Elaborado por: Moreira Suzuki Advocacia para Negócios
Formatado por: Aline Gomes
Aprovado por: Jacqueline Fenilli
Revisão: 0.0

CARTILHA SOBRE PROTEÇÃO DE DADOS PESSOAIS PARA ASSOCIADOS

MAN-LGPD-2

ACIM
ASSOCIAÇÃO COMERCIAL E EMPRESARIAL DE MARINGÁ

SUMÁRIO

INTRODUÇÃO 01

PARTE 1 | Compreendendo a Lei Geral de Proteção de Dados (LGPD)

1.1. O que é a LGPD e a quem ela se aplica? 03

1.2. O que são dados pessoais e dados pessoais sensíveis? 03

1.3. No que consiste o tratamento de dados? 04

1.4. Quem são os "agentes de tratamento" de dados? Qual a diferença entre um controlador e um operador? 05

1.5. Qual o papel do Encarregado? 06

PARTE 2 | Empresários como Titulares de Dados Pessoais

2.1. Direitos dos Empresários como Titulares de Dados 08

2.2. Acesso pleno às informações referentes aos dados tratados 09

PARTE 3 | Empresários como Controladores de Dados Pessoais

3.1. Observância aos direitos e princípios impostos pela Lei Geral de Proteção de Dados (LGPD) 12

3.2. Implementação de um processo completo de adequação à LGPD 14

3.3. Cuidados e Orientações Gerais 19

Olá, empresárias e empresários!

A Lei Geral de Proteção de Dados (LGPD) entrou em vigor em 2020. Trata-se de uma lei específica para regulamentar o uso de dados pessoais no Brasil, que impõe medidas de segurança e dispõe sobre os direitos dos titulares dos dados.

Nós, da ACIM, com o objetivo de auxiliar empresas e empreendedores a compreender melhor a legislação – que indiscutivelmente impacta todos os negócios do país – e promover as adequações necessárias aos novos parâmetros legais, trazemos a presente cartilha, que contém os principais pontos de atenção relacionados à LGPD.

De fato, a conformidade com as normas de proteção de dados se mostra relevante aos empresários não apenas pelos fatores regulatórios e reputacionais relacionados aos negócios profissionais – isto é, evitando-se as sanções impostas pela legislação e garantindo a competitividade e prestígio perante parceiros, fornecedores e clientes, que exigirão a implementação desses cuidados –, mas também pelo aspecto pessoal, na medida em que seus próprios dados e de todas as pessoas que integram a equipe da empresa também são titulares de dados que devem exigir a observância e respeito aos seus direitos.

Em outras palavras, ao passo em que os empreendedores são titulares de dados pessoais, que merecem ter garantias de segurança e acesso aos direitos e informações relacionados aos seus próprios dados, também desenvolvem negócios responsáveis por controlar e operar dados pessoais de terceiros e, por isso, devem garantir essa mesma segurança aos demais titulares no desempenho de suas atividades.

Diante disso, elaboramos uma cartilha bastante clara e objetiva para: (i) expor informações relacionadas ao acesso a direitos garantidos pela LGPD, por parte dos titulares; (ii) quais os principais cuidados, obrigações e medidas a serem observados pelas empresas no tratamento de dados de terceiros e; (iii) apontar dicas práticas e os pontos de atenção mais importantes para a implementação da LGPD nas empresas.

Em suma, esta cartilha se propõe a esclarecer alguns conceitos e informar, de maneira fácil, os direitos e deveres de empresas e empresários quando o assunto é Lei Geral de Proteção de Dados.

PARTE 1

Compreendendo a Lei Geral de Proteção de Dados (LGPD)

Para melhor compreender os direitos e obrigações relacionados à proteção de dados e impostos pela LGPD, é preciso esclarecer alguns dos conceitos basilares trazidos pela legislação.

1.1. O QUE É A LGPD E A QUEM ELA SE APLICA?

A LGPD, conforme dito no início deste documento, é uma lei específica dedicada a regulamentar o uso de dados pessoais no Brasil, impondo medidas de segurança a serem observadas, de modo a privilegiar os direitos dos titulares dos dados.
Sua aplicação se estende tanto a pessoas naturais quanto pessoas jurídicas que realizem, em suas atividades, operações de **tratamento de dados pessoais.**

1.2. O QUE SÃO DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS?

Dados pessoais são aqueles que identificam ou podem identificar o titular, de uma maneira bastante objetiva. São exemplos: nome, CPF, RG ou endereço, dentre tantos outros.

Já os **dados pessoais sensíveis** são aqueles que indicam 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.

1.3. NO QUE CONSISTE O TRATAMENTO DE DADOS?

“Tratar” dados significa desenvolver qualquer tipo de operação que envolva dados pessoais, tais como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A título ilustrativo, caracterizam operações de tratamento a coleta de informações de clientes, funcionários ou terceiros para fins de cadastro ou registro, armazenamento dessas informações em bancos de dados (físicos ou digitais) e acesso a esses dados para fins de elaboração de documentos, contatos com os titulares, envio de newsletters e demais operações semelhantes.

O “ciclo de vida” de um dado pessoal dentro de uma empresa, então, abrange desde a sua coleta, com a entrada do dado nos servidores e armazenamento nos bancos de dados da empresa, passando por todos os usos e atividades nos quais está envolvido, até o eventual arquivamento ou eliminação.

Por se tratar de uma definição notoriamente ampla, que envolve praticamente todas as atividades intrínsecas ao desenvolvimento de um negócio e aplicável tanto a pessoas naturais e jurídicas, **é certo que a aplicabilidade da lei engloba praticamente todas as empresas do Brasil.**

1.4. QUEM SÃO OS "AGENTES DE TRATAMENTO" DE DADOS? QUAL A DIFERENÇA ENTRE UM CONTROLADOR E UM OPERADOR?

Se, por um lado, os "Titulares" de dados são as pessoas naturais a quem se referem os dados objeto de tratamento, os **agentes de tratamento de dados**, para a LGPD, são as pessoas físicas ou jurídicas responsáveis por realizar essas operações de tratamento de dados dos titulares.

Estes agentes são divididos em "Controlador" e "Operador" pela legislação, de acordo com o papel que desempenham na utilização dos dados pessoais.

Ao **Controlador** competem as decisões essenciais a respeito dos procedimentos de tratamento de dados, de modo que é o responsável por determinar o propósito (finalidade) e o meio pelo qual se realizará o tratamento dos dados em uma determinada atividade. Todavia, embora o Controlador seja o responsável pela definição do propósito e do meio de realização do tratamento de dados, ele não necessariamente precisa executar o meio de tratamento, podendo delegar esta tarefa – hipótese da qual desponta a figura do Operador.

Operador, então, é o agente que recebe as delegações do Controlador acerca do meio de tratamento dos dados. Assim, é um agente que pode executar o tratamento de dados em nome do Controlador, seguindo instruções emanadas por ele e vinculando-se a estas instruções, não possuindo autonomia ou ingerência sobre decisões essenciais relacionadas ao propósito da atividade de tratamento.

Assim, ainda que detenha certa discricionariedade para a tomada de decisões, essas decisões devem se restringir ao aspecto operacional da atividade, jamais podendo o Operador tomar decisões de caráter essencial ou que impactem no *propósito* da atividade de tratamento de dados.

Em suma, os agentes se diferenciam pelo poder decisório e, também, pela essencialidade

das decisões que podem tomar, de modo que o Controlador possui grande liberalidade para a tomada de decisões, enquanto as decisões do Operador devem estar vinculadas ao propósito pré-definido pelo Controlador e se limitar ao âmbito de operacionalização da atividade delegada, como o meio e a forma de execução.

1.5. QUAL O PAPEL DO ENCARREGADO?

A LGPD traz, ainda, a figura do "**Encarregado**", que é uma pessoa – física ou jurídica – indicada pelos agentes de tratamento para **atuar como o canal de comunicação** entre os agentes, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD – órgão responsável por zelar pela proteção de dados pessoais no Brasil, garantir a aplicação e fiscalizar o cumprimento da LGPD).

É ele o responsável por colher demandas, reclamações e comunicações dos titulares e da ANPD, prestar os devidos esclarecimentos, orientar os agentes para que sejam tomadas as providências cabíveis, garantir a observância de medidas de segurança de dados implementadas, orientar funcionários e parceiros a respeito dos procedimentos e cuidados necessários e lidar com eventuais incidentes de segurança e vazamento de dados.

Como visto, embora não se confunda com um "agente de tratamento", o Encarregado também desempenha um papel fundamental nas atividades de tratamento, integrando a equipe dos Controladores e Operadores e fazendo valer a LGPD no âmbito de cada empresa.

PARTE 2

Empresários como Titulares de Dados Pessoais

Todos os empresários e integrantes da equipe de uma empresa são também titulares de seus próprios dados pessoais, que são constantemente utilizados por outras empresas, parceiros, fornecedores e clientes para a realização de atos diversos, como pagamentos, emissão de notas fiscais, recibos, registro do histórico de negócios, manutenção de cadastros de contatos, dentre tantas outras atividades comuns ao meio negocial.

Assim, é importante que todos os empresários conheçam seus próprios direitos e tenham pleno acesso às informações vinculadas aos seus dados.

2.1. DIREITOS DOS EMPRESÁRIOS COMO TITULARES DE DADOS

A Lei Geral de Proteção de Dados, além de trazer uma lista de direitos do titular, busca auxiliar e garantir que os titulares conheçam e tenham meios de efetivar esses direitos relacionados aos dados pessoais.

Espera-se que as empresas, então, possibilitem meios que concretizem o acesso dos titulares a todos esses direitos, para garantir que sejam integralmente observados e respeitados.

Em regra, todos os direitos listados abaixo podem ser exercidos diretamente pelo titular de dados ou por meio de um representante legalmente constituído, por meio do contato com os agentes de tratamento na pessoa do Encarregado. Cabe aos titulares, então, a prerrogativa de, a qualquer momento, solicitar:

- A confirmação da existência de tratamento de seus dados pessoais (art. 18, I, da LGPD);
- Acesso aos seus dados pessoais (18, II, da LGPD);
- Correção de dados incompletos, inexatos ou desatualizados (art. 18, III, da LGPD);

- Eliminação dos seus dados pessoais, resguardadas as hipóteses previstas no art. 16 da LGPD* (art. 18, IV e VI, da LGPD);
- Anonimização de seus dados pessoais que sejam desnecessários, excessivos, ou que estejam sendo tratados fora dos limites da LGPD (art. 18, IV, da LGPD);
- Bloqueio do tratamento dos seus dados pessoais que sejam desnecessários, excessivos, ou que estejam sendo tratados fora dos limites da LGPD (art. 18, IV, da LGPD);
- Portabilidade de seus dados pessoais (art. 18, V, da LGPD);
- Informação sobre as entidades públicas e privadas com as quais são realizados eventuais compartilhamentos de dados (art. 18, VII, da LGPD);
- Direito a não consentir com o fornecimento de dados e as informações sobre as consequências dessa negativa (art. 18, VIII, da LGPD);
- Direito de revogar o consentimento previamente concedido ao tratamento de dados (arts. 8º, §5º e 18, IX, da LGPD);
- Direito de peticionar contra a Nação Digital perante a Autoridade Nacional de Proteção de Dados (art. 18, §1º, da LGPD);
- Direito de não se sujeitar a, ou solicitar revisões de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, incluindo *profiling* (art. 20 da LGPD).

2.2. ACESSO PLENO ÀS INFORMAÇÕES REFERENTES AOS DADOS TRATADOS

Os direitos acima listados, frutos dos princípios norteadores da LGPD, deixam claro que a legislação busca garantir aos Titulares de Dados que detenham a

* Cumprimento de obrigação legal ou regulatória; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; transferência a terceiro, desde que respeitados os requisitos de tratamento; uso exclusivo da Nação Digital, vedado seu acesso a terceiro, e desde que anonimizados os dados.

chamada “Autodeterminação Informativa”, isto é, que possuam controle sobre seus próprios dados pessoais.

Assim, cabe também aos próprios titulares certificar que as atividades de tratamento envolvendo seus dados sejam realizadas de forma adequada e proporcional, além de exigir informações claras, completas e transparentes, livremente acessíveis, para que possam efetivamente exercer seus direitos como titulares dos dados como desejarem.

Uma atividade de tratamento pode contar um fluxo relativamente complexo e longo de dados pessoais. Assim, para garantir essa autodeterminação informativa aos titulares, é importante que Controladores e Operadores forneçam informações detalhadas acerca de todos os aspectos relevantes das operações de tratamento, tais como:

- Confirmar aos Titulares que seus dados estão, realmente, sendo tratados;
- Expor **quais os dados coletados**, armazenados, mantidos e utilizados nas atividades de tratamento desenvolvidas e **quais os meios de coleta**;
- Informar **qual o propósito (finalidade)** para o qual os dados são empreendidos – garantindo que seja uma finalidade pertinente e que, para isso, não sejam coletados dados excessivos ou desnecessários;
- Comunicar **quem tem acesso a esses dados**, especialmente se houver **compartilhamento de dados pessoais com terceiros** – bem como quem seriam esses terceiros e qual a razão desse compartilhamento;
- Garantir que sejam implementadas **medidas de segurança adequadas** a proteger a confidencialidade, integridade e inviolabilidade dos dados tratados;
- Expor **onde e como os dados são armazenados**;
- Informar qual seria o **prazo de armazenamento** dos dados e **qual a forma de eliminação** após a conclusão da finalidade para a qual foram coletados;
- Anunciar **canais de comunicação** para que os titulares possam exercer seus direitos, tirar dúvidas, fazer sugestões, reclamações e quaisquer esclarecimentos que desejarem.

PARTE 3

Empresários como Controladores de Dados Pessoais

Agora que você conhece os seus próprios direitos como titular de dados, é necessário compreender que todos os clientes e consumidores também possuem os mesmos direitos, na posição de titulares de dados, valorizando a própria segurança e o controle de suas próprias informações, assim como vocês empresários.

Diante disso, esta etapa da cartilha se dedicará a indicar dicas de adequação das empresas às novas normas de proteção de dados, cuidados e medidas gerais que devem ser observados e orientações para garantir a segurança de todos os dados pessoais que estejam sob a responsabilidade de suas empresas.

3.1. OBSERVÂNCIA AOS DIREITOS E PRINCÍPIOS IMPOSTOS PELA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Além dos direitos e informações expostos nas seções anteriores desta Cartilha, é importante que os empresários conheçam os princípios estabelecidos pela LGPD e que devem nortear todas as operações de tratamento de Dados por eles realizadas. Tais princípios poderão ser encontrados para leitura e conhecimento mais profundo no art. 6º, VII, da LGPD, transcrito a seguir:

> *Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
>
> ***I - FINALIDADE:*** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> ***II - ADEQUAÇÃO:*** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - NECESSIDADE: limitação do tratamento 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;

IV - LIVRE ACESSO: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - QUALIDADE DOS DADOS: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - TRANSPARÊNCIA: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - SEGURANÇA: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - PREVENÇÃO: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - NÃO DISCRIMINAÇÃO: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Em geral, conhecer seus próprios direitos como Titular de Dados ajuda imensamente na compreensão do que é realmente importante, qual o espírito da LGPD e o que é preciso garantir também aos seus clientes e consumidores – fatores estes que são abarcados pelos princípios dispostos acima e que devem nortear a conduta dos agentes de tratamento.

3.2. IMPLEMENTAÇÃO DE UM PROCESSO COMPLETO DE ADEQUAÇÃO À LGPD

Como se vê de todo o exposto, a LGPD traz um novo paradigma relacionado à forma como os negócios tratam dados pessoais. A legislação busca modificar a cultura de acúmulo de dados e coleta indiscriminada para uma mentalidade de atenção à segurança, prevenção e transparência.

Posto que as atividades de tratamento sempre fizeram parte da rotina de todas as empresas, o processo de adequação às novas normas que buscam regular a forma como esse tratamento é realizado certamente é complexo e não pode ser subestimado.

Tal processo exige uma análise intensa de todos os setores da empresa, com o mapeamento de todo o fluxo de dados nas diversas atividades desenvolvidas até o momento de eliminação e a implementação prática das devidas adequações em cada uma das etapas.

Nesse contexto, o processo de adequação requer não apenas o auxílio técnico e jurídico, mas uma mudança de cultura, com a conscientização e comprometimento de gestores e colaboradores, de modo a perpetuar as adequações feitas e manter a empresa adequada.

O primeiro passo, portanto, é entender que tal processo não se trata de um "*ônus*" para buscar a conformidade com processos meramente "*burocráticos*"; pelo contrário, trata-se de uma oportunidade de organizar, otimizar e alinhar os processos, reduzir riscos de segurança, reduzir custos desnecessários e construir uma reputação positiva perante parceiros e clientes.

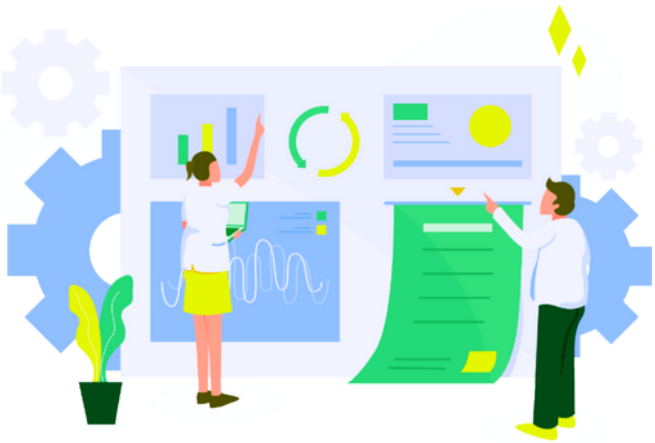
Em outras palavras, o processo de adequação não ocorre do dia para a noite, devendo ser planejado com antecedência e executado/implementado gradualmente; todavia, certamente as empresas se beneficiarão de seus frutos no longo prazo.

Como forma de facilitar a implementação desse processo pelos associados ACIM, trazemos abaixo alguns dos **principais pontos de atenção** que devem ser observados pelos empresários no momento de implementar um projeto de conformidade em seus negócios.

3.2.1. MAPEAMENTO DO FLUXO DE DADOS DA EMPRESA

Mapear o fluxo de dados da empresa é indispensável para entender que tipo de dados são tratados pela empresa e qual o "caminho" percorrido por ele entre os diversos setores, até sua eliminação.

Esta etapa dará uma perspectiva geral sobre o funcionamento prático do negócio e servirá como base fundamental para todas as demais, razão pela qual deve ser o primeiro ponto de atenção a ser observado em um projeto sério de conformidade.



Esta etapa envolve a busca de respostas para perguntas como: quais são os dados coletados? *Os dados tratados pela empresa são pessoais, ou pessoais sensíveis? Como, e por quem, é realizada a coleta? Quem possui acesso a cada um deles? Há compartilhamento com terceiros? Qual o público atingido pelas atividades de tratamento? Por quanto tempo e em quais meios os dados serão mantidos? Como e quando serão eliminados? Quem se responsabiliza por seu processamento? Qual é a finalidade do tratamento e coleta? Quais dados são essenciais à prestação do serviço, e quais são suplementares ou dispensáveis?*

As respostas obtidas permitirão o estabelecimento de diretrizes e um plano de ações eficaz e condizente com a realidade da empresa.

3.2.2. ADEQUAÇÃO DE CONTRATOS E DOCUMENTOS

Muito provavelmente, uma das maiores necessidades que exsurgirão após o primeiro passo será a adequação dos documentos já utilizados pela empresa.

Realmente, em se tratando da nova realidade do tratamento de dados, será de

suma importância rever documentos como contrato social, contratos de trabalho, contratos de fornecimento e/ou parceria, contratos de compra e venda ou prestação de serviços, para que sejam adaptados à nova realidade, de modo a proteger os interesses de todos os envolvidos: empresa, colaboradores, parceiros, fornecedores e clientes.

Essa adequação busca, de modo geral, materializar os direitos e obrigações impostos pela LGPD, dispondo sobre questões como:

- Qual o papel de cada parte em cada uma das relações contratuais, com a respectiva divisão de responsabilidades;
- Indicação dos dados tratados, período e meio de armazenamento;
- Finalidade do tratamento de dados;
- Regulamentação sobre eventual compartilhamento ou terceirização do tratamento de dados;
- Regulamentação de confidencialidade.

Como visto, os princípios, deveres e cuidados gerais impostos pela LGPD, aplicáveis aos agentes que exercem atividades de tratamento de dados, podem servir para balizar as principais questões que impactarão as relações contratuais.

3.2.3. ELABORAÇÃO DE DOCUMENTOS COMPLEMENTARES ESPECÍFICOS

Além da adequação dos contratos e documentos já utilizados na rotina da empresa, um dos grandes passos em direção à conformidade é complementar o arcabouço de documentos com a elaboração de todos os documentos que se fizerem necessários.

Este rol de documentos complementares pode envolver os contratos relacionados ao Encarregado, o *Data Processing Agreement**, relatório de

* Documento utilizado para regular eventuais compartilhamentos de dados, especificando os requisitos de tratamento, suas finalidades, bem como delimitando as responsabilidades no caso de infração por uma das partes.

impactos à proteção de dados, manual de boas práticas, termos de consentimento e cartilhas informativas.

Além disso, considerando a grande relevância de marketing e publicidade nos meios virtuais, as empresas que possuírem site próprio também precisarão elaborar (ou atualizar) suas políticas de privacidade e termos de uso, deixando-as em destaque nas suas respectivas páginas.

3.2.4. CONTRATAÇÃO DE UM ENCARREGADO

Por servir como meio de comunicação com as autoridades de proteção de dados e os próprios titulares, além de servir como um dos líderes de implementação da LGPD no âmbito interno da empresa, a contratação de um encarregado capacitado deve ser um dos grandes pontos de atenção nos processos de conformidade.

Em geral, é preferível prezar pela proximidade e multidisciplinariedade, privilegiando pessoas (físicas ou jurídicas) que conheçam, com certa intimidade, a realidade prática da empresa – isto é, que tenha familiaridade com diversos aspectos, como o operacional, financeiro, gestão de pessoas, etc. –, para que possa dar respostas rápidas e assertivas sempre que solicitado.

O Encarregado também deve ter certa autonomia e, idealmente, não acumularia funções, a fim de evitar eventuais conflitos em sua atuação.

3.2.5. TREINAMENTO E ORIENTAÇÃO DA EQUIPE E REFORMA DA CULTURA DE TRABALHO

Mais do que executar um plano de ações, é preciso garantir a manutenção do estado de conformidade da empresa. Para isso, faz-se necessário adotar novas políticas internas e fazer um trabalho de divulgação e orientação com toda a equipe.

Garantir a adequação aos ditames legais não é responsabilidade apenas do

setor jurídico, TI ou dos recursos humanos, mas sim de toda a empresa. Assim, é preciso que todos internalizem a cultura estabelecida pela LGPD, que preza por valores como a transparência, clareza, informação ampla, segurança e preservação da intimidade e privacidade.

3.2.6. ESCOLHA CRITERIOSA DE FORNECEDORES E PARCEIROS

De nada valerá toda a reforma estrutural e cultural se não houver, também, um procedimento mais criterioso na escolha das empresas com as quais você irá se envolver.

Afinal, além do fator econômico e prático, a adequação também impacta o aspecto reputacional da empresa, na medida em que é importante para os consumidores buscar empresas que ofereçam segurança, assim como para os demais empresários, que procuram se envolver com empresas que possuam o mesmo nível de responsabilidade que eles.

Dessa forma, buscar uma rede de empresas que também estejam em processo de adequação trará, além de um respaldo reputacional entre os consumidores, uma maior segurança na proteção dos dados que estejam sob os cuidados de sua empresa.

3.2.7. DAR TRANSPARÊNCIA AOS TITULARES E EXPOR O ESTADO DE CONFORMIDADE

Todas as diversas medidas implementadas não serão plenamente efetivas se os titulares dos dados não tiverem conhecimento delas. Assim, é interessante que as adequações promovidas sejam veiculadas também aos titulares por meio de documentos, cartilhas e/ou informativos claros e acessíveis.

Estas medidas, além representarem o cumprimento com o dever de observância aos princípios e obrigações impostos pela LGPD, também fortalecerão a reputação da empresa e gerará uma maior confiança por parte de terceiros – como clientes, parceiros, fornecedores e colaboradores.

3.3. CUIDADOS E ORIENTAÇÕES GERAIS

Embora não integram, essencialmente, o processo de adequação e conformidade à LGPD, algumas medidas e cuidados gerais podem ser implementados pelas empresas a fim de maximizar os resultados de seu processo. Tendo isso em vista, passamos a apresentar algumas práticas benéficas em termos de proteção de dados e cuidados que auxiliarão no cumprimento de todas as medidas de segurança com os dados dos titulares:

- O processo de adequação deve refletir o que a empresa ***realmente é, não como deveria ser***. Não há sentido em listar ou divulgar processos internos e medidas de segurança que não possuem aplicação prática – especialmente porque o estado de conformidade pode ser gradualmente aperfeiçoado com o tempo. Em outros termos, é importante evitar gerar expectativas incoerentes, devendo-se sempre prezar pela transparência, clareza e honestidade perante os titulares;

- Mapear e *fluxogramar* os processos internos de uma forma completa, exibindo-os internamente aos colaboradores, pode ajudar na compreensão do funcionamento do negócio por toda a equipe e auxiliar na internalização da cultura de proteção de dados;

- As regras e diretrizes estabelecidas devem ser comunicadas o quanto antes aos interessados. Preferencialmente, após o processo de adequação, é importante divulgar os principais pontos relacionados à proteção de dados desde o início da relação com clientes, parceiros e colaboradores, por meio dos documentos pertinentes;

- Os processos e medidas de adequação devem ser permanentemente revistos e reavaliados, tanto para garantir que ainda sejam seguros e façam sentido para a empresa, quanto para evitar que fiquem ultrapassados ou que deixem de ser implementados na prática rotineira da empresa;

- Ao utilizar serviços de terceiros – desde serviços de fornecimento e parcerias comerciais até serviços de armazenamento em nuvem, sites e plataformas –, procure conhecer o estado de conformidade deste terceiro

e busque privilegiar aqueles que já ofereçam certa maturidade em matéria de adequação à LGPD;

- Exija de parceiros e empresas terceirizadas que também se comprometam a cumprir integralmente as regras da LGPD e todas as medidas de segurança necessárias nos processos de tratamento de dados;
- Sempre que possível, recomenda-se a segmentação das permissões de acesso à colaboradores ou setores específicos, que efetivamente precisem do acesso aos dados para desenvolver suas funções ou atividades específicas, a fim de manter a inviolabilidade dos dados manuseados pela empresa e evitar acessos desnecessários ou vazamentos;
- Caso um titular entre em contato para pedir qualquer tipo de informação relacionada aos seus dados pessoais, é interessante que seja encaminhado para um setor competente, geralmente liderado pelo Encarregado;
- É importante certificar a identidade do titular sempre que este for usufruir de um serviço ou caso requeira informações acerca de dados ou informações de quaisquer serviços previamente realizados;
- Jamais fornecer quaisquer dados ou informações dos Titulares para terceiros que não estejam devidamente autorizados pelo próprio titular. Ainda que o terceiro apresente a autorização, obedecer aos protocolos e verificar a identidade deste terceiro;
- Ao atender clientes ou realizar processos seletivos, coletar estritamente os dados necessários para a identificação ou realização da atividade pretendida, evitando a coleta de dados excessivos e desnecessários, especialmente dados pessoais sensíveis;
- Evitar a utilização de meios como o WhatsApp ou E-mail para a coleta de dados pessoais ou, sucessivamente, implementar um plano de eliminação rápido e eficaz sobre estes meios, evitando que os dados permaneçam indefinidamente armazenados (e, muitas vezes, duplicados) em meios inseguros.
- Informar os titulares da existência de todos os documentos, cartilhas e informativos relacionados à proteção de dados e onde podem ser

encontrados, estimulando-os a realizar a leitura completa de todos eles e a entrar em contato para prestar qualquer tipo de esclarecimento;

- Tomar cuidados especiais no manuseio de documentos físicos, para manter a organização e evitar a perda ou a separação de documentos do mesmo titular em locais diversos;
- Não conectar os computadores corporativos da empresa em redes estranhas ou que, por qualquer razão, não sejam sabidamente seguras e confiáveis;
- Elabore um plano de ação para os casos de ocorrência de incidente de segurança ou vazamento de dados e, assim que uma dessas situações for detectada, aja de forma proativa, tomando as providências cabíveis o mais rápido possível, de modo a minimizar os eventuais danos causados;
- Na medida do possível, procure anonimizar os dados pessoais obsoletos, para que possam ser reutilizados ou eliminados sem riscos.

Vale ressaltar, por fim, que o processo de conformidade deve ser feito sob medida para cada negócio, levando em consideração suas particularidades, de modo a refletir a realidade específica de sua empresa.