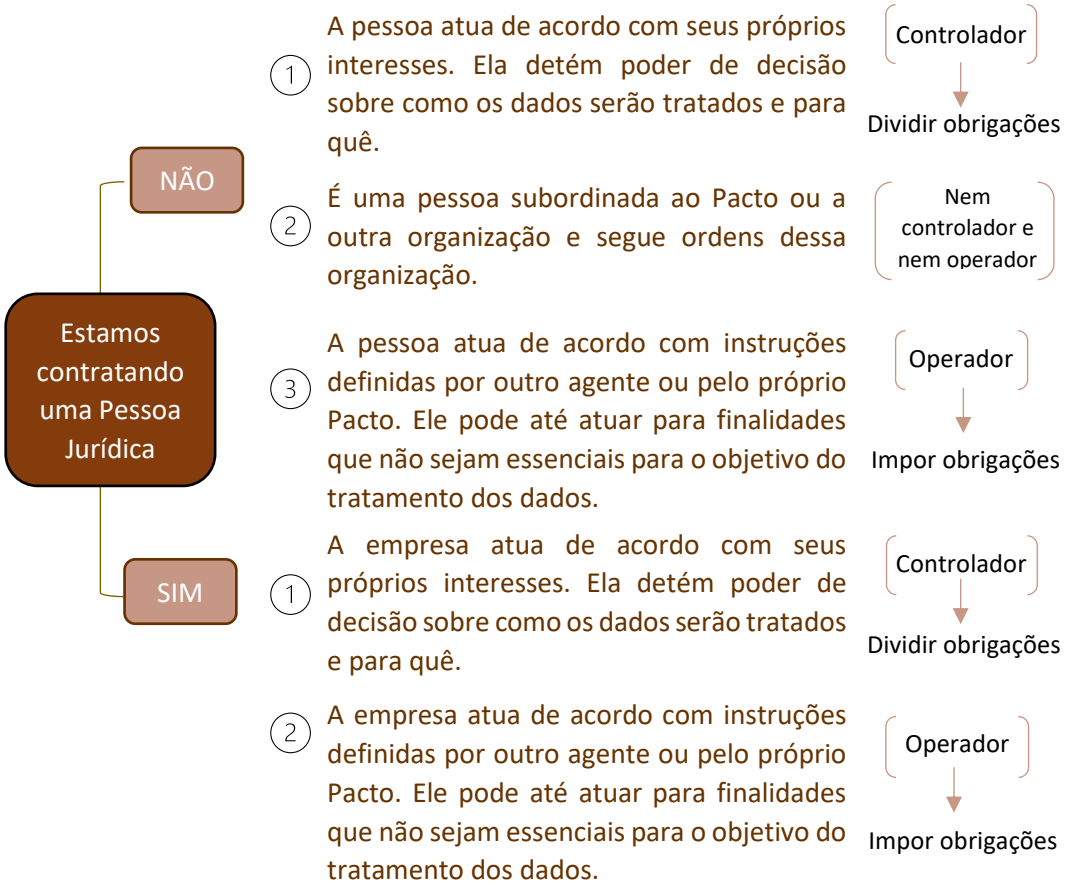
Atenção: As previsões dos artigos 15 e 16 se aplicam somente quando não existe qualquer outra finalidade de uso dos dados. Se os dados forem utilizados para outra finalidade, o controlador deve decidir optar por uma das justificativas dos artigos 7º ou 11º da lei. Reunimos no ANEXO II hipóteses comuns de armazenamento de dados legitimados pelas bases legais mais apropriadas.

## Avaliações de terceiros e contratos

Antes de fechar um contrato é necessário que a empresa ou organização que trata dados pessoais verifique o nível de conformidade daquele prestador de serviço que está sendo contratado. Para isso, indicamos a aplicação do Checklist presente no Anexo à essa política.

Enquanto acontece o preenchimento desse questionário é importante entender a posição do dos contratados e definir qual a posição do PACTO:

Já sabemos que se o PACTO tiver qualquer finalidade própria de tratamento dos dados pessoais a organização será controladora dos dados pessoais. Ela será operadora somente se não tiver qualquer objetivo próprio que dependa dos dados pessoais compartilhados com a outra pessoa/organização.



## Transferências Internacionais

Em caso de necessidade de transferência de dados para fora do Brasil é necessário verificar se a legislação daquele país é similar à do nosso país. Por exemplo, os países da União Europeia estão submetidos à Leis de Proteção de Dados igualmente ou até mais protetivas que a do Brasil, sendo considerados seguros para a transferência internacional de dados pessoais. Já os Estados Unidos da América, não possuem uma Lei federal sobre o tema, apresentando-se como uma opção menos segura para a transferência.

## Monitoramento e melhoria

O PACTO mantém e monitora continuamente a sua estrutura de proteção de dados pessoais considerando a necessidade de melhoria contínua dos processos de proteção das informações a seu dispor. Isso ocorre por meio de aplicação de checklists e do monitoramento dos posicionamentos das autoridades internacionais.

## Resposta aos incidentes de segurança

### 1 Identificação e notificação interna do incidente

Cientes do que significa um incidente de segurança - ou seja, qualquer situação de vulneração da integridade, disponibilidade ou confiabilidade das informações – devemos sempre nos comunicar sobre a possibilidade de ocorrência dessas situações. A partir dessa notificação inicial as etapas posteriores serão destravadas.

Para conferir o que pode ser considerado um incidente de segurança, todos devem se familiarizar com o tema através do seguinte vídeo: **Risco e Incidentes de Segurança.**

### 2 Comitê de crise

A partir da notificação, deve ser formado um Comitê de Crise e se não houver pessoas suficientes para isso, recomenda-se a inclusão de escritório especializado na situação e da mobilização do staff disponível para lidar em tempo parcial com a situação. Preferencialmente, o comitê deve contar com pessoas de diferentes áreas e expertises, como Segurança da Informação, TI, Jurídico, Proteção de Dados etc., para garantir a multidisciplinaridade de atuação, quando do Incidente.

Quando de ocorrências pontuais, sempre será necessário envolver pessoas da área/departamento afetado, sobretudo quando da avaliação de impacto do incidente e das medidas a serem adotadas para mitigar os efeitos da ocorrência.

## 3 Avaliação de risco do Incidente com Dados Pessoais

Para saber se será necessário notificar às autoridades e os titulares de dados o risco das consequências do incidente, **para os titulares de dados,** deverá ser avaliado. Somente o risco de dano relevante para os titulares de dados deve ser notificado, ou seja, situações nas quais os titulares dos dados podem ter sido colocados em risco. É muito importante ter em mente que nem todo incidente precisa ser comunicado à ANPD ou, muito menos, aos titulares de dados pessoais.

A avaliação do risco do Incidente ocorrido considerará duas variáveis: o volume de dados pessoais acessados através do incidente e a sensibilidade dos dados pessoais afetados pelo Incidente.A junção desses dois valores, nos eixos da escala, ditará se o risco envolvido é alto, médio ou baixo. Veja a seguir:

| | AVALIAÇÃO DE RISCO DO INCIDENTE COM DADOS PESSOAIS | | |
|---|---|---|---|
| ALTO VOLUME DE DADOS PESSOAIS ACESSADOS | Alto | Alto | Alto |
| MÉDIO VOLUME DE DADOS PESSOAIS ACESSADOS | Médio | Alto | Alto |
| BAIXO VOLUME DE DADOS PESSOAIS ACESSADOS | Baixo | Médio | Médio |
| | BAIXA SENSIBILIDADE DE DADOS PESSOAIS AFETADOS NO INCIDENTE | MÉDIA SENSIBILIDADE DE DADOS PESSOAIS AFETADOS NO INCIDENTE | ALTA SENSIBILIDADE DE DADOS PESSOAIS AFETADOS NO INCIDENTE |

Volume de dados pessoais

Sensibilidade dados pessoais

Para avaliar o risco é necessário identificar e determinar essas duas variáveis (volume e sensibilidade) e, em seguida, encontrar o ponto de intersecção das variáveis na escala. Nesse sentido, os parâmetros de volume e sensibilidade são os seguintes:

| **Volume de pessoas atingidas** (quanto menos pessoas possivelmente atingidas, menor o risco[1] atrelado ao | **Sensibilidade dos dados** (quanto menor a sensibilidade dos dados afetados, menor o risco atrelado ao vazamento dos dados pessoais) |
|---|---|

[1]Sugerimos que esses valores sejam ponderados, quando da apresentação dessas diretrizes em reunião específica com o escritório. Isso porque algumas opiniões sobre esses parâmetros consideram percentuais da população nacional.

| Incidente) | | | |
|---|---|---|---|
| Risco relevante para os titulares de dados | Descrição | Risco de dano relevante para os titulares de dados | Descrição |
| Alto | X pessoas podem ter sido afetadas pelo incidente afetadas pelo incidente | Alto | Dados Pessoais de crianças ou adolescentes, Dados Pessoais Dados Sensíveis ou que possam gerar discriminação ao titular; dados bancários, de pagamento ou de proteção ao crédito, pesquisa que pode revelar o posicionamento político dos entrevistados |
| Médio | Y pessoas podem ter sido afetadas pelo incidente afetadas pelo incidente | Médio | Dados Pessoais imediatamente identificáveis (e.g. nome, e-mail, CPF), combinados ou não com informações comportamentais (e.g. histórico de atividades, preferências etc.) |
| Baixo | Z pessoas podem ter sido afetadas pelo incidente afetadas pelo incidente | Baixo | Dados anonimizados, Dados Pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), Dados Pessoais de difícil identificação |

Avaliado o risco, segundo as diretrizes acima fornecidas, com o apoio da régua de risco, a atuação do Comitê de Crise, do Encarregado e, até, da assistência jurídica externa deverá considerar o seguinte:

| **Risco baixo**<br>O Comitê deve se reunir para avaliar a questão imediatamente e: | **Risco médio**<br>O Comitê deve se reunir para avaliar a questão imediatamente e: | **Risco Alto**<br>O Comitê deve se reunir para avaliar a questão imediatamente e atuar exclusivamente para solucionar a questão. |
|---|---|---|
| ● Documentar os motivos pelos quais o incidente foi considerado não relevante. | ● Estipular as medidas de correção imediatas para a área e colaboradores diretamente envolvidos no Incidente, | ● Alocar o(a) líder da área ou projeto afetado onde o Comitê de Crise estiver trabalhando; |

| | | |
|---|---|---|
| | registrando as recomendações e as execuções;<br>● Avaliar necessidade de notificação à ANPD e/ou aos titulares, registrando a avaliação, independentemente de positiva ou negativa;<br>● Em caso de notificação à ANPD, documentar todo o processo e acompanhar a evolução da notificação periodicamente;<br>● Após solução do Incidente, novo treinamento deve ser feito para colaboradores do PACTO, assim que possível.<br>● Tudo deve ser documentado e permanecer aos cuidados do Encarregado. | ● Estipular as medidas de correção imediatas para a área e colaboradores diretamente envolvidos no Incidente, registrando as recomendações e as execuções;<br>● Notificar imediatamente todos os colaboradores envolvidos no Incidente para adoção das medidas mitigadoras e preventivas definidas;<br>● Notificar à ANPD e os titulares de dados em até 48 horas da ciência do incidente.<br>● Após solução do incidente, novo treinamento deve ser feito, com absoluta prioridade, para colaboradores do PACTO.<br>● Tudo deve ser documentado e permanecer aos cuidados do Encarregado. |

Após a adoção das medidas sugeridas acima, o PACTO poderá estipular medidas complementares, de acordo com cada Incidente.

## 4 Registro e Notificação

Além dos procedimentos internos, poderá ser necessário comunicar a agentes externos, como Autoridades, titulares e/ou parceiros etc., sobre a ocorrência de um Incidente com Dados Pessoais. É **obrigação** do controlador comunicar à ANPD e ao titular em havendo risco ou dano relevante aos titulares. A seguir, as diretrizes para as situações em que a comunicação externa seja obrigatória ou avaliada pertinente pelo Comitê de Crise.

| Apenas se identificado risco para os titulares de dados pessoais | | |
|---|---|---|
| **Notificação** | **Prazo** | **Conteúdo obrigatório** |
| ANPD (Autoridade Nacional de Proteção de Dados Pessoais) | Imediatamente ou em até 2 dias úteis do ocorrido | • a descrição da natureza dos dados pessoais afetados;<br>• as informações sobre os titulares envolvidos; |

| | | |
|---|---|---|
| Titulares de dados eventualmente afetados | Após a resposta da Autoridade sobre o ocorrido | • a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;<br>• os riscos relacionados ao incidente;<br>• os motivos da demora, no caso de a comunicação não ter sido imediata; e<br>• as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. |
| Se o Pacto for OPERADOR | Sempre verificar o contrato para compreender o tempo combinado com o Controlador. | Comunicação necessária toda vez que for detectado que o Incidente (independentemente de risco) afeta dados controlados por empresas terceiras, sobre os quais o PACTO apenas exerce papel de Operador. |

A depender do incidente de segurança, como, por exemplo, na hipótese de ocorrência de um crime cibernético (aqueles que ocorrem por meio de sistemas de computação ou rede de computadores), será necessário acionar também autoridades policiais.

| | |
|---|---|
| Registro interno do ocorrido | • Descrição detalhada do Incidente de Segurança (o que ocorreu);<br>• Categoria de Dados Pessoais envolvidos;<br>• Categoria de Titulares Envolvidos;<br>• Possíveis riscos decorrentes do Incidente, especialmente em relação aos Titulares de Dados;<br>• Medidas adotadas com o objetivo de reverter as consequências do Incidente de Segurança;<br>• Motivos da demora, seja na identificação, apuração ou comunicação do incidente à ANPD e aos Titulares (se o caso);<br>• Fundamentos pelos quais o Pacto decidiu por não comunicar ANPD e Titulares de Dados (se o caso);<br>• Grau de esforço necessário para a recuperação do incidente;<br>• Impacto em serviços e produtos; e<br>• Tipologia do incidente (não observação à confidencialidade, integridade ou disponibilidade do dado). |

# Anexo I - Checklist de Fornecedores

| PACTO DE PROMOÇÃO DA EQUIDADE RACIAL | DADOS DO CONTRATADO: (nome da empresa, CNPJ...)<br>TIPO DE SERVIÇO CONTRATADO: (Ex. assessoria de comunicação para eventos) | | |
|---|---|---|---|
| | PERGUNTAS | RESPOSTAS | OBSERVAÇÕES |
| GOVERNANÇA | A empresa **já está adequada**, ou **já iniciou o processo de adequação à Lei Geral de Proteção de Dados Pessoais - LGPD** (Lei nº 13.709/2018)? | | |
| | A empresa registra as suas atividades de tratamento de dados, de acordo com as legislações relacionadas? (Ex: log de atividades dentro do sistema, usuários logados, relatórios de alterações, trilhas de auditoria, etc) | | |
| | A empresa já adequou os seus contratos com terceiros à LGPD? | | |
| | A empresa já adequou os seus contratos com funcionários à LGPD? Alternativamente, os funcionários do Contratado assinam acordos de confidencialidade para tratar os dados pessoais? | | |
| | A empresa possui **Encarregado de Dados** (DPO) designado? | | |
| | O contratado **possui uma estrutura de governança** de dados pessoais (Encarregado nomeado, treinamentos constantes, Políticas referentes aos tratamentos de dados pessoais dentro da empresa)? | | |
| | **Há algum procedimento** já estabelecido na empresa para efetivação dos **direitos dos titulares** dos dados pessoais? | | |
| | O Contratado já recebeu **requisições de titulares** de dados pessoais ou de autoridades a respeito dos tratamentos que realiza em suas atividades de prestação de serviço? | | |

| | | | |
|---|---|---|---|
| | A empresa **possui um plano de resposta a incidentes** de segurança? | | |
| | O contratado possui uma **Política de Privacidade** capaz de expor de forma ostensiva e clara que tipos e como são realizados os tratamentos de dados pessoais durante o seu serviço? | | |
| | A empresa possui **Política de Segurança da Informação** (PSI) devidamente documentada, atualizada, publicada e disponível para todos, nos termos da LGPD? | | |
| | | | |
| DADOS PESSOAIS TRATADOS PELO CONTRATADO | Descreva os **dados pessoais aos quais terá acesso durante a prestação do serviço.**<br><br>a) São **dados pessoais** (nome, ID, IP, geolocalização) ou **dados pessoais sensíveis** (Raça, etnia, orientação política ou religiosa...)<br>b) **A quem se referem os dados tratados** (ex: cidadãos de uma cidade, funcionários do Instituto, crianças, adolescentes, grupos em situação de vulnerabilidade) | | |
| | São utilizados **apenas dados necessários** para a prestação de serviços contratados? | | |
| | Depois da prestação dos serviços os dados acessados serão **deletados**? Se não o forem, serão **anonimizados**, **criptografados** e etc.? | | |
| | O Contratado utiliza **medidas técnicas** (segurança da informação), **administrativas e físicas** para proteger os dados pessoais que estão sendo tratados? Se sim, quais? | | |

| | | | |
|---|---|---|---|
| | **Onde** ocorrerá a prestação do serviço e o tratamento dos dados (no próprio país onde a unidade contratante está sediada ou no exterior)? | | |
| | Há **transferência internacional** de dados? Se sim, para qual **finalidade** (ex: armazenamento, prestação de contas, suporte técnico...) | | |
| | | | |
| SEGURANÇA | Existe algum **padrão de segurança da informação** implementado no contratado (IS0 27001, COBIT, NIST Cybersecurity framework...). | | |
| | A empresa possui **Política de Segurança da Informação** (PSI) devidamente documentada, atualizada, publicada e disponível para todos, nos termos da LGPD? | | |
| | A empresa **já sofreu incidente de segurança** (vazamento de dados pessoais, acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito), fiscalização por autoridades administrativas, ou é réu em processos referentes a LGPD, etc.? | | |
| | A empresa **já sofreu algum ataque de hackers**? Se sim, favor descrevê-lo(s). | | |
| | A empresa **possui vulnerabilidades identificadas em seus sistemas**? Se sim, favor descrevê-lo(s). | | |

# Anexo II – Prazos de retenção

**DOCUMENTOS OPERACIONAIS**

| Documento | Prazo de Retenção | Fundamento | Observações |
|---|---|---|---|
| Contratos comerciais (e que contenham dados pessoais e/ou cujas atividades prestadas envolvem o tratamento de Dados Pessoais) | 10 anos após o término de todas suas obrigações | Art. 205, CC | Prazo prescricional do CC. |
| Documentos cadastrais de clientes – pessoa física | 5 anos | Art. 27 e 43, § 1º, CDC | Com relação aos dados obtidos a partir de aplicações da internet, recomendamos que esse prazo seja contado a partir do último login/atividade do cliente na aplicação. |

**REGISTROS DE SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO**

| Documento | Prazo de Retenção | Fundamento | Observações |
|---|---|---|---|
| Logs de aplicações de internet | 6 meses | Art. 15, MCI | - |
| Registros de tecnologia e segurança da informação incluindo relatórios, de incidentes de segurança e documentos derivados, licenças de softwares, documentação relacionada ao desenvolvimento de sistemas, relatórios de continuidade do negócio e a recuperação de desastres, especificações de testes, logs de acesso a sistemas críticos, auditorias de segurança da informação, perfis de acesso. | 10 anos | Art. 205, CC | Na ausência de período de retenção específico definido por lei, o prazo de prescrição geral é de 10 anos (art. 205, CC). |

**DOCUMENTOS FISCAIS E TRIBUTÁRIOS**

| Documento | Prazo de Retenção | Fundamento | Observações |
|---|---|---|---|
| Contribuição sindical e patronal | 5 anos | Art. 173 c/c art. 195, CTN | - |
| Documentos fiscais/tributários da Receita Federal, Secretarias de fazenda Estaduais e Prefeituras Municipais | 5 anos | Art. 173 c/c art. 195, CTN | Incluem-se nesse item: obrigações acessórias, declarações, livros fiscais, notas fiscais, comprovantes de recolhimento dos tributos. Antes da destruição de qualquer documento fiscal após esse prazo, a Gerência Jurídica deve ser consultada para verificar a necessidade de manutenção dos mesmos por mais tempo. |

| | | | |
|---|---|---|---|
| Registros fiscais que envolvam pagamentos, contribuições e quaisquer outras obrigações tributárias vinculadas a pessoas físicas, incluindo Comprovante de Rendimentos Pagos ou Creditados e de Retenção na Fonte, Demonstrativo de Apuração de<br><br>Contribuições Sociais – DACON,<br><br>Demonstrativo de Notas Fiscais – DNF, documentos, papéis de trabalho, relatórios e pareceres relacionados aos serviços realizados pelo Auditor Independente.<br><br>Registros contábeis incluindo todos os documentos usados ou relevantes para a preparação das contas anuais da empresa, notas fiscais, recibos e declarações de fornecedores, orçamentos, registros de folha de pagamento e salário (incluindo detalhes sobre horas extras, bônus, despesas e benefícios em espécie), despesas de viagem e subsistência para funcionários. | 5 anos contados do primeiro dia do exercício seguinte àquele em que o lançamento poderia ter sido efetuado | Arts. 173 c/c,<br><br>174 c/c e<br><br>195, CTN | Antes da destruição de qualquer documento fiscal após esse prazo, a Gerência Jurídica deve ser consultada para verificar a necessidade de manutenção por mais tempo. |

**DOCUMENTOS SOCIETÁRIOS**

| Documento | Prazo de Retenção | Fundamento | Observações |
|---|---|---|---|
| Instrumentos de mandato | Determinado em cada caso, conforme observação | Art. 206, §3º, VII, item b do CC; e art. 287, II, b, 2. | O prazo de retenção de procurações dependerá do prazo de prescrição dos atos que forem praticados com base na procuração.<br><br>Além disso, a ação contra o administrador que houver outorgado a procuração em violação à lei ou estatuto prescreve em 3 (três) anos (contados da aprovação do balanço referente ao exercício em que a violação tenha sido praticada). |
| • Atas de reuniões do conselho e do comitê Livro de atas dos diretores corporativos e acionistas<br>• Avisos, arranjos e documentos da reunião anual<br>• Informações de membros do conselho | 10 anos | Art. 100, LSA c/c art. 205, CC. | Os documentos devem ser mantidos durante toda existência da sociedade e após seu término, durante o prazo geral de prescrição de 10 anos (art. 205, CC) |

| | | | |
|---|---|---|---|
| • Procurações<br>• Livros de atas subsidiários<br>• Livro de homenagem e memorial<br>• Comunicações dirigidas para ou do Conselho de Administração, acionistas, investidores e outras partes interessadas | | | |
| Atos societários (alterações de contrato social; atas de reunião de sócios; atas de reunião do conselho de administração; AGO; AGE etc.) | Determinado em cada caso, conforme observação. | - | A legislação societária não prevê prazo para guarda de Atos Societários. Contudo, para avaliar o período de guarda, é importante observar o prazo prescricional das ações judiciais que podem anular ou pedir reparação contra deliberações tomadas em cada Ato Societário. |

**DOCUMENTOS DE RECURSOS HUMANOS (TRABALHISTAS E PREVIDENCIÁRIOS**

*(Considerar para a guarda dos documentos comprobatórios de recolhimento de benefícios previdenciários o prazo de 5 anos, conforme o art. 225, §§5º e 22 e 348, Decreto nº 3048/99.)*

| Documento | Prazo de Retenção | Fundamento | Observações |
|---|---|---|---|
| Termo de Rescisão do Contrato de Trabalho | 5 anos | Art. 7º, XXIX, CF , art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Aviso Prévio | 5 anos | Art. 7º, XXIX, CF, art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Pedido de Demissão | 5 anos | Art. 7º, XXIX, CF , art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Cadastro Geral de Empregados e Desempregados (CAGED), a contar da data da postagem | 5 anos | Art. 2º, § 1º, Portaria MTE nº 1.129/14 | - |
| Cartões, fichas ou livros de ponto | 5 anos | Art. 7º, XXIX, CF, art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Recibos de pagamento | 5 anos | Art. 7º XXIX, art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Recibos de adiantamento salarial | 5 anos | Art. 7º, XXIX, CF, art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Acordos de compensação e/ou prorrogação de horas | 5 anos | Art. 7º, XXIX, CF, art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Solicitação de abono de férias | 5 anos | Art. 7º, XXIX, CF, art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Recibos de abono e gozo de férias | 5 anos | Art. 7º, XXIX, CF, art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Atestados médicos | 20 anos | Art. 104, Lei nº 8213/91 e NR7, item 7.4.5.1 | Deve-se acompanhar a discussão sobre a imprescritibilidade em relação a eventuais doenças de trabalho, para eventual alteração desse prazo |

| | | | |
|---|---|---|---|
| Autorização para descontos não previstos em lei | 5 anos | Art. 7º, XXIX, CF , art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Vale-transporte | 5 anos | Art. 7º, XXIX, CF , art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Guias de recolhimento de contribuição sindical e assistencial para contribuições descontadas e não recolhidas | 5 anos | Prazo tributário acima. | |
| Relação de contribuição sindical e assistencial | 5 anos | Prazo tributário acima. | |
| Comprovante de entrega da<br><br>Comunicação de Dispensa (CD) | 5 anos | Art. 7º, XXIX, CF , art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Recibo de entrega do requerimento Seguro-<br><br>Desemprego (SD) | 5 anos | Art. 7º, XXIX, CF , art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| CIPA, documentos relativos à eleição. | 5 anos | NR5, item 5.40 | |
| Folha de pagamento | 5 anos | Art. 7º, XXIX, CF , art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Recibo e ficha de salário-família | 10 anos | Art. 7º, XXIX, CF | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Atestados médicos relativos a afastamento por incapacidade ou salário-maternidade | 20 anos | NR7, item 7.4.5.1 | . Deve-se acompanhar a discussão sobre a imprescritibilidade em relação a eventuais doenças de trabalho. Pode-se adotar o prazo da NR7 (dados obtidos nos exames médicos, incluindo avaliação clínica e exames complementares, as conclusões e as medidas aplicadas). |
| Guias da previdência Social (GPS) | 5 anos | Art. 45, Lei 8.212/91 e Súmula Vinculante nº 8, STF | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Documentos relativos ao PIS/PASEP, a contar da data prevista para seu recolhimento | 5 anos | Art. 10,<br><br>Decreto-lei<br><br>2.052/83 | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Histórico Clínico do empregado (prontuário individual) | 20 anos | -NR7, item 7.4.5.1 | Deve-se acompanhar a discussão sobre a imprescritibilidade em relação a eventuais doenças de trabalho, para eventual alteração desse prazo |
| Documentos relativos ao FGTS | 5 anos, exceto se necessários para ações ajuizadas até 13/11/2019. | STF, RE 522897 | A prescrição pode ser de 30 anos para empregados na fase de transição - Súmula 362 do TST. O prazo de 30 anos é aplicável se a ação foi ajuizada até 13/11/2019. Posteriormente, o prazo é de 5 anos. |
| RAIS | 5 anos | Art. 8º Portaria MTE Nº 1.207/08 | |

| | | | |
|---|---|---|---|
| Contratos de trabalho | 5 anos | Art. 7º, XXIX, CF , art. 11, CLT | Prazo prescricional – contado a partir do término do contrato de trabalho. |
| Livros ou fichas de registro de empregados | 5 anos | - | Não há período legal determinado. Sugerimos o prazo de 5 anos |

**DOCUMENTOS JURÍDICOS**

| Documento | Prazo de Retenção | Fundamento | Observações |
|---|---|---|---|
| Inclui contratos, acordos, memorandos, pareceres, procurações. | 11 anos contados do término do contrato ou relação de negócios 5 anos contados do término da relação com o consumidor | Código Civil, Art. 205 Código de Defesa do Consumidor, Art. 27 | |
| Registros relacionados a Compliance, incluindo relatórios de exercícios de monitoramento e revisões de processos internos, auditorias por órgãos reguladores, registros de ações corretivas e preventivas decorrentes de auditorias internas ou externas etc. | - | - | Recomenda-se a análise caso a caso para determinação de prazos adequados às finalidades do PACTO. |
| Registros relacionados à prevenção à fraude, gerenciamento de fraude, detecção de fraude e investigação de fraudes. | 10 anos contados a partir da liquidação da empresa | Código Civil, Art. 205 | |

**DOCUMENTOS DE FACILITIES**

| Documento | Prazo de Retenção | Fundamento | Observações |
|---|---|---|---|
| Memorandos de revisão de aluguel e documentos de acompanhamento, documentos do projeto para novos edifícios e melhorias , contratos relacionados com construção, documentos relacionados à manutenção de edifícios, reparos, licenças, pesquisas e inspeções, relatórios arquitetônicos, documentos relacionados à engenharia de estruturas, engenharia mecânica e elétrica e relatórios de serviços de drenagem, contratos de manutenção e arquivos relacionados, programas e cronogramas de manutenção, registro de manutenção. | 10 anos contados a partir da liquidação da empresa | Código Civil, Art. 205 Lei 8.245/1991 (Lei de Locação) | |

| | | | |
|---|---|---|---|
| Gravações de câmeras de segurança, base de crachás, registros de acessos às dependências da empresa, fotografias, digitais. | 10 anos contados do término da relação com terceiro/prestador de serviço/visitante. | Código Civil, Art. 205 | |

# Anexo III – Técnicas de anonimização

Técnicas de anonimização, conforme referência, é considerada boa prática[2]. De acordo com o CEPI-FGV a anonimização é em si uma forma de proteção dos titulares de dados, cujas informações são utilizadas na pesquisa, uma vez que resguardam as pessoas de uma identificação pessoal.

Acontece que, nem sempre a anonimização será a melhor técnica para proteger os dados, uma vez que a reidentificação dos dados pessoais pode ser realizada facilmente, se os dados foram processados em conjunto com outras bases de dados. Assim, de acordo com a FGV, é importante prestar atenção aos seguintes pontos para avaliar a qualidade da anonimização como técnica de segurança:

a. Observe o nível do risco de reidentificação dos titulares de dados - a técnica de anonimização empregada demanda esforços significativos de tempo e custo para identificar os indivíduos a quem os dados se referem?
b. Observe as inferências possíveis a partir da base de dados - a técnica empregada impede a realização de inferências sobre os titulares de dados mesmo sem identificá-los pessoalmente?
c. Observe o risco de composição de atributos - os bancos de dados podem ser compostos com outros bancos de dados disponíveis publicamente ou em poder de quem acessa os dados, para facilitar a identificação dos titulares?
d.

Feito este raciocínio, abaixo apresentamos algumas técnicas para anonimizar os dados pessoais em poder do PACTO, evitando a identificação dos titulares de dados pessoais:

1. Mascarar os dados – determinadas partes de dados são substituídas por outros tipos de caracteres ou letras:

Exemplo:

Antes da anonimização:

| CEP | Nº de vezes que faz exercício | Idade |
|---|---|---|
| 0975236 | 5 | 23 |
| 0875214 | 3 | 16 |
| 0589974 | 6 | 45 |

Depois da anonimização:

| CEP | Nº de vezes que faz exercício | Idade |
|---|---|---|
| 0XXXX36 | 5 | 23 |
| 087XXX4 | 3 | 16 |
| 05XXXXX | 6 | 45 |

2. Pseudonimização – substituição pelos dados pessoais por números ou códigos, sendo que só a alta gestão do projeto consegue acessar os dados pessoais para identificar os usuários a partir dos números:

[2] COMISSÃO DE PROTEÇÃO DE DADOS PESSOAIS DE SINGAPURA. Guide to Basic Data Anonymization Techniques

Antes da anonimização:

| Nome | Nº de vezes que faz exercício | Idade |
|---|---|---|
| Mario Kart | 5 | 23 |
| Príncipe Encantado | 3 | 16 |
| Peixe Grande | 6 | 45 |

Depois da anonimização:

| Nome | Nº de vezes que faz exercício | Idade |
|---|---|---|
| 4112 | 5 | 23 |
| 6285 | 3 | 16 |
| 4257 | 6 | 45 |

3. Generalização – criar faixas para identificar o valor que se quer tornar anônimo:

Antes da anonimização:

| Nome | Nº de vezes que faz exercício | Idade |
|---|---|---|
| Mario Kart | 5 | 23 |
| Príncipe Encantado | 3 | 16 |
| Peixe Grande | 6 | 45 |

Depois da anonimização:

| Nome | Nº de vezes que faz exercício | Idade |
|---|---|---|
| 4112 | 5 | Entre 20 e 26 |
| 6285 | 3 | Entre 14 e 20 |
| 4257 | 6 | Entre 35 e 45 |

4. Agregar os dados – quando você não precisa de uma base de dados completa para atingir o seu objetivo, você pode resumir os dados em formato de indicadores:

Antes da anonimização:

| Nome | Valor doado mensalmente: | Valor doado anualmente: |
|---|---|---|
| Doador A | 40 | 480 |
| Doador B | 60 | 360 |
| Doador C | 50 | 600 |

Depois da anonimização:

| Valor das doações mensais: | Nº de doações recebidas: | Total doado no ano: |
|---|---|---|
| 30-40 | 8 | 1.000 |
| 41- 50 | 12 | 6.000 |
| 51-60 | 5 | 3.000 |