PRINCIPAIS PONTOS PARA A ADEQUAÇÃO DE DISTRIBUIDORAS À LGPD

target
SISTEMAS

INTRODUÇÃO

A **Lei Geral de Proteção de Dados** (Lei nº 13.709/2018) regulamenta e institui uma série de **deveres** e **obrigações** envolvendo as operações que realizam tratamento de dados pessoais. Agora, o Brasil passa a contar com a proteção de dados com mais força e disciplina, a partir da vigência da Lei e da criação da **Autoridade Nacional de Proteção de Dados (ANPD)**. Na prática, as empresas terão que rever muitas de suas práticas para garantir um tratamento adequado a estes dados. A LGPD, sem dúvidas, é a grande inovação no cenário da proteção de dados brasileira e, por isso, ao mesmo tempo que representa grande avanço, também desperta **muitas dúvidas**.

Embora a proteção de dados seja de significativa importância, já que estes, em alguma medida, se fazem presentes em praticamente qualquer atividade, ela ainda é **recente na cultura brasileira**. Pela falta de costume, é natural que muitas empresas estejam sem saber o que precisam fazer para estarem de acordo com a LGPD. Por isso, a Target, atenta às necessidades de seus parceiros distribuidores e comprometida com a privacidade, dando seguimento ao conteúdo publicado anteriormente no artigo **"A LGPD na distribuição"** disponível neste link, preparou este ebook para que o distribuidor saiba mais **concretamente** o que ele precisa fazer para que sua atividade esteja em conformidade com a lei.

Este ebook é direcionado às distribuidoras e elaborado com base no próprio projeto de adequação da Target, bem como na experiência pautada nas relações entre a Target e seus clientes distribuidores. Lembramos que o roteiro sugerido a seguir **não tem por objetivo esgotar** as questões que cada empresa deve se atentar, mas sim oferecer meios para que cada distribuidora possa **iniciar seu processo** de adequação já tendo, de **forma clara** e **concreta**, os pontos básicos em mente.

VOCÊ IRÁ ENCONTRAR DETALHES SOBRE ESSAS ETAPAS NESTE EBOOK

1

CONSTITUIR UM COMITÊ PARA TRATAR OS ASSUNTOS RELACIONADOS À LGPD

2

NOMEAR UM DPO OU ENCARREGADO DE DADOS

3

RELAÇÃO COM FORNECEDORES: OS DADOS QUE COMPARTILHO COM OUTRAS EMPRESAS

4

RELAÇÃO DE TRABALHO COM FUNCIONÁRIOS

5

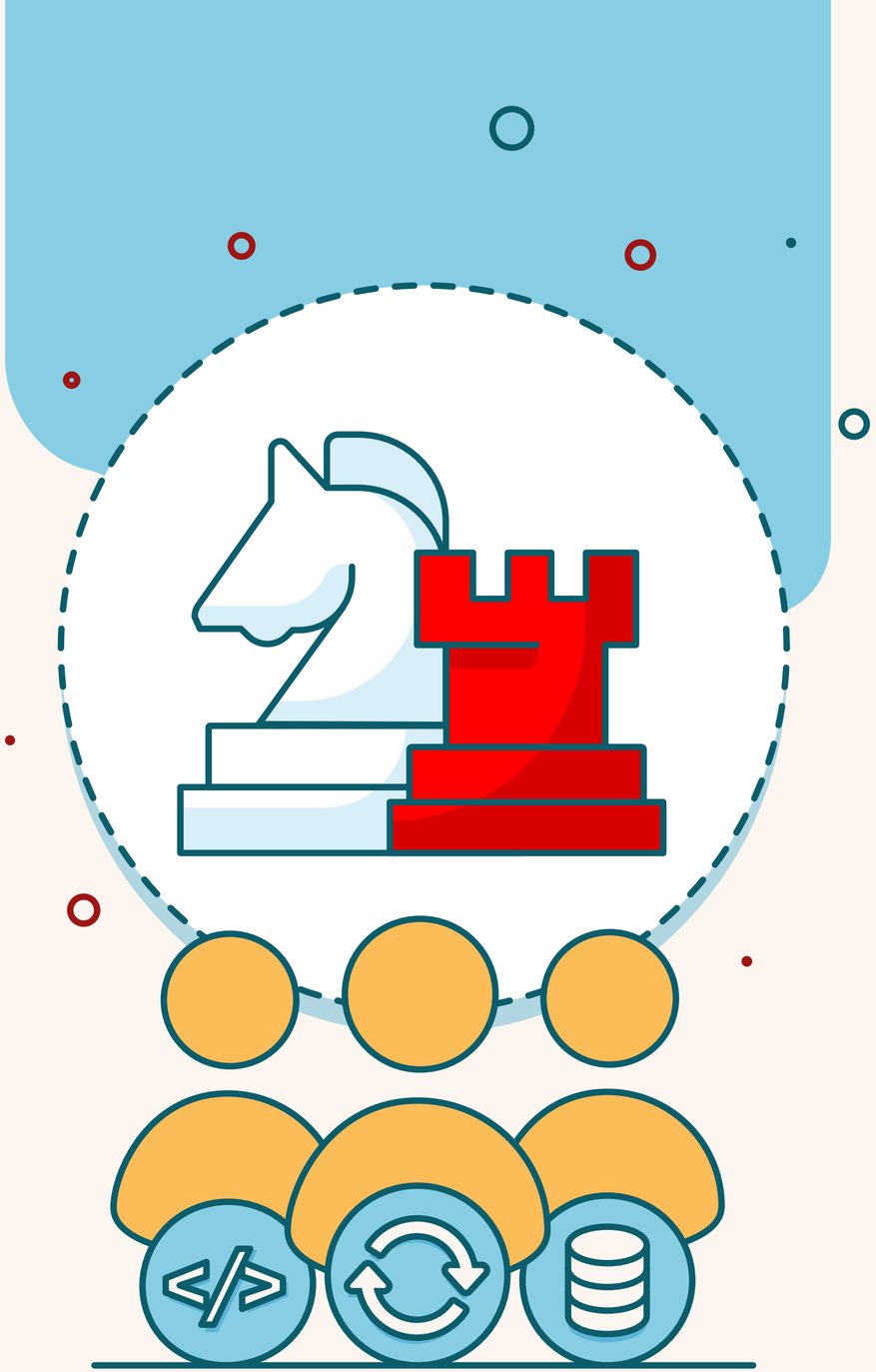
GARANTIR MEIOS DE ATENDER AOS DIREITOS DO TITULAR DOS DADOS

6

ELABORAR UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7

ELABORAR UMA POLÍTICA DE PRIVACIDADE



1. CONSTITUIR UM COMITÊ PARA TRATAR OS ASSUNTOS RELACIONADOS À LGPD

O QUE É E PARA QUE SERVE O COMITÊ?

Para começar, é necessário criar um comitê de privacidade e proteção de dados pessoais para **gerenciar a execução** do plano de ação de adequação à lei. O **plano de ação** é aquele que, considerando a situação da empresa, estabelecerá quais as medidas a serem implementadas para se **adequar à legislação**.

QUEM DEVE FAZER PARTE DO COMITÊ?

O comitê **tomará decisões** e **aprovará documentos** relacionados a adequação à LGPD. Por isso, deverá reunir pessoas que tenham amplo conhecimento do funcionamento da empresa e dos processos de tratamento de dados pessoais, além de terem capacidade para **estabelecer caminhos estratégicos** de atuação. Nesse sentido, a **alta administração** da empresa, **necessariamente** deverá compô-lo, podendo, ainda, haver inclusão de outros setores importantes, como o RH, a Administração, o Jurídico, o Marketing, o Compliance etc.

COMO FORMAR O COMITÊ?

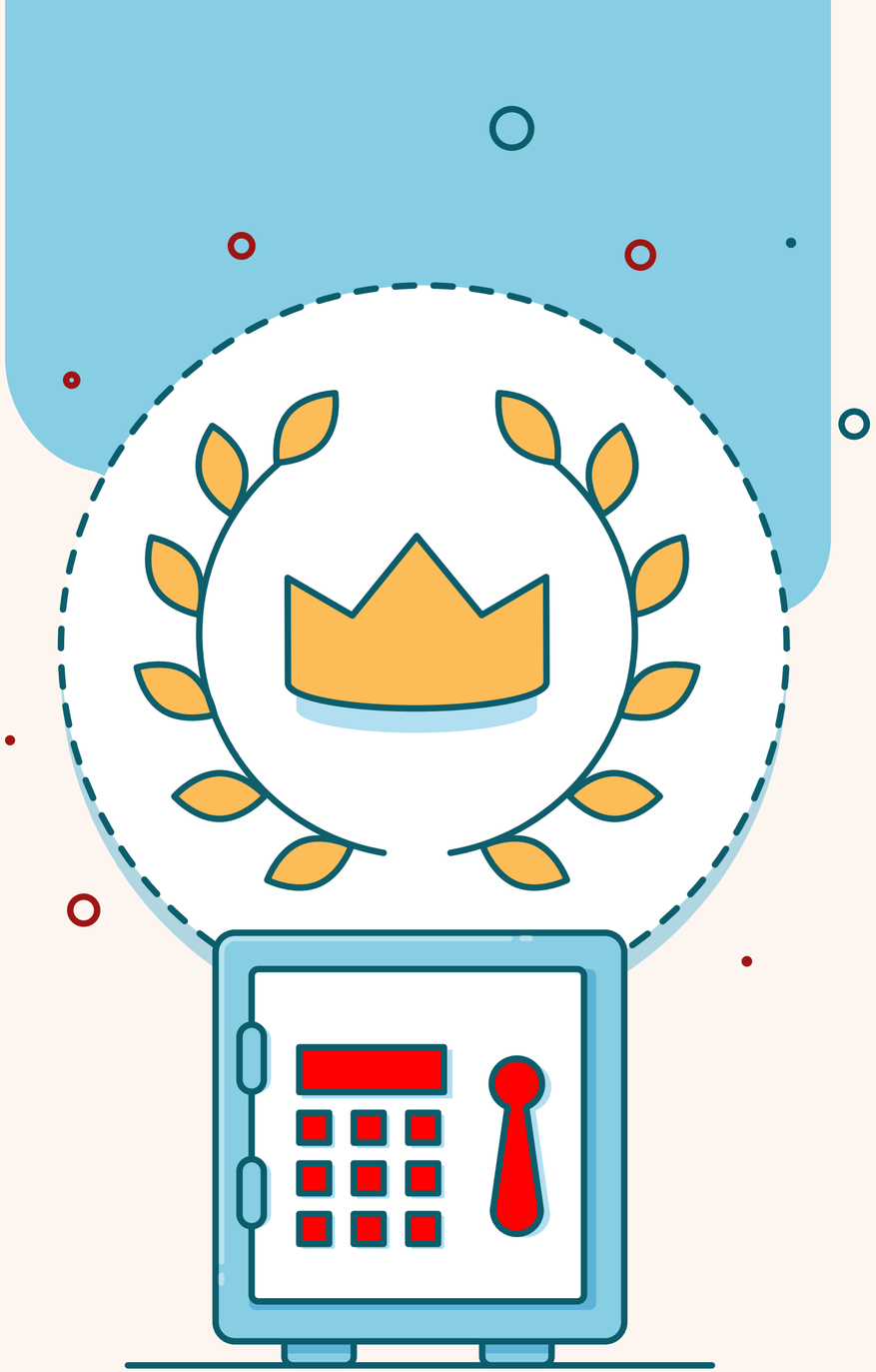
O tamanho do comitê poderá variar a depender do **volume de dados** em tratamento e do tamanho da companhia, podendo ser algo em torno de três ou quatro pessoas. Aqui, **menos é mais**. Por ser um grupo que lidará com questões estratégicas e sensíveis sobre a atividade da empresa, precisa ter **autonomia** e **agilidade** para tomar decisões e, por isso, o ideal é que seja formado por uma **quantidade limitada** de pessoas

ENVOLVIMENTO COM O DPO

Além disso, por ser formado por pessoas de diferentes áreas da empresa, poderá **apoiar** o encarregado de dados nas implementações de melhorias nos **processos de negócios**.

RESUMO:

- **Convoque** o time decisor da empresa para uma reunião
- **Exponha** o conteúdo enviado pela Target
- Provoque uma eleição e registre em ata para ser **assinado por todos**
- Arquive esse documento, pois é **um marco** para a sua empresa
- **Comunique sua equipe** sobre a constituição do Comitê



2. NOMEAR UM DPO OU ENCARREGADO DE DADOS

O QUE FAZ O DPO?

De acordo com a lei, o Comitê deverá nomear um **encarregado de proteção de dados**, (também conhecido como data protection officer (DPO)) e que será o responsável da empresa por:

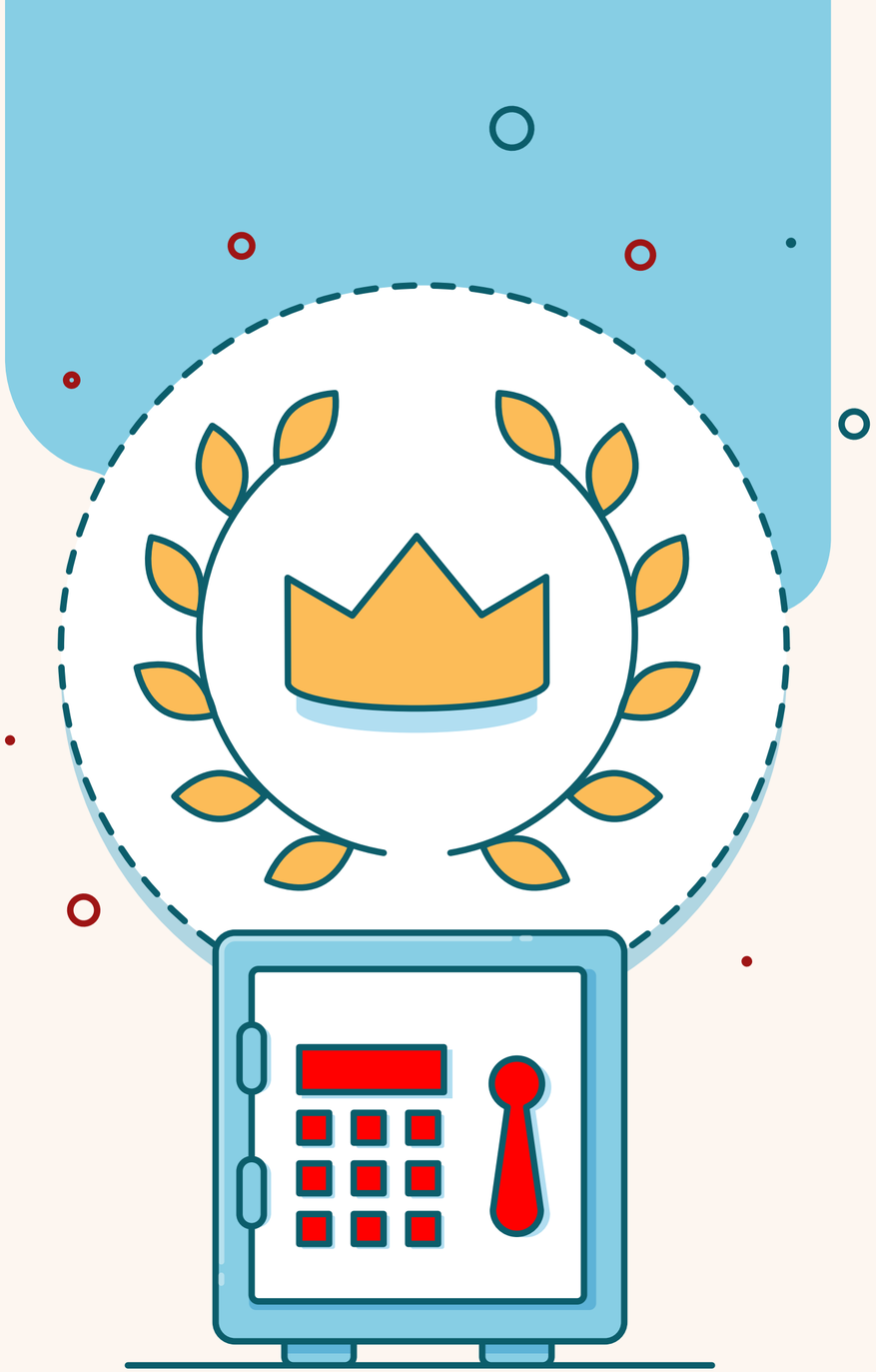
- Aceitar reclamações e comunicações dos titulares, **prestar esclarecimentos** e **adotar providências**;
- Receber comunicações da autoridade nacional e adotar providências;
- **Orientar** os funcionários e os contratados sobre as normas de proteção de dados pessoais;
- **Executar** as demais atribuições determinadas pela empresa ou normas complementares.

Na prática, caberá a este profissional acompanhar **todo o ciclo de vida dos dados** que trafegam na empresa – ele terá que saber como são coletados, por quais meios, como são usados, com quem são compartilhados e como são descartados – para poder responder adequadamente às solicitações dos titulares de dados e às comunicações da ANPD, bem como para poder prestar as devidas **orientações** sobre a atividade de tratamento de dados da empresa. Isso significa que o DPO deverá estar envolvido em **todos os projetos** da organização que envolvam **dados pessoais**, bem como deverá ser a última instância na decisão de manipulação de dados.

QUEM PODE SER DPO?

Para a nomeação do DPO, o comitê poderá optar por uma pessoa física, podendo esta ser um terceiro ou um funcionário da organização, ou jurídica (DPO as a service), como consultorias, escritórios de advocacia, dentre outras empresas.

Ainda que seja um funcionário da empresa, o encarregado deverá ter **plena independência** para priorizar as questões relativas à privacidade, sem gerar um choque com suas outras funções ou tarefas. Isso, porque o DPO precisa ter **autonomia** e **poder** para, inclusive, refutar os interesses da empresa quando as movimentações envolverem práticas ilegais de tratamento de dados, para que a direção da companhia tome as decisões sobre sua atividade da forma mais consciente possível



2. NOMEAR UM DPO OU ENCARREGADO DE DADOS

quanto às suas consequências em termos de **responsabilização** em razão do tratamento de dados.

A lei não traz exigências quanto aos requisitos de formação deste profissional ou necessidade de alguma certificação. Porém, pelas atribuições impostas na LGPD, recomenda-se que o ocupante da função tenha **conhecimentos multidisciplinares**, de modo que seja capaz de conhecer e interpretar a legislação a respeito de proteção de dados, lidar com órgãos governamentais, entender aspectos de tecnologia e segurança da informação, transitar em assuntos de compliance, governança e normas coorporativas e ainda conhecer a operação da empresa. Deverá somar a sua isenção e capacidade operacional em **direcionar** todos esses conhecimentos para penetrar na empresa a cultura na qual a privacidade tem status de valor social a ser efetivamente protegido pelas organizações.

Por fim, vale lembrar que a questão do perfil do profissional, embora importante, não extingue a necessidade da formação de um **comitê de privacidade e proteção de dados**, o qual dará suporte ao encarregado e ajudará na operação de compliance em proteção de dados pessoais, em **especial nas questões de segurança da informação**.

CANAL DE COMUNICAÇÃO

Após o encarregado ser nomeado, é necessário criar um **canal de comunicação** para que os titulares de dados pessoais, a ANPD e demais interessados possam entrar em contato com ele. Além disso, a empresa deve **divulgar as informações** de contato do encarregado publicamente, preferencialmente no seu website.

RESUMO:

- Avalie sua equipe e se **houver alguém com o perfil**, faça a nomeação
- Não havendo, fale com o seu jurídico ou busque indicações com parceiros para ter essa responsabilidade terceirizada
- Uma vez definido o DPO, crie um e-mail DPO@distribuidora.com.br
- Se tiver um site institucional, inclua esse contato para o **canal ficar aberto** ao público em geral

3. RELAÇÃO COM FORNECEDORES: OS DADOS QUE COMPARTILHO COM OUTRAS EMPRESAS

REQUISITO PARA NEGOCIAR COM FORNECEDORES

É preciso **garantir** que os fornecedores com quem **você compartilha dados pessoais**, sejam eles indústrias ou prestadores de serviço (como fornecedores de gestão de recursos humanos, de folha de pagamento, de plano de saúde, de recrutamento, de contabilidade, de compra e venda, de emissão e controle de notas fiscais, de prestação de serviços jurídicos, de sistemas, entre outros) estejam em **conformidade com a LGPD**.

COMO GARANTIR QUE MEUS FORNECEDORES ESTÃO ADEQUADOS A LGPD?

1. Termo de conformidade

Uma forma simples de certificar a conformidade de seus fornecedores é por meio de um **termo de conformidade**, pelo qual eles irão assumir que realizam adequadamente o tratamento de dados pessoais nos termos do que a LGPD estabelece.

Clique aqui para baixar um modelo de termo de conformidade.

2. Revisão contratual

Também será necessário procurar seu **departamento jurídico** para **revisar ou adicionar** cláusulas que digam respeito aos dados tratados pela empresa no meio físico ou digital.

O contrato deve conter as obrigações desse fornecedor ou parceiro segundo os princípios da LGPD. É preciso destacar, por exemplo, a obrigação de **não desviar a finalidade do tratamento dos dados**, tendo em vista que o operador (fornecedor) deve tratar os dados pessoais de acordo com as instruções determinadas pelo controlador (distribuidora), a não ser que seja exigido de outra forma pela legislação nacional ou por norma regulatória da ANPD.

O contrato também deve prever a **confidencialidade** e **sigilo** dos dados pessoais, mesmo após o término da relação estabelecida. E mais, o dever de confidencialidade deve abranger os colaboradores dos agentes de tratamento, incluindo quaisquer trabalhadores temporários que tenham acesso aos dados pessoais.

3. RELAÇÃO COM FORNECEDORES: OS DADOS QUE COMPARTILHO COM OUTRAS EMPRESAS

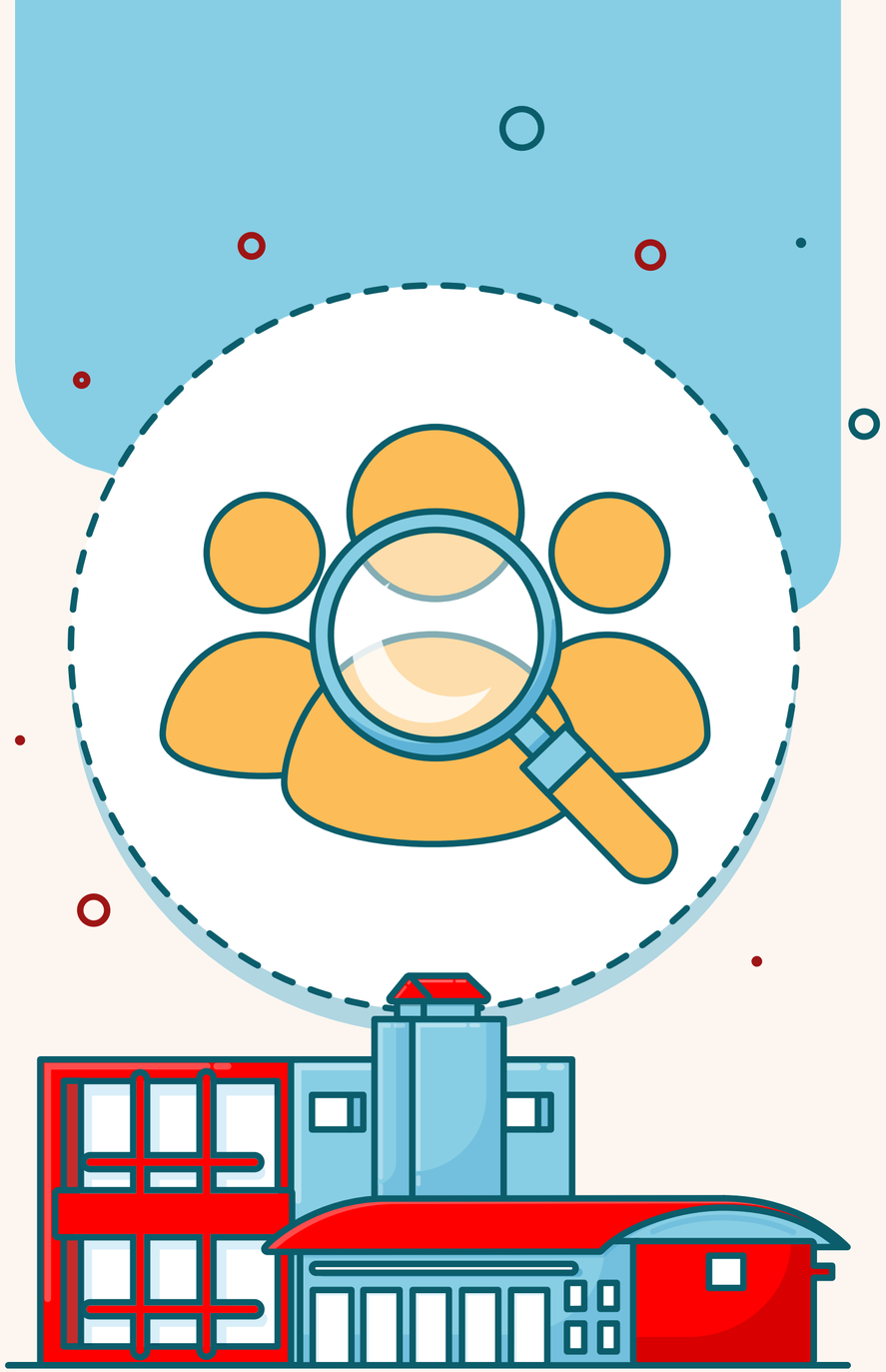
É importante também **estabelecer regras** sobre a responsabilidade por danos. No caso de um incidente de segurança, por exemplo, é interessante estabelecer o dever de assistência entre os agentes, (fornecedores e distribuidora), contendo a forma e o prazo em que serão feitas as notificações ou comunicações internas sobre eventuais comprometimentos à base de dados, podendo, ainda, prever as **medidas técnicas** e **organizacionais adequadas para garantir a segurança** de quaisquer dados pessoais que estejam tratando.

E OS DADOS QUE EU RECEBO DE OUTRAS EMPRESAS?

Vale lembrar que quando a empresa colher, receber ou acessar dados de outras empresas prestadoras de serviços terceirizados, como, por exemplo, empresas que disponibilizam mão de obra para serviços de limpeza, manutenção, segurança, dentre outros, também será **necessário adaptar** os contratos a fim de se discriminar, minunciosamente, as questões que permeiam o tratamento dos dados pessoais dos empregados.

RESUMO:

- Garanta que os fornecedores com quem você compartilha dados pessoais estão em **conformidade** com a LGPD através de um **Termo de Conformidade**;
- **Revise os contratos** com empresas das quais você recebe ou para as quais você envia dados pessoais, incluindo ou ajustando cláusulas que digam respeito ao tratamento de dados pessoais de acordo com as disposições da LGPD.



4. RELAÇÃO DE TRABALHO COM FUNCIONÁRIOS

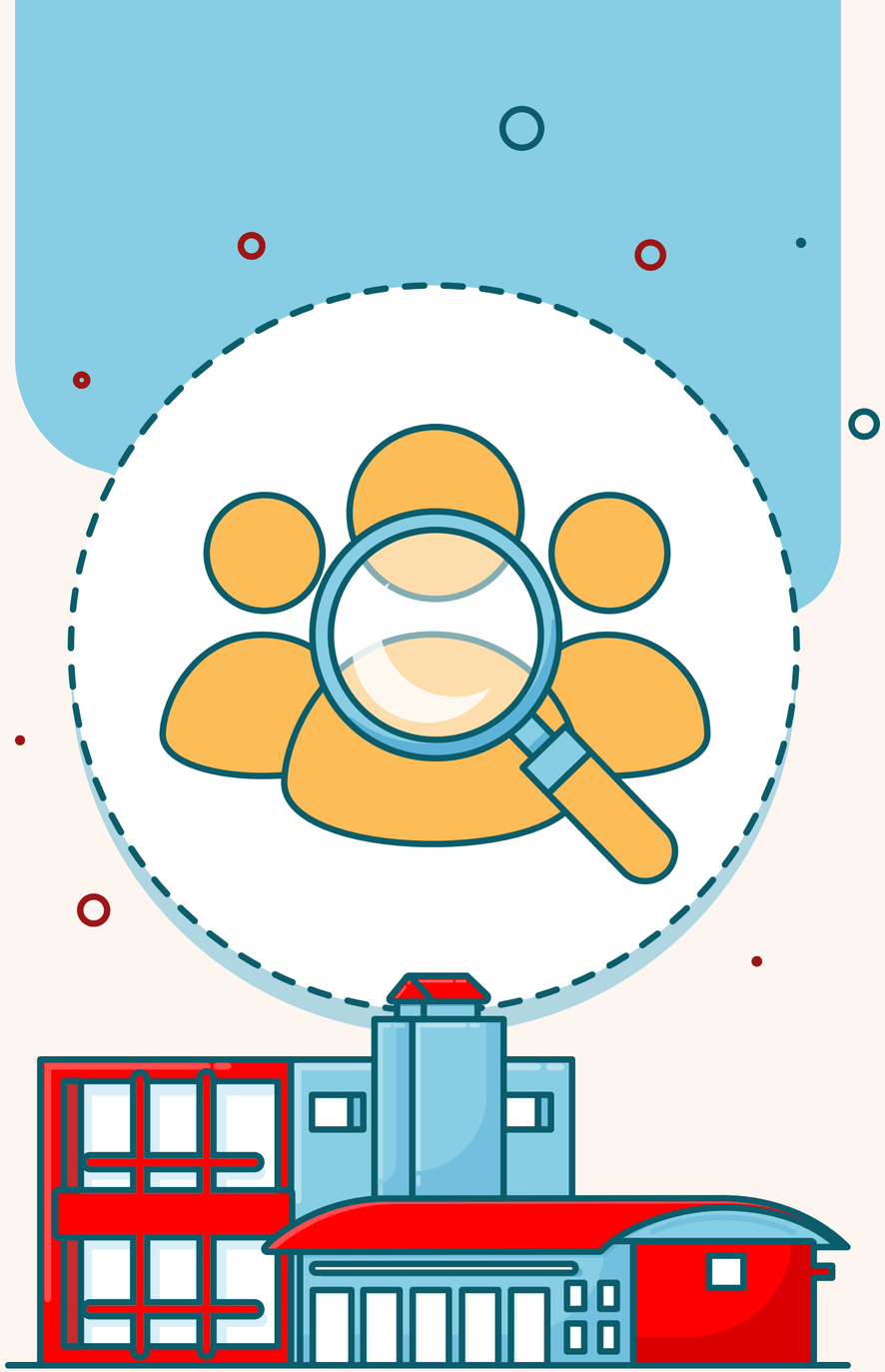
O departamento de Recursos Humanos é uma área que merece **muita atenção**, isso porque nele estão concentrados os dados de todos os funcionários da empresa, inclusive **dados sensíveis**, aqueles que dizem respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, e dados que sejam referentes à saúde ou à vida sexual e e informações genéticas ou biométricas.

Neste sentido, é de extrema importância documentar todo os processos relacionados ao RH, descrevendo como os dados pessoais são armazenados, qual a finalidade da coleta, quanto tempo esses dados ficam armazenados na empresa, quem tem acesso a eles, se são compartilhados com algum terceiro, etc. A recomendação é sempre **coletar o mínimo de dados possível, e não coletar dados sensíveis, quando estes não forem necessários** para alguma finalidade específica. Nos casos, porém, em que for necessário o tratamento de dados sensíveis, será preciso obter o consentimento do funcionário para o tratamento deles, além de garantir que acesso a eles será extremamente limitado.

SITUAÇÕES DE TRATAMENTO DE DADOS PESSOAIS ENVOLVENDO O RH:

Para facilitar a visualização, listamos a seguir algumas **situações comuns** envolvendo o tratamento de dados pessoais pelo RH para se atentar, lembrando, porém, que podem existir outras hipóteses dependendo do contexto de cada empresa.

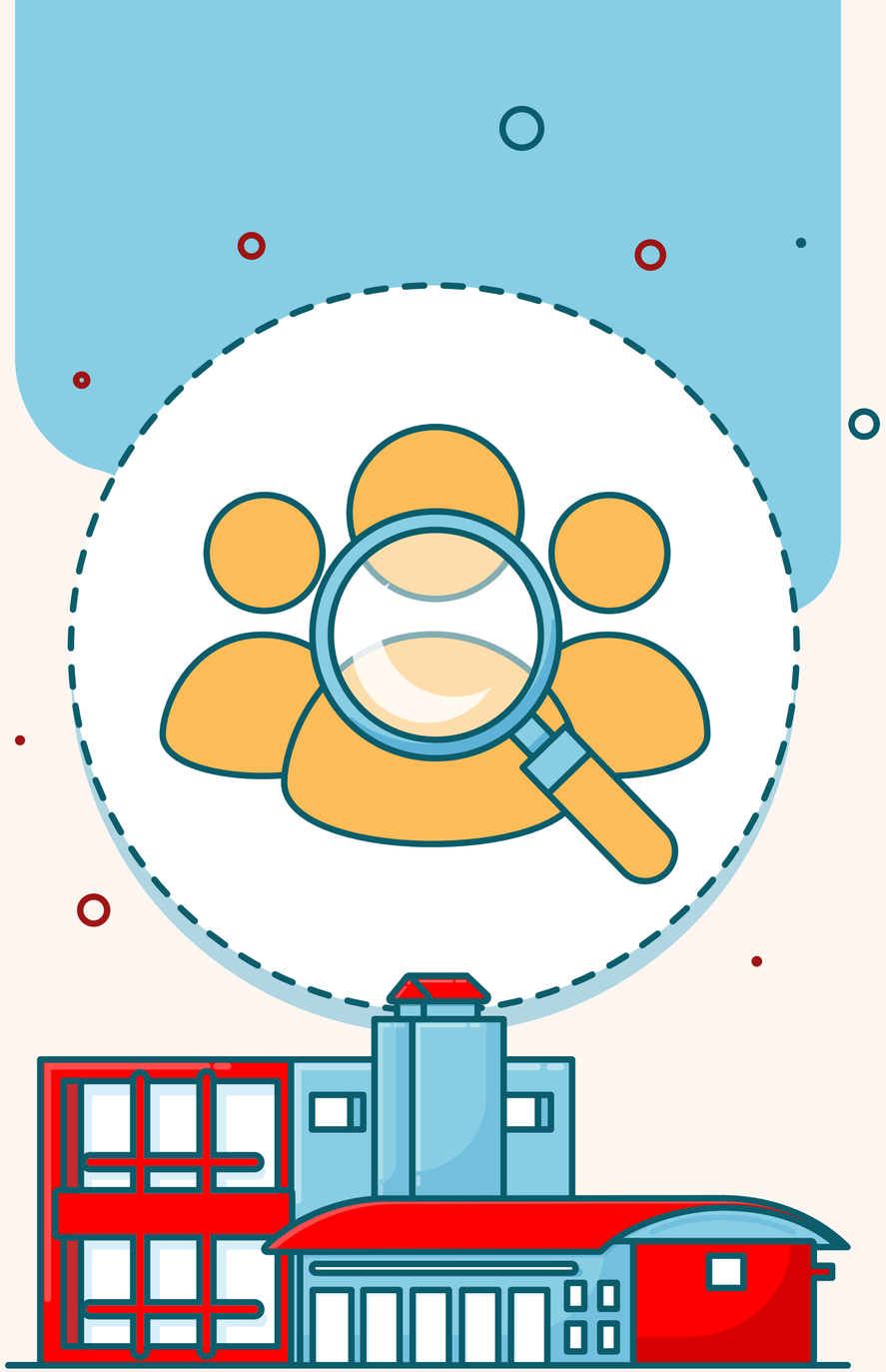
- ***Processo de seleção de novos funcionários:*** há coleta de dados pessoais a partir do momento que a empresa recebe o currículo do candidato. Tendo isso em vista, é preciso fornecer ao candidato a política de tratamento desses dados desde o primeiro momento em que ele fornece seus dados. Ainda, aqui, é indiferente ao empregador saber dados sensíveis como etnia, orientação sexual, dentre outros, razão pela qual tais dados não devem ser coletados.
- ***Ficha de registro:*** na ficha de registro é comum que contenha dados pessoais e dados sensíveis, a exemplo da filiação sindical. Portanto, é necessária a limitação de acesso à ficha de registro do funcionário.
- ***Realização de exames:*** pela lei, todos os funcionários celetistas são obrigados a rea-



4. RELAÇÃO DE TRABALHO COM FUNCIONÁRIOS

lizar o exames médicos periódicos, os quais abrangem a avaliação clínica, anamnese ocupacional e exames físico e mental, sendo possível haver exames complementares em alguns casos. Contudo, não podem ser solicitados exames que possam expor a saúde do trabalhador a fim de causar-lhe discriminação, a exemplo dos exames de HIV, gravidez, câncer etc.

- ***Recebimento de atestados:*** embora não seja obrigatório o preenchimento da CID (Classificação Internacional de Doenças e Problemas Relacionados à Saúde) no atestado médico, caso haja identificação da doença e/ou o motivo do afastamento, pela LGPD, tais dados passam a ser dados sensíveis e, portanto, precisarão de política específica de guarda e acesso.
- ***Compartilhamento de dados com seguradoras, planos de saúde, entidades sindicais:*** pela LGPD o compartilhamento desses dados precisará de autorização expressa do titular, principalmente quando se tratar de dados de familiares e de terceiros. A exceção virá quando essas informações decorrerem de pedido judicial, de obrigação legal ou para fins de dados de estatística do governo.
- ***Menor aprendiz:*** antes a autorização dos representantes legais era necessária apenas na rescisão do contrato, agora o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico, em que destaque, dado por pelo menos um dos pais ou pelo responsável legal.
- ***Monitoramento interno e externo do ambiente da empresa (e-mails, redes sociais, dispositivos funcionais, dispositivos pessoais, geolocalização):*** a LGPD não proíbe o monitoramento interno e externo do funcionário, mas tal monitoramento deverá ser justificado e com o consentimento do funcionário, zelando pela transparência, finalidade e necessidade.
- ***Teletrabalho e proteção de dados:*** quando o funcionário faz uso de computador ou e-mail institucional, é permitido o acesso pelo empregador com o conhecimento do funcionário. Já em caso de uso de equipamentos pessoais, tal acesso não atende à finalidade da LGDP.



4. RELAÇÃO DE TRABALHO COM FUNCIONÁRIOS

REVISÃO DOS CONTRATOS DE TRABALHO:

Ainda, é necessário proceder à revisão dos contratos de trabalho, incluindo nele cláusulas a respeito do **tratamento de dados de forma destacada** ou **elaborar aditivos a ele com tais disposições**, inclusive no que se refere ao consentimento nos casos em que este é exigido para o tratamento de dados pessoais (dados sensíveis e dados pessoais cujo tratamento não se justifique simplesmente em razão de obrigação legal ou execução do contrato de trabalho).

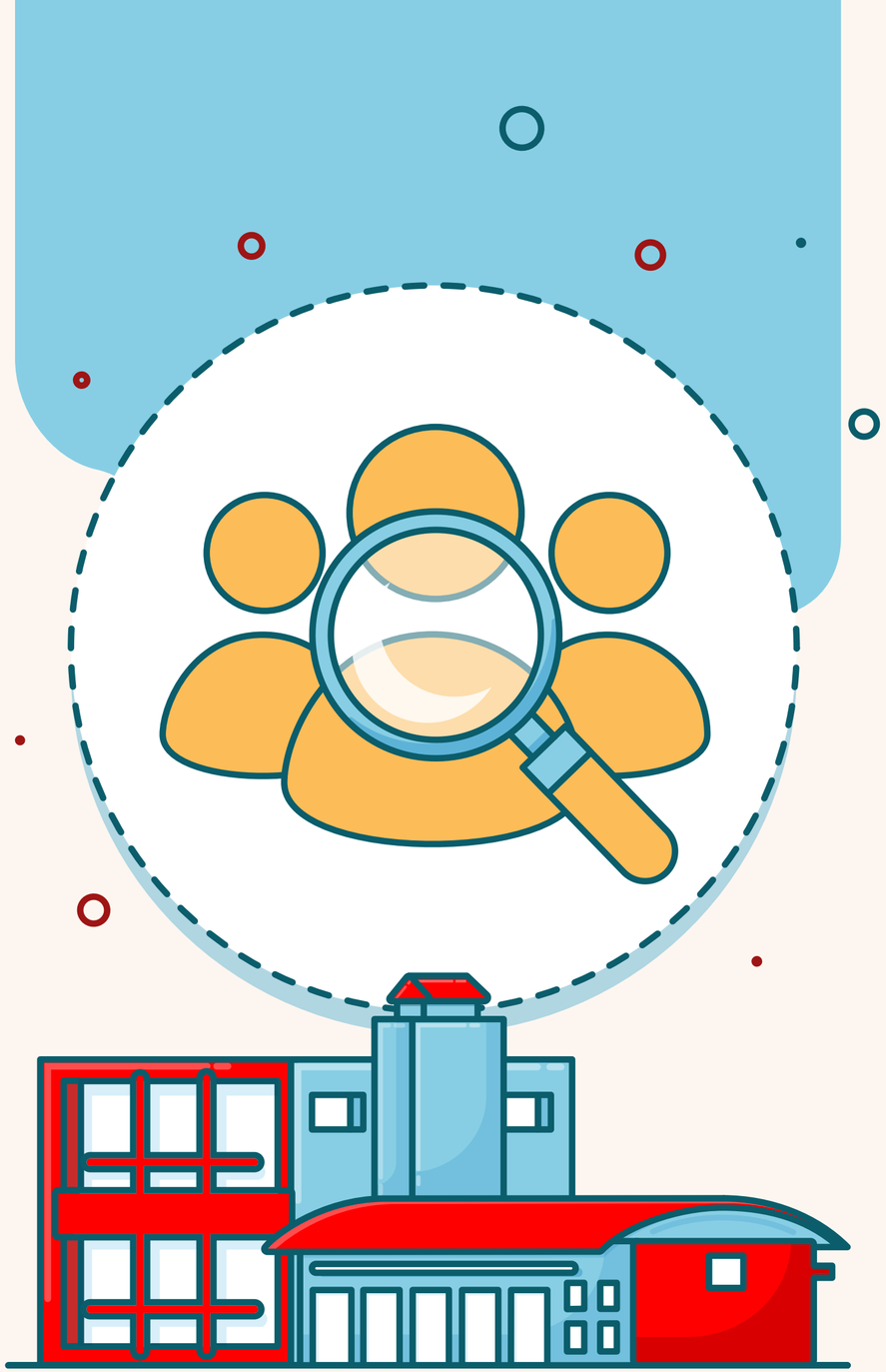
TREINAMENTO:

Além disso, considerando que os dados pessoais que a empresa lida passam pelas pessoas que nela trabalham, um dos pontos principais é o treinamento dos funcionários para que durante o **exercício de suas funções** atuem de acordo a **Política de Privacidade** e a **Política de Segurança da Informação** da empresa.

TERMO DE RESPONSABILIDADE:

Para isso, além do treinamento, é recomendável que o departamento jurídico elabore um termo de responsabilidade em que o funcionário **declare estar ciente** e **concordar com as políticas de proteção de dados** da organização e convocar o RH para incluir a assinatura deste termo no processo de contratação, bem como garantir que todos os funcionários já contratados o assinem.

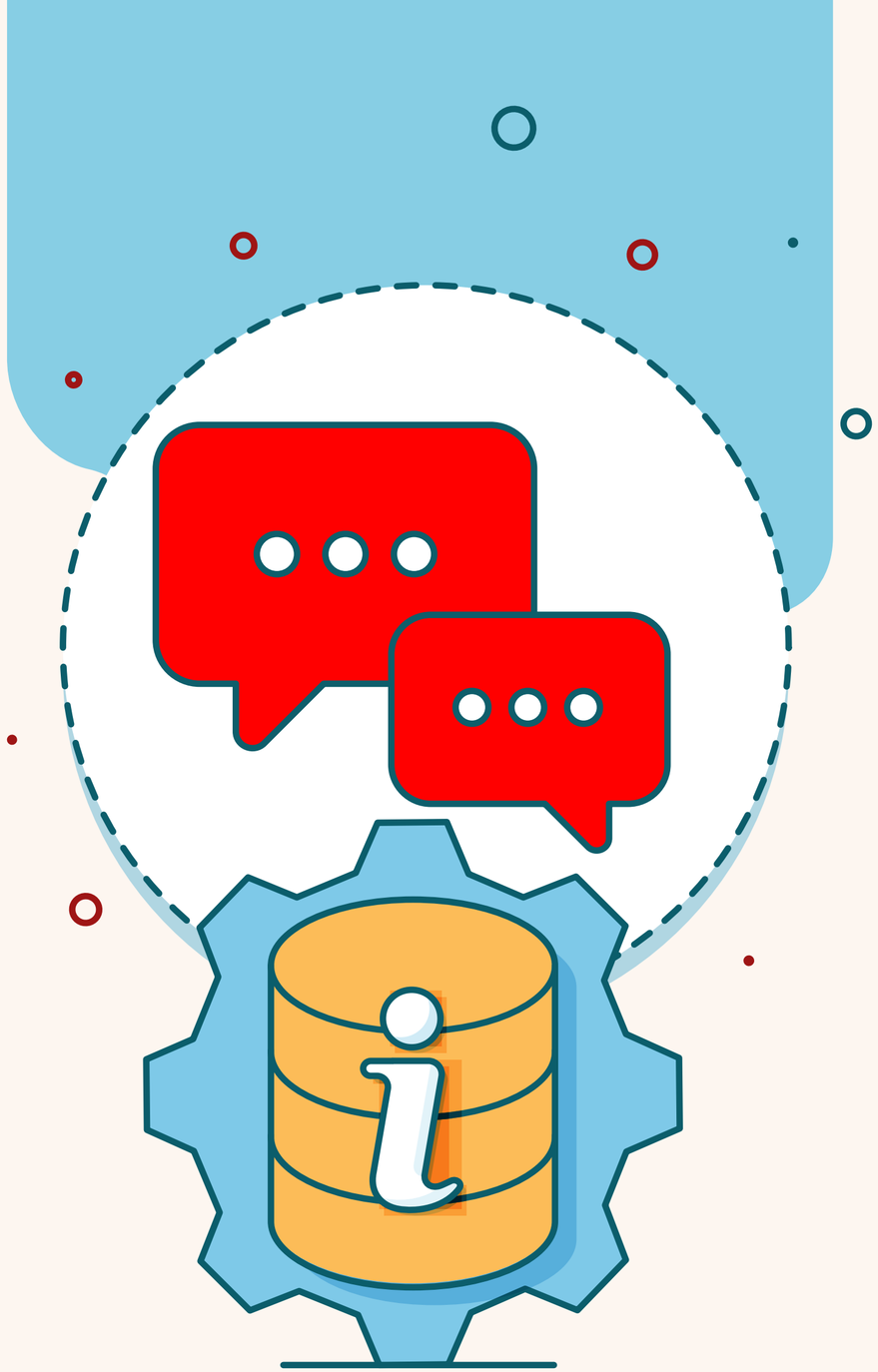
Clique aqui para baixar um modelo de termo de responsabilidade.



4. RELAÇÃO DE TRABALHO COM FUNCIONÁRIOS

RESUMO:

- Colete o **mínimo** de dados pessoais possível, sobretudo evitando ter acesso a dados sensíveis quando estes não forem necessários;
- **Documente** todo os processos relacionados ao RH que envolvam tratamento de dados pessoais;
- Revise os contratos de trabalho ou elabore aditivos, **incluindo cláusulas a respeito do tratamento de dados** de forma destacada;
- Treine seus funcionários para que durante o exercício de suas funções, atuem de acordo a **Política de Privacidade** e a **Política de Segurança da Informação** da empresa;
- Elabore um **Termo de Responsabilidade** para que o funcionário declare estar ciente, concordando com as políticas de proteção de dados da organização e garantindo que todos os funcionários o assinem.



5. GARANTIR MEIOS DE ATENDER AOS DIREITOS DO TITULAR DOS DADOS

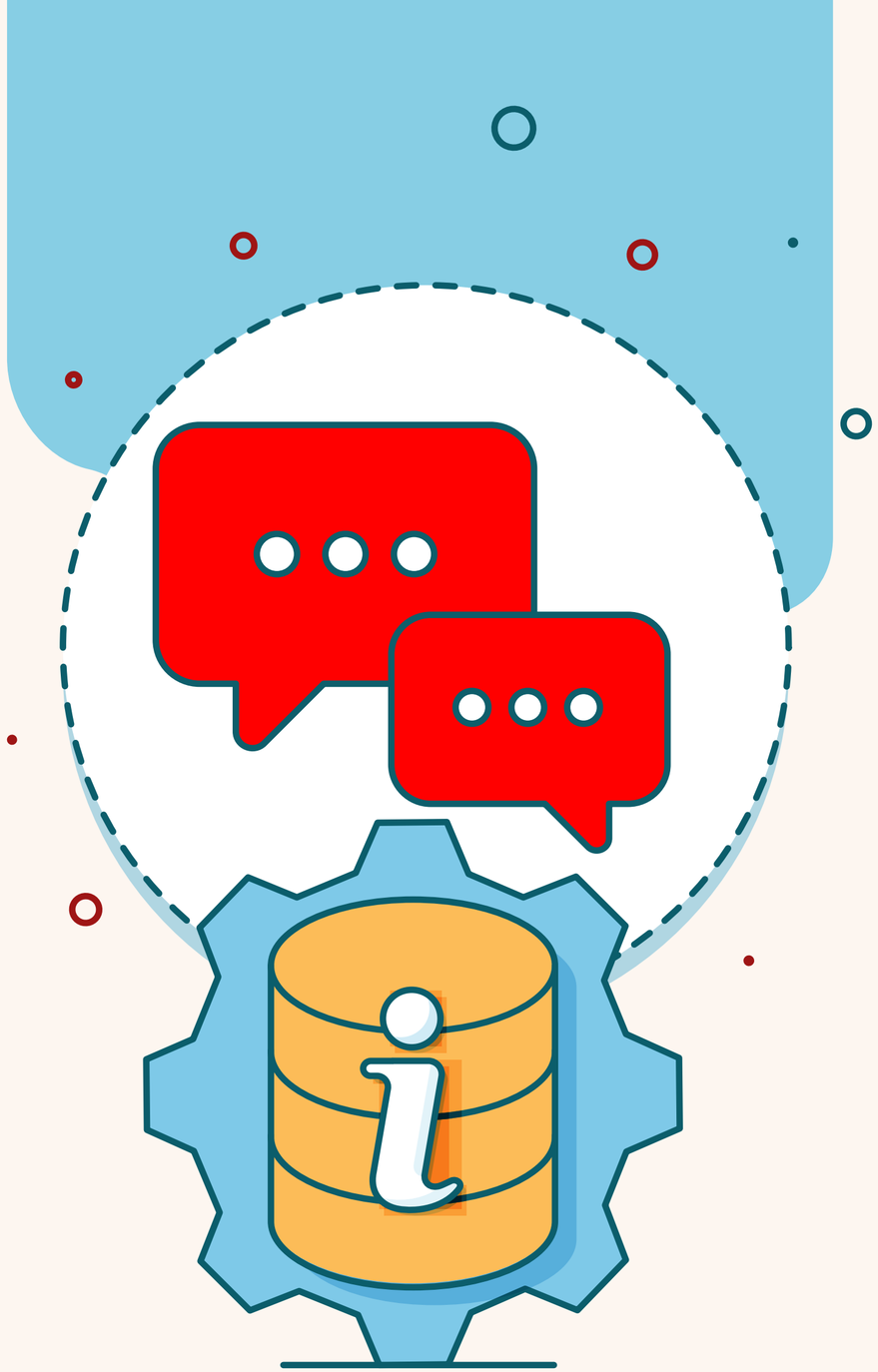
QUAIS OS DIREITOS DO TITULAR DE DADOS PESSOAIS?

Com relação aos seus clientes pessoa física e a seus funcionários, é preciso se atentar aos direitos que a lei assegura aos titulares de dados. O titular dos dados tem **direito** à confirmação do tratamento de seus dados; ao **acesso facilitado** a informações sobre o **tratamento de seus dados** pessoais; **correção de dados incompletos, inexatos** ou **desatualizados; à anonimização, bloqueio** ou **eliminação** de dados desnecessários, excessivos ou tratados em desconformidade com a lei; à **transferência de seus dados** pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa; se **opor ao tratamento** de seus dados pessoais quando verificado o **descumprimento de disposições da LGPD**; e **revogar o consentimento** dado anteriormente para o tratamento de seus dados pessoais.

COMO GARANTIR ESSES DIREITOS?

A empresa deve adequar sua **estrutura operacional** e **técnica** para viabilizar e cumprir com todos os direitos que a lei garante ao titular dos dados, desenvolvendo mecanismos para permitir que estes exerçam seus direitos, de forma **facilitada** e **gratuita**, mantendo um canal de comunicação para receber os pedidos acima indicados.

Tendo isso em vista, estamos **desenvolvendo melhorias** para viabilizar às distribuidoras, por intermédio do sistema da Target, atender de maneira **facilitada** a eventuais pedidos por parte dos titulares de dados, como a possibilidade de anonimização ou bloqueio dos dados pessoais, a obtenção de consentimento para o cadastro dos dados no sistema e a extração de um relatório sobre o uso e guarda dos dados.



5. GARANTIR MEIOS DE ATENDER AOS DIREITOS DO TITULAR DOS DADOS

COMO RECEBER OS PEDIDOS DOS TITULARES DE DADOS?

Como visto, a pessoa responsável por receber e responder estes pedidos é o DPO, mas é preciso **estabelecer como será o processo para requerimento de exercício destes direitos**. Uma forma de receber os pedidos que muitas empresas têm adotado é por meio de um **formulário assinado**, o qual pode ser disponibilizado aos titulares através de contato com o DPO por e-mail. Ainda, é importante que, por meio deste formulário ou de qualquer outro meio que se escolha adotar, seja **possível confirmar** que o **requerente é o próprio titular dos dados**.

Clique aqui para seguir um modelo de formulário de requerimento

RESUMO:

- Adeque sua estrutura operacional e técnica **viabilizando mecanismos** para permitir que os titulares exerçam seus direitos, de forma facilitada e gratuita;
- Mantenha um **canal de comunicação** para receber os pedidos dos titulares;
- Elabore um **formulário de solicitação** de exercício de direitos para que os titulares preencham de acordo com o seu pedido, assinem e enviem ao DPO por e-mail.

6. ELABORAR UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O QUE É UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO?

É claro que um dos pontos fundamentais a respeito da proteção de dados pessoais é a **segurança da informação**. A política de segurança da informação deve observar a confidencialidade, assegurando que as informações da empresa sejam **acessadas apenas por pessoas autorizadas**; a integridade dos dados, de modo que estes apresentem informações confiáveis, íntegras e verdadeiras; e a disponibilidade dos dados, garantindo que estes estejam disponíveis para uso sempre que demandados por alguém com **permissão de acesso**.

COMO ELABORAR?

Para elaborar uma política de segurança da informação, é preciso identificar o que já existe na empresa em relação à proteção de dados, e **identificar todas as ameaças e vulnerabilidades** que existem ou podem vir a existir. Para isso, é importante considerar os diferentes níveis de acesso que as várias categorias de usuários terão e classificar a **confidencialidade dos dados**.

A Política de segurança da informação **deve observar normas técnicas**, como ISO 27001 e ISO 27002, e deve abordar o uso de criptografia e outros recursos de proteção de dados; política de backup, recuperação e recursos de prevenção de perda de dados; políticas de senhas e restrições de acesso; normas sobre o uso geral de dispositivos, incluindo uso da internet, instalação de softwares e acesso por dispositivos pessoais; rotinas de auditoria; boas práticas de uso do e-mail corporativo e penalidades aplicáveis.

6. ELABORAR UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

QUEM DEVE PARTICIPAR DA ELABORAÇÃO?

Como todos os setores da empresa são afetados pela política de segurança da informação, é importante que haja o **máximo de representação possível na equipe destacada para elaborar a política**. Assim, os aspectos específicos de áreas diferentes podem ser considerados, evitando que as normas estabelecidas sejam desrespeitadas por incompatibilidade com as tarefas de um setor.

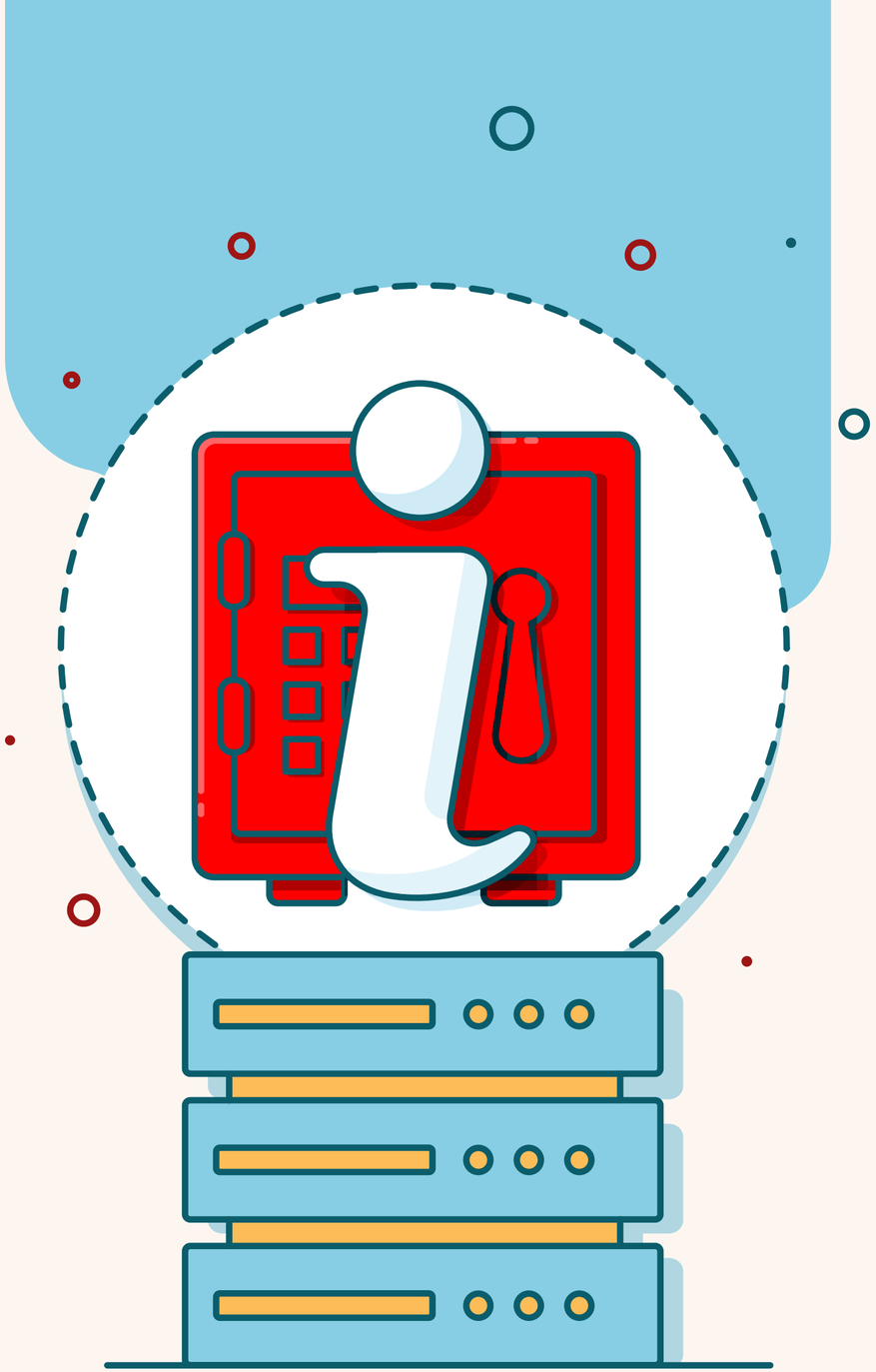
O RH deve acompanhar a elaboração, garantindo que as regras estabelecidas respeitam as leis trabalhistas. É importante, também, que a política esteja **de acordo com a cultura organizacional, missão, visão e valores da empresa**. Afinal, ela é parte da estratégia do negócio.

E OS DADOS QUE ESTÃO NO SISTEMA DA TARGET?

Com relação aos dados armazenados nos sistemas de gestão, **a Target já está tomando as medidas necessárias** para garantir a adequada segurança dos dados.

RESUMO:

- Organize uma equipe para elaborar a **Política de Segurança da Informação** com representantes de todos os setores da empresa que serão afetados por ela;
- **Certifique-se que Política aborda:** uso de criptografia e outros recursos de proteção de dados; política de backup, recuperação e recursos de prevenção de perda de dados; políticas de senhas e restrições de acesso; normas sobre o uso geral de dispositivos, incluindo uso da internet, instalação de softwares e acesso por dispositivos pessoais; rotinas de auditoria; boas práticas de uso do e-mail corporativo; e penalidades aplicáveis.



7. ELABORAR UMA POLÍTICA DE PRIVACIDADE

O QUE É UMA POLÍTICA DE PRIVACIDADE?

Por fim, mas não menos importante, você deve ter uma Política de Privacidade contendo as **práticas e medidas de Privacidade e Segurança adotadas** pela organização com o objetivo de levar transparência aos titulares dos dados pessoais a respeito do tratamento que realiza.

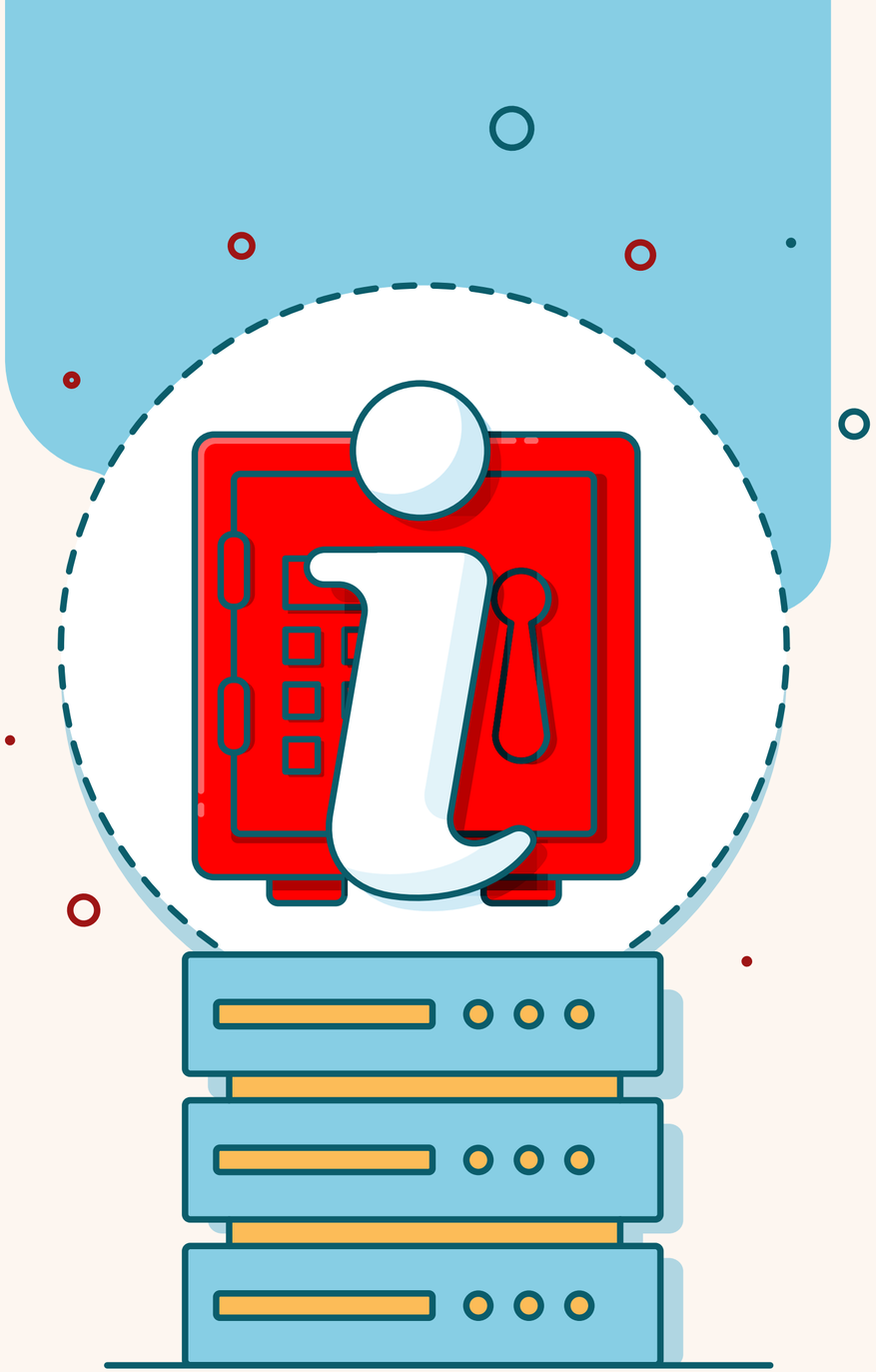
A POLÍTICA PRECISA SER ACESSÍVEL

Tendo isso em vista, é importante que a Política seja escrita em **linguagem simples e objetiva e esteja publicada em um local de fácil acesso**, como, por exemplo, o website da empresa.

O QUE A POLÍTICA DEVE CONTER?

A Política de Privacidade deve conter:

- **Informações gerais** sobre a empresa, como razão social, CNPJ e endereço.
- **Informações sobre o tratamento de dados**, indicando quais dados pessoais são coletados, inclusive os dados não informados pelo usuário, como IP, localização etc.; de onde os dados são coletados (fonte); para quais finalidades os dados são utilizados; onde os dados ficam armazenados; o período de armazenamento dos dados (retenção); com quem esses dados são compartilhados (parceiros, fornecedores, subcontratados); a política de cookies (quais cookies são coletados, para quais finalidades, como são tratados, se há compartilhamento, quanto tempo ficam armazenados);
- Informações sobre **medidas de segurança** adotadas pela empresa;
- Informações sobre **exercícios de direitos**, indicando quais são os direitos do titular, como ele pode solicitá-los e como a empresa atende aos direitos requeridos.
- Informações de contato do **Data Protection Officer (DPO)** ou **encarregado de proteção de dados** da organização.
- **Data da última alteração** da Política de Privacidade.



7. ELABORAR UMA POLÍTICA DE PRIVACIDADE

QUEM DEVE ELABORAR?

A Política de Privacidade, pelo seu conteúdo, pode ser elabora pelo **Comitê de Privacidade juntamente com o setor Jurídico e o DPO**, nos casos em que estes não constituam o comitê.

Resumindo todas as dicas acima, preparamos um modelo que poderá ser utilizado como **referência** na elaboração da sua Política de Privacidade. Lembrando que cada empresa tem seu cenário específico e, por isso, a Política deve ser **adaptada** e **complementada** de acordo com a sua realidade.

Clique aqui para baixar o modelo de Política de Privacidade.

RESUMO:

- Convoque o **Comitê de Privacidade** juntamente com o setor **Jurídico** e o **DPO** para elaborar a **Política de Privacidade**;
- Escreva a Política de Privacidade em **linguagem simples** e **objetiva**;
- Certifique-se que Política de privacidade contém: informações gerais sobre a empresa, o tratamento de dados, as medidas de segurança adotadas pela empresa; o exercício dos direitos dos titulares, o contato do DPO, e data da última alteração da Política de Privacidade.
- Publique em um local de **fácil acesso** como, por exemplo, o website da empresa;
- Determine um período para revisão da Política de Privacidade e a **mantenha atualizada**.

CONHEÇA A TARGET SISTEMAS
ERP FEITO PARA DISTRIBUIDORES

CONHEÇA O ERP

LEIA MAIS CONTEÚDOS SOBRE DISTRIBUIÇÃO

BLOG

target SISTEMAS

TELEFONES

São Paulo/SP 11 3801.4015 | Porto Alegre/RS 51 3019.9189
Recife/PE 81 3269.8919 | Ribeirão Preto/SP 16 3442.7816
Salvador/BA 71 3013.4862 | Goiânia/GO 62 3432.9072
Rio de Janeiro/RJ 21 3449.1775 | Vitória/ES 27 9 98059156