CAMILA CATANHO

CHECKLIST COMPLETO

# POLÍTICA DE PRIVACIDADE

## PASSO A PASSO PARA ELABORAR A SUA

## Sobre a autora

**Camila Catanho** é advogada, apaixonada por tecnologia, inovação e negócios. Têm mais de 13 anos de experiência e é especialista em direito digital . Atua na área societária, contratual e de proteção de dados, com o objetivo de auxiliar empresas a viabilizar novos negócios e diminuir os riscos.

camila_catanho

www.linkedin.com/in/camilacatanho

# CHECKLIST PARA ELABORAÇÃO DE POLÍTICA DE PRIVACIDADE

Esse ebook traz as seções que geralmente compõe uma política de privacidade e explica de maneira resumida quais informações incluir em cada uma, seu objetivo é meramente informativo e não substitui uma consultoria profissional.

**Atenção! NÃO EXISTE MODELO PADRÃO DE POLÍTICA DE PRIVACIDADE**, cada empresa deve ter a sua política baseada no seu mapeamento de dados, em seu negócio e segmento, nos procedimentos internos e na segurança da informação, sendo que dependendo da empresa as seções podem ser incluídas, expandidas ou excluídas.

Lembre-se, a política de privacidade serve para dar transparência ao titular dos dados e para cumprir o princípio da prestação de contas pela empresa, assim é importante que ela sempre reflita a realidade.

## APRESENTAÇÃO DA EMPRESA E DA POLÍTICA DE PRIVACIDADE

É uma introdução, que aborda um pouco da história da empresa, das áreas em que atua, sua missão e valores. Explica também, de forma geral e resumida a preocupação da organização com o tratamento de dados pessoais e com a privacidade de seus clientes e colaboradores.

Nessa seção também é mencionada o que á a política de privacidade, e o âmbito de aplicação desta (ex: site, aplicativo, etc ou a toda a organização).

Essa introdução não é obrigatória, mas é uma boa prática e situa o usuário.

## GLOSSÁRIO

Explica o significado dos termos técnicos mencionados na política de privacidade, como por exemplo: dados pessoais, dados sensíveis, controlador, operador, etc.

O art. 5º da LGPD (lei 73.709/2018) pode ser usado como inspiração para a elaboração do glossário.

Essa seção também não é obrigatória, mas é uma boa prática e ajuda o usuário a entender melhor a política, dando aplicação ao princípio da transparência.

## DADOS OFICIAIS DA EMPRESA

Mesmo com a introdução, é importante ter uma seção facilmente localizável dentro da política que identifique a empresa como responsável pelo tratamento dos dados pessoais, ou seja, como controladora dos dados pessoais, e informe sua razão social, número de CNPJ e o endereço da sede.

## DADOS TRATADOS E FINALIDADE DO TRATAMENTO

Essa é a **seção mais importante da política** de privacidade. Os titulares de dados devem ser informados sobre quais de seus dados estão sendo tratados pela empresa e qual a finalidade do tratamento.

Lembrando que tratamento de dados é qualquer operação realizada com os dados pessoais, como coleta, armazenamento, classificação, transmissão, eliminação, etc.

Geralmente, para facilitar a elaboração e as futuras atualizações da política geralmente dividimos os dados tratados em grupos. Esses grupos podem ser separados em:

- tipos de dados = dados de cadastro, dados de pagamento, dados de saúde, etc;
- tipos de departamentos que tratam dados = dados do marketing, dados do RH, dados de compra, etc;
- tipos de titulares de dados = dados de clientes, dados de funcionários, dados de leads, etc.

Em se tratando de empresas que atuam em mercados mais regulados ou tem um público mais consciente recomenda-se também incluir a base legal para o tratamento dos dados pessoais, conforme estabelecido nos arts. 7º e 9º da LGPD (ex: consentimento, legítimo interesse, cumprimento de obrigação legal, etc).

**Atenção!** Para a elaboração desta parte da política antes é necessário ter realizado o **MAPEAMENTO DE DADOS PESSOAIS**, no qual são identificados todos os dados pessoais tratados pela empresa, qual a finalidade do tratamento, com quem esses dados são compartilhados e, caso feito por consultoria especializada neste momento também é identificada qual é a base legal que autoriza o tratamento dos dados.

## DIREITOS DOS TITULARES

A lei geral de proteção de dados estabelece vários direitos aos titulares de dados, sendo que como boa prática é recomendável informá-los ao titular. Os principais direitos do titular estão expostos no art. 18 da LGPD (lei 13.709/2018), que recomendamos como ponto de partida para a elaboração desta seção.

## FORMA DE CONTATO OU INDICAÇÃO DO DPO

É necessário informar um canal de contato para que o titular de dados possa se comunicar com a empresa e exercer seus direitos, esse canal também pode ser usado pela ANPD.

Todas as empresas não enquadradas como agentes de tratamento de pequeno porte, nos termos da resolução n. 2 da ANPD devem indicar um DPO – data protection officer, ou encarregado de proteção de dados, nos termos do art. 41 da LGPD. Uma das funções do encarregado é comunicar-se com os titulares de dados e com a ANPD, assim suas informações de contato devem estar disponíveis ao público, sendo necessário indicá-las na política de privacidade, nesse caso pode-se indicar somente as informações do DPO.

**Atenção!** Nem todas as microempresas ou empresas de pequeno porte são classificadas como agentes de pequeno porte, pois a resolução n.2 trás exceções, a depender das características do tratamento de dados realizado pela empresa, assim antes de decidir não nomear um DPO deve-se verificar se não existe hipótese de exceção.

## COMPARTILHAMENTO DE DADOS PESSOAIS

Deve-se informar ao titular com quem são compartilhados seus dados pessoais, é muito comum compartilhar dados com fornecedores, prestadores de serviço, parceiros comerciais ou empresas do mesmo grupo. Ex: escritório de contabilidade, empresa de transporte, empresas de tecnologia (Google, Microsoft, Zoom), etc. Essa seção também é feita com base no mapeamento de dados.

Cada empresa deve avaliar o nível de detalhe exposto na política de privacidade, se será ou não indicadas o nome de todas as empresas e todos os dados. Essa avaliação depende do tipo de dado compartilhado, de quem

é o público e do negócio. No mínimo deve ser informado em linhas gerais os tipos de dados compartilhados e os tipos de empresa com quem os dados são divididos.

## TRANSFERÊNCIA INTERNACIONAL DE DADOS

O titular de dados deve ser informado sobre a existência de transferência internacional de dados pessoais, especificando para quais países os dados são transferidos e, conforme o caso, especificando também os tipos de dados transferidos.

**Atenção!** Muitas vezes há na empresa transferência internacional sem que o empresário tenha consciência disso, isso porque atualmente usamos muitos recursos tecnológicos de big techs como google, grupo meta, zoom, telegrama, etc, essas empresas geralmente têm servidores, que armazenam os dados utilizados em seus softwares, em outros países, assim a maioria das empresas realiza transferências internacionais de dados.

## TEMPO DE ARMAZENAMENTO DOS DADOS

Os dados pessoais podem ser armazenados somente pelo tempo suficiente para cumprirem a finalidade do tratamento realizado, sendo que o titular deve ser informado sobre o tempo de armazenamento.

Em regra, não é preciso detalhar de forma pormenorizada o tempo de armazenamento de todos os dados pessoais na política de privacidade, porém deve-se mencionar em linhas gerais o tempo de armazenamento dos principais dados coletados ou ao menos o critério para definir este tempo (por exemplo: tempo de prescrição).

**Atenção!** Apesar de não ser necessário fazer a descrição de tempo de armazenamento de cada dado na política de privacidade divulgada aos titulares de dados a empresa deve internamente ter um documento

chamado tabela de temporalidade, no qual constam o tempo de retenção de todos os dados, essa tabela é necessária para fazer a gestão da eliminação dos dados após o período determinado, o que é obrigatório conforme a LGPD

## SEGURANÇA DA INFORMAÇÃO

A política de privacidade deve conter as principais medidas de segurança da informação adotadas pela empresa. Não é preciso, nem recomendado, descrever todas as medidas adotadas, mesmo porque tal descrição pode facilitar um ataque ou a identificação de uma vulnerabilidade por pessoa mal intencionada.

**Atenção!** Assim como para o tempo de retenção dos dados, a empresa deve ter um documente interno, chamado política de segurança da informação, em que são descritas as salvaguardas de segurança, as medidas de gestão, os planos de backups de dados e atualizações, e o plano de resposta a incidentes e restauração do sistema.

Ter e aplicar uma política de segurança da informação é de extrema importância para as empresas, independentemente da LGPD, pois ela irá dificultar a ocorrência de um incidente de segurança da informação, como um ataque hacker, e garantir que o sistema poderá ser restaurado caso mesmo assim um incidente ocorra, o que é essencial principalmente em negócios que usam muita tecnologia e dados como por exemplo e-commerces, startups, seguros, etc.

## COOKIES

É preciso informar ao titular de dados se seu site usa cookies, quais são esses cookies e quais os dados coletados através deles, é uma boa prática também

informar ou compartilhar link explicando como desabilitar os cookies diretamente no navegador.

Atenção! Seu site deve ter também um banner de cookies informando o titular de dados sobre os cookies existentes e permitindo que ele escolha quais os cookies quer deixar ativos, com exceção dos cookies funcionais que, como relacionados ao funcionamento do site podem ser obrigatórios. Cookies que não coletam dados pessoais também podem ser obrigatórios.

## ALTERAÇÕES NA POLÍTICA DE PRIVACIDADE

É uma boa prática alertar o titular de dados que a política de privacidade pode ser alterada e que o mesmo deve checar regularmente a página referente a política de privacidade. Para usuários cadastrados também é uma boa prática enviar e-mail informando sobre mudanças da política de privacidade quando estas ocorrerem.

## DATA DE ELABORAÇÃO DA POLÍTICA

Deve ser informada a data de elaboração da política de privacidade vigente, sendo que internamente a empresa deve arquivar o histórico de versões da política de privacidade.