A Nova Lei de Proteção de Dados para Pequenas e Médias Empresas

PROTESTE

Google

SOBRE ESTA CARTILHA

Esta cartilha foi desenvolvida pela PROTESTE – Associação Brasileira de Defesa do Consumidor –, em parceria com o Google e com o Baptista Luz Advogados, e busca apresentar pontos de atenção e aspectos da LGPD relevantes às micro e pequenas empresas. Possui um caráter meramente informativo e não substitui nem deve ser entendido como aconselhamento jurídico.

CONTEÚDO

INTRODUÇÃO

Como se proteger em um mundo cada vez mais movido a dados? Esse foi o questionamento que levou à criação da Lei Geral de Proteção de Dados, conhecida como **LGPD**, e que passa a valer em agosto de 2020. À primeira vista, parece que a LGPD é uma lei complexa e que não foi feita sob medida para micro e pequenas empresas, mesmo que suas regras se apliquem a **todos os tipos de empresas**, independentemente do tamanho e do setor, online ou offline.

No entanto, mesmo as pequenas empresas possuem um papel importante para garantir a proteção dos dados das pessoas, e existem vários **passos práticos** que podem ser tomados para cumprir a lei e criar um ambiente de segurança e proteção de dados em seu negócio. Pensando nisso, esta cartilha foi criada para fornecer um conjunto simples de etapas para micro e pequenas empresas entenderem melhor como funciona a LGPD e implementarem **ações positivas no dia a dia dos negócios**.

Fique Esperto!

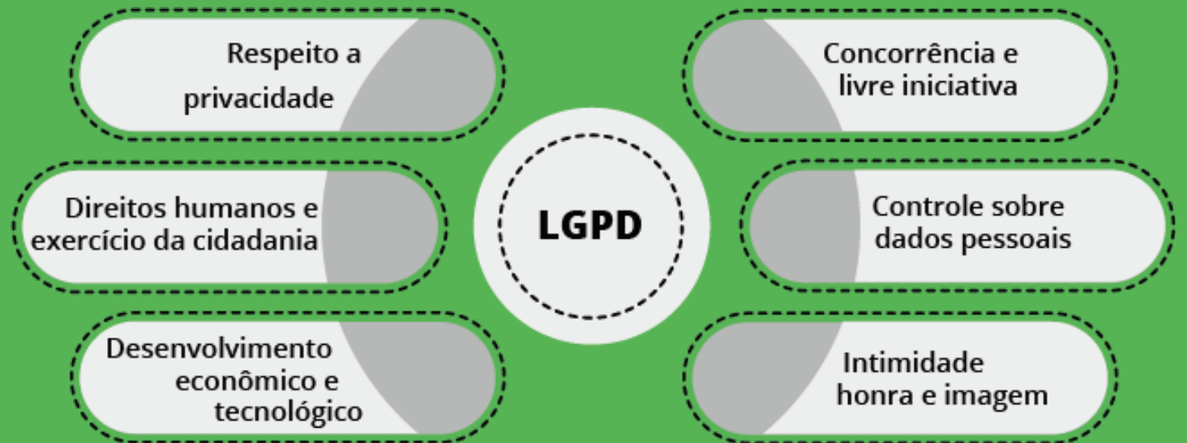
A lei entra em vigor em agosto de 2020. Até lá e mesmo depois disso, o governo pode criar novas regras específicas, que podem beneficiar micro e pequenas empresas. Essas regras devem ser criadas por meio de um órgão chamado Autoridade Nacional de Proteção de Dados. Acompanhe o site da PROTESTE para ver novidades que podem impactar os seus negócios.

O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS?

Todo mundo gosta de ganhar desconto em uma loja fazendo um cadastro, acessar uma rede social de graça em troca de publicidade ou mesmo participar de uma pesquisa para ganhar um vale-compras. Estamos cheios de exemplos de situações em que as pessoas não veem problema em fornecer alguns dados pessoais como nome, endereço, CPF e outros para receber alguma vantagem.

Ao mesmo tempo, ninguém fica feliz quando descobre que aquelas informações foram compartilhadas, sem justificativa, para alguma outra empresa ficar fazendo telemarketing, enviando um monte de e-mail ou mesmo usando seus dados para alguma fraude. Isso sem contar o transtorno que causa um vazamento de dados importantes, como números de cartão de crédito, senhas e informações bancárias.

Pensando nesses e outros aspectos, vários países pensaram em leis para orientar empresas a protegerem melhor dados pessoais, visando coibir abusos e práticas que possam ter um impacto indesejado na vida das pessoas. No Brasil, isso veio com a Lei n. 13.709/18, a LGPD, que traz muitas obrigações que terão impacto direto em praticamente qualquer empresa.



A LGPD vale pra todo mundo: empresas grandes ou pequenas, digitais ou não. Até agosto de 2020, todas as empresas vão ter que repensar vários aspectos do dia a dia de suas atividades, com o objetivo de cumprir as exigências da lei e proteger melhor seus consumidores, funcionários e parceiros comerciais. É um desafio e tanto, mas que **vai ajudar o Brasil** a ser mais competitivo em relação a outros países **e, também, evitar abusos** no uso de dados por empresas que não respeitam a privacidade e os direitos de seus clientes. Importante ter em mente que a LGPD não irá inviabilizar nenhum modelo de negócio, na verdade, irá ajudar muitos destes, pois confere um regime mais flexível e, ao mesmo tempo, mais seguro, no uso de dados pessoais quando comparado às leis atuais.

Decifrando o juridiquês

A LGPD é grande e complexa, e é fácil se perder no meio de tantos jargões jurídicos. Para descomplicar, **deciframos alguns dos mais importantes conceitos da LGPD**, aos quais micro e pequenas empresas precisam ficar atentas:

Conceito	O que é?	Por que é importante saber?
Titular	É a pessoa física a quem os dados pessoais se referem	Os titulares podem ser desde clientes e funcionários, até parceiros de negócio. Os dados pessoais de todos esses titulares devem ser respeitados.
Dado Pessoal	É qualquer informação relacionada a uma pessoa física, identificada ou identificável, ou individualizada	Se for dado pessoal, precisa ser protegido. RG, CPF, endereço e data de nascimento são alguns exemplos. Dados como histórico de compras, localização geográfica e preferências de consumo também podem ser considerados dados pessoais. Em suma, qualquer informação sobre uma pessoa.

Conceito	O que é?	Por que é importante saber?
Dado Anonimizado	É o dado relativo a um titular que não pode ser mais identificado, considerando a utilização de meios técnicos razoáveis na ocasião de seu tratamento	Dados anonimizados, em regra, estão fora do escopo de aplicação da LGPD. Assim, em uma pesquisa de mercado, os dados quantitativos, que digam respeito a um grupo grande de indivíduos (Exemplo: mulheres de 30 anos no estado de São Paulo) são considerados anonimizados por não serem capazes de identificar uma pessoa específica. Mas, para efetivamente ser considerado anonimizado, não deve ser mais possível saber a quem a informação se refere. Portanto, se algum número aleatório é atribuído a uma pessoa no lugar do seu nome ou CPF, por exemplo, mas que permite depois saber quem é essa pessoa, essa informação não será considerada anonimizada.

Conceito	O que é?	Por que é importante saber?
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 natural	A LGPD não proíbe o uso desses dados, apenas determina que merecem um cuidado extra. Se sua empresa coleta e utiliza alguns desses dados, vale refletir sobre a necessidade de utilizá-los e, se for realmente importante, buscar criar práticas e controles mais rigorosos para esses casos.
Bases Legais	Uma base legal é uma hipótese prevista na lei que autoriza que as empresas coletem, compartilhem ou de qualquer forma, utilizem os dados pessoais	Sem base legal, você não pode utilizar dados pessoais, simples assim. A mais conhecida das bases legais é o consentimento, mas vamos falar mais pra frente de outras hipóteses, pois a LGPD traz várias, e nenhuma vale mais do que a outra.

Conceito	O que é?	Por que é importante saber?
Tratamento	É qualquer uso que pode ser feito com dados pessoais, incluindo, mas não se limitando, por exemplo, coleta, registro, armazenamento, organização, consulta, divulgação, compartilhamento, transmissão, classificação, reprodução, processamento e avaliação	Em suma, tudo que se fizer com os dados pessoais é considerado tratamento pela LGPD. E todo tratamento de dados pessoais deve ser feito de acordo com a LGPD, sem exceção. Mais pra frente, vamos falar das melhores práticas para o tratamento de dados.
Controlador de Dados Pessoais	É a pessoa ou empresa que determina como e por que os dados são tratados	O controlador acaba assumindo mais obrigações na LGPD. Por exemplo, se eu tenho dados pessoais dos meus clientes e eu decido quando e como vou enviar um e-mail marketing para eles, eu sou um controlador. Na verdade, não é nem necessário ter os dados ou ter acesso a estes. Basta ser quem determina para o que os dados serão utilizados. Assim o fez, será considerado controlador.

Conceito	O que é?	Por que é Importante Saber?
Operador de Dados Pessoais	É a pessoa ou empresa que realiza o tratamento dos dados em nome de um controlador	O operador é, geralmente, um contratado do controlador, e tem menos obrigações e menos responsabilidades do que o controlador. No mesmo exemplo acima, se eu contrato uma agência para organizar minha base de contatos e disparar e-mail marketing, essa agência é operadora. Se eu contrato uma empresa para armazenar dados numa cloud, esta é operadora.
Encarregado	É a pessoa, física ou jurídica, interna ou externa, indicada para realizar o acompanhamento das atividades de proteção de dados dentro da empresa	Em alguns casos, pode ser que a empresa precise indicar quem é o responsável para servir como ponto de contato para titulares e autoridades.

AGORA COM A LGPD, QUANDO E COMO POSSO TRATAR DADOS PESSOAIS?

Importante relembrar que a LGPD não veio para impedir a coleta, armazenamento ou a utilização dos dados pessoais de indivíduos: a **LGPD apenas estabeleceu diretrizes de como esses dados devem ser mais bem utilizados para proteger as pessoas**. Aliás, em algumas situações, como dito acima, a LGPD torna o tratamento de dados pessoais até mais flexível se comparada com a realidade atual.

A LGPD enumera uma série de **bases legais** que podem ser utilizadas como fundamento para o tratamento de dados pessoais. Nenhuma delas vale mais do que a outra, portanto será sempre necessário buscar a base legal mais adequada para autorizar o uso dos dados pessoais. Em outras palavras, não é necessário obter o consentimento do titular para tudo que será feito com o dado. Dentre as bases legais, é interessante destacar:

Consentimento

Nada mais é do que a autorização do indivíduo para tratar seus dados pessoais. Contudo, o consentimento exige que uma série de cuidados sejam observados para ser considerado válido:

Deixe a pessoa escolher!

O consentimento deve refletir a livre escolha do titular, por meio de uma ação afirmativa. É necessário um ato do titular que permita efetivamente concluir que ele ou ela concorda com a forma que seus dados serão utilizados. Atenção: checkboxes pré-selecionados em sites não são considerados válidos, muito menos o simples rolar do texto de uma política de privacidade.

Seja transparente

O consentimento pressupõe informações claras, objetivas e suficientes para que a pessoa decida, de maneira consciente, se concorda com o tratamento de seus dados pessoais. Não tente esconder o jogo, transparência traz confiança!

Deixe claro para que sua empresa vai usar os dados

O titular de dados deverá autorizar o tratamento de dados para uma finalidade específica e determinada. Autorizações genéricas (como, por exemplo, “iremos utilizar seus dados para melhorar a sua experiência”) não são válidas e, sempre que possível, autorizações específicas para cada finalidade (o que chamamos de consentimento granular) são mais transparentes e claras para o titular, tendo mais chances de serem consideradas válidas.

Registre o consentimento

Assim como você guarda recibos e contratos assinados, vai ser preciso também registrar quando, para que e como o titular consentiu (por exemplo, e-mail, telefone, formulário de cadastro etc.), sob o risco de o consentimento não poder ser utilizado como meio de prova.

Importante lembrar que:

Para tratamento de dados de crianças, ou seja, pessoas de até 12 anos, sempre será necessário o consentimento dos pais e/ou do responsável legal. São apenas duas as hipóteses em que o tratamento dos dados de crianças não precisará deste consentimento: (i) quando a coleta for necessária para contatar os pais ou o responsável legal; ou (ii) quando utilizado para a proteção da criança.

Cumprimento de obrigações legais

Se uma lei ou uma regulamentação exige a utilização dos dados pessoais para algum motivo específico, não é preciso solicitar a autorização do titular de dados. É necessário cumprir o disposto na lei, nem que para isso seja necessário tratar dados pessoais do titular.

EXEMPLOS PRÁTICOS

Se você é um pequeno comerciante, você precisa coletar dados pessoais de seus clientes, como o CPF, para poder emitir a nota fiscal de um produto que será entregue na sua residência; nesse caso, não é necessário pedir a autorização do indivíduo, já que esta é uma obrigação legal para cumprimentos de exigências fiscais. O registro de certas informações de empregados para fazer a folha de pagamento é considerado cumprimento de uma obrigação legal, pois o empregador terá que compartilhá-las com a Receita Federal, por exemplo.

Cumprimento de contratos

Essa é a base legal que permite a utilização dos dados pessoais quando necessários para o cumprimento de obrigações de um contrato do qual o titular seja parte. Neste caso, novamente, não é necessário pedir a autorização do titular.

EXEMPLOS PRÁTICOS

No momento que se vai contratar com um fornecedor, é permitido verificar a situação dos sócios junto à Receita Federal, já que estes são dados necessários para a execução de procedimentos preliminares ao contrato que será celebrado. Aplicativos de entrega em domicílio também precisam de endereço completo para realizar a entrega no local correto, portanto, não precisam pedir autorização do titular para poder compartilhar tais dados com o restaurante escolhido.

Legítimo Interesse

Essa é a base legal que permite à empresa tratar dados pessoais, mesmo sem autorização do titular, para finalidades que visem apoiar ou promover as suas atividades ou de terceiros, o que ficou conhecido como interesses legítimos, desde que respeitados os direitos e liberdades do titular.

EXEMPLOS PRÁTICOS

É muito comum que os estabelecimentos comerciais enviem e-mail em campanhas de marketing digital, com o objetivo de criar e manter o relacionamento com clientes, gerando mais resultados nas vendas e melhorando a retenção de clientes, por exemplo. Para tanto, normalmente as empresas utilizam-se de dados como informações cadastrais e comportamento do cliente no site. Nesse caso, considerando que o indivíduo já possui uma relação pré existente com o estabelecimento comercial, não é necessária a autorização do indivíduo para a coleta desses dados e sua utilização, podendo esses estabelecimentos valerem-se do legítimo interesse. Outro exemplo muito importante é a coleta de dados para fins de prevenção à fraude. Caso fosse necessário pedir autorização para tratar dados para essa finalidade, os fraudadores nunca as concederiam. Neste caso, é um interesse legítimo da empresa tratar os dados, sem autorização prévia do titular, para a finalidade específica de prevenção à fraude.

Atenção aos Dados Sensíveis!

Dados Sensíveis são uma categoria de dados pessoais, que diz respeito a temas mais delicados e podem sujeitar seu titular a práticas discriminatórias. A lei lista todos os tipos de dados que entram nessa classificação: 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

Em razão de seu potencial discriminatório, os Dados Sensíveis merecem uma proteção especial. Sempre quando o tratamento envolver Dados Sensíveis, por exemplo, quando uma campanha de marketing é segmentada em razão da raça, orientação sexual ou opinião política do indivíduo, este tratamento pode vir a ser considerado ilegal.

EXEMPLO PRÁTICO

Uma escola de natação, assim como qualquer academia de ginástica, quando solicita de seus alunos o preenchimento do questionário de prontidão para atividade física, coleta dados de saúde, que são considerados Dados Sensíveis. Da mesma forma, essas empresas, ao fazer o controle de acesso de seus alunos por meio da identificação biométrica, coletam dados biométricos que também estão dentro da categoria de Dados Sensíveis. Tendo em vista a sensibilidade e o potencial discriminatório desses dados, é necessário que as empresas tenham maior atenção a esses dados, estabelecendo um nível de proteção mais robusto.

PRINCÍPIOS GERAIS E MELHORES PRÁTICAS

PRINCÍPIOS GERAIS E MELHORES PRÁTICAS

A LGPD estabelece alguns princípios que se aplicam a todas as atividades de tratamento de dados. Respeitar esses princípios talvez seja a forma mais eficiente de estar adequado às regras de tratamento de dados. Essa prática, inclusive, também é conhecida como *"privacy by design"*, termo bonito que determina que produtos e serviços devem pensar em privacidade e proteção de dados desde a sua concepção. Alguns deles incluem: **finalidade, transparência, adequação e necessidade.** Você pode entender mais sobre esses quatro princípios fazendo algumas perguntas sempre que precisar tratar dados pessoais:

- os dados pessoais serão tratados para uma **finalidade** específica?
- a pessoa foi **informada** de maneira clara e transparente sobre como os dados serão tratados e por quais motivos?
- a forma de utilização do dado é **adequada** ao contexto em que os dados foram coletados, ou seja, é compatível com a finalidade que se informou à pessoa?
- é realmente **necessário** utilizar aqueles dados para atingir os propósitos almejados pela empresa?

EXEMPLOS PRÁTICOS

É cada vez mais comum que bares e casas noturnas peçam um cadastro para o cliente ao entrar no estabelecimento, muitas vezes por motivos legítimos (fazer uma comanda e registrar um número de telefone em caso de perda). Nesses casos, é importante sempre registrar somente os dados necessários, como nome e telefone, por exemplo, e informar o cliente sobre como e para que aqueles dados podem vir a ser utilizados. Se o estabelecimento também quiser coletar outros dados (como e-mail) para enviar promoções ou informações sobre eventuais eventos no local, o cliente deve ser informado e ter a escolha em não fornecer.

Outra prática recorrente é pedir o CPF do titular para abrir uma comanda: será que é realmente necessário para a prestação do serviço o uso do CPF do cliente? Se for, é necessário explicar as razões, que não podem ser, simplesmente, porque o sistema pede tal dado – lembrando que políticas como a Nota Fiscal Paulista (ou suas equivalentes em outros Estados) são voluntárias. Talvez seja possível se valer de outros tipos de dados menos intrusivos.

Isso também vale para lojas: muitas têm exigido um cadastro do cliente para, por exemplo, realizar a troca de um produto, incluindo nome, endereço completo, e-mail... esses dados são realmente necessários para um cliente simplesmente fazer uma troca? Certamente, a resposta é não. Logo, se o interesse da loja é, na verdade, coletar dados para oferecer novas ofertas no futuro, é importante explicar antes para o cliente e dar a ele a opção de entregar ou não esses dados.

Outro exemplo são escolas e creches, em que muitas vezes a direção armazena uma série de informações sobre uma criança, com objetivos legítimos, como permitir que um professor possa fazer uma avaliação melhor sobre o comportamento do aluno. Mas será que todos os dados são realmente necessários? E mais: será que os pais sabem, de forma transparente, como e por que esses dados são tratados?

Outro princípio importante é o da **segurança e prevenção**. Ao tratar dados pessoais, é preciso adotar medidas para evitar toda e qualquer violação de segurança que, de forma acidental ou não, possa levar à perda, adulteração, divulgação ou ao acesso não autorizado de dados pessoais ou uso inadequado destes, bem como medidas de prevenção de danos que possam ocorrer em razão do tratamento. Guardar as informações em locais seguros é essencial. No caso de informações digitais, é importante que os sistemas sejam protegidos, e que somente as pessoas autorizadas possam acessar os dados pessoais.

É importante lembrar que os dados pessoais **nunca podem ser usados para discriminação.** Por exemplo, um comerciante não pode usar dados de orientação sexual para impedir o acesso dessas pessoas a produtos e serviços, atitude grave e que pode, inclusive, ser criminalizada.

Por último, há o princípio da **prestação de contas**, que determina que é necessário ter meios para comprovar a observância e o cumprimento das normas de proteção de dados pessoais. Em outras palavras: não basta estar de acordo, é necessário provar

que está de acordo. Isso pode ser feito, dentre outras formas, por meio das políticas e práticas descritas nesta cartilha.

Existe uma série de dicas para colocar em prática esses e outros princípios previstos na lei. Tais dicas seguem abaixo:

Implemente recursos visuais. Procure utilizar recursos visuais como imagens, tabelas, vídeos e infográficos, que podem facilitar a compreensão do titular sobre quais dados são coletados e tratados e como é feito tal tratamento. Além das informações ficarem mais atrativas e compreensíveis, tais recursos podem proporcionar uma melhor experiência do titular com o produto ou serviço;

Políticas de privacidade facilmente acessíveis. Sempre deixe suas políticas de privacidade facilmente acessíveis ao titular. Tenha em mente que as políticas devem ser disponibilizadas de forma ostensiva e aparente nos sites;

Clareza e objetividade são essenciais. Procure sempre oferecer informações de forma simples e direta, evitando ambiguidades e termos muito técnicos em seus documentos e políticas;

Deixe o titular no controle. Sempre que possível, dê liberdade para o titular concordar ou não com o fornecimento de seus dados pessoais.

Obter o consentimento, quando possível, de forma granular, não coletar dados excessivos (ou dar a opção de não serem coletados) e não deixar checkboxes pré-marcadas em sites podem ser boas ideias;

Permita o gerenciamento de dados. Deixe o titular gerenciar suas escolhas na forma do uso dos seus dados: se ele quiser revogar o consentimento, ou alterar seus dados, ou até mesmo apagá-los, é seu dever ajudá-lo;

Esteja sempre disponível para o titular. Procure criar um canal de atendimento para que os titulares entrem em contato de maneira fácil e simples para tirar dúvidas sobre o tratamento de dados pessoais. Tenha em mente que o exercício dos direitos dos titulares deve ser tão fácil e simples como a forma que os dados pessoais foram obtidos;

Tenha uma política de descarte dos dados. Toda a vida do dado tem que ter começo, meio e fim. Quando não for mais possível justificar a manutenção do dado pessoal, seja porque a finalidade já foi atingida, a base legal não mais se sustenta, ou se tornaram excessivos, é necessário apagá-lo. E apagar é diferente de manter no backup. Até para manter no backup é necessário ter uma base legal. Como boa prática, é interessante estabelecer prazos internos que irão determinar o tempo de vida do dado.

LGPD EM 8 PASSOS

1 Entenda como sua empresa trata dados pessoais

O primeiro passo é entender como sua empresa trata dados pessoais. Comece a refletir sobre **como esses dados são coletados** (você pede um cadastro? registra uma preferência no site?), **que tipos de dados são coletados** e **o que é feito com esses dados**. Origem, tipo e finalidades, simples.

Se você leu esta cartilha até aqui, talvez esse simples exercício já faça você pensar em que base legal seria mais adequada para esse tratamento. Esse exercício também pode ajudar a entender como os princípios que falamos na parte anterior podem ser observados – conferir se os dados são realmente necessários e como o titular possui transparência sobre o tratamento, por exemplo.

2 Não se esqueça do site

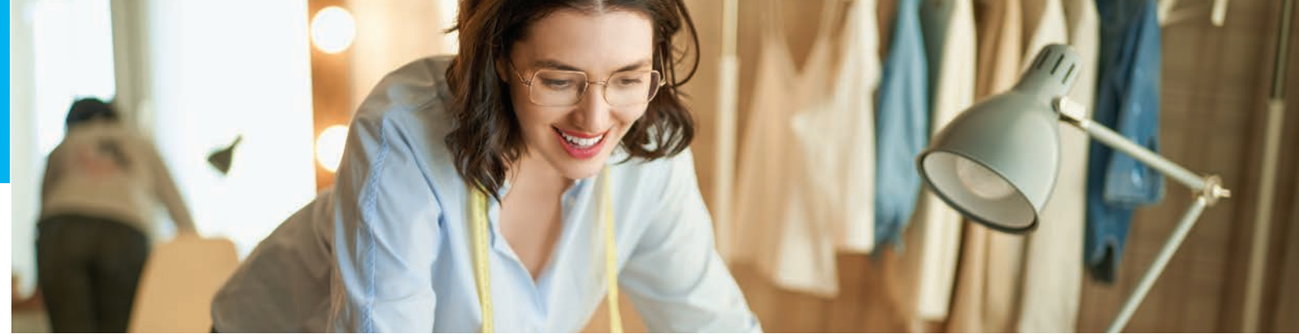
A maior parte das coletas de dados pessoais ocorrem hoje pela internet – na prática, o site será o primeiro "lugar" que as pessoas vão procurar para saber mais sobre como a empresa protege os dados pessoais. Nesses casos, importante se atentar a alguns pontos:

- **Política de Privacidade:** deverá ser apresentada de forma clara, acessível e ostensiva, devendo conter, entre outros aspectos: (a) tipos de dados coletados; (b) finalidades específicas do tratamento; (c) identificação e informações de contato do controlador; (d) informações sobre compartilhamento de dados; e (e) menção expressa aos direitos dos titulares e como exercê-los;
- **Formulários de Cadastro:** deverão ser avaliados e eventualmente ajustados, especialmente para que sejam coletados apenas os dados necessários para os propósitos pretendidos – o preenchimento de dados extras deve ser sempre opcional, e a utilização para finalidades diferentes deve ser, preferencialmente, baseada no consentimento do titular;
- **Aviso de Cookies*:** verifique se o site da sua empresa precisa que você tenha um aviso de que o site utiliza cookies para coletar dados do usuário. Se for o caso, esse aviso deve indicar: (a) a finalidade da coleta; (b) quais tipos de dados são coletados; e (c) um checkbox que permita o "aceite" ou a "recusa" da coleta.

***Cookies são pequenos arquivos, obtidos normalmente na forma de texto, armazenados pelo navegador ao acessar uma página da web. Para realizar suas funções, os cookies podem gravar determinadas informações dos usuários da página web, como nome, localização, senha, IP do usuário, especificações técnicas do dispositivo utilizado etc.**

3 Cuidados com as comunicações de marketing

As atividades de marketing geralmente envolvem tratamento de dados pessoais, especialmente para direcionar mensagens de publicidade e realizar prospecção comercial. É um ponto bastante delicado e, para garantir que as atividades de marketing exercidas estejam de acordo com a LGPD, vale ficar atento às seguintes recomendações:



☑

Garanta que os titulares possam optar por não receber suas comunicações de marketing e que sejam devidamente avisados sobre isso

Respeite os direitos do titular, dando acesso facilitado às informações sobre o tratamento de dados, utilizando-os somente para as finalidades autorizadas e guardando os dados com segurança

Permita que o indivíduo opte por não receber mais a comunicação a qualquer momento. Por exemplo, coloque um botão de "cancelar assinatura" ao final dos seus e-mails marketing

☒

Não adicione automaticamente pessoas à sua lista de e-mails caso não tenha feito um contato inicial ou caso não haja uma relação pré-existente

Não compre mailings e listas de contatos se não tiver base legal legítima e adequada, inclusive questionando os fornecedores sobre sua responsabilidade sobre esse tema

Não use checkboxes pré-marcados quando sua empresa não tem uma relação pré-existente com o indivíduo - isso não constitui consentimento e pode confundir o titular

4 Permita que os titulares exerçam seus direitos

De acordo com a LGPD, os titulares têm vários direitos que sua empresa deve permitir que exerçam. É necessário, portanto, ter processos internos para que tais direitos sejam atendidos. O não atendimento é a forma mais fácil de chamar a atenção da empresa para alguma autoridade, pois o titular poderá fazer uma denúncia. Dentre os direitos elencados na LGPD, o artigo 18 destaca:

Direito	O que é ?
Acesso	Solicitar à empresa informações e cópia sobre os dados que possui sobre o titular e a forma como estes são tratados. Quando isso ocorrer, a solicitação do titular pode ser atendida, por exemplo, por meio da disponibilização de uma cópia dos dados pessoais que a empresa detenha. Isso tem que ser feito em até 15 dias
Retificação	Solicitar a correção dos seus dados pessoais, caso identifique que alguns deles estão incorretos ou desatualizados
Exclusão	Solicitar a exclusão dos seus dados pessoais dos sistemas e base de dados da empresa (a empresa deverá excluir os dados, salvo se houver uma razão para mantê-los, como uma obrigação legal ou um interesse legítimo em que não é permitida uma oposição)
Restringir o Tratamento	Pedir à empresa para suspender o tratamento de seus dados pessoais para determinadas finalidades, ou seja, permitir o uso para algumas finalidades e não para outras. A empresa pode garantir esse direito, por exemplo, por meio da adoção do botão de "cancelar a assinatura" nos e-mails enviados
Objeção ao Tratamento	O titular pode se opor ao tratamento de seus dados, considerando o impacto a seus direitos. Em alguns casos, a empresa poderá demonstrar que tem motivos legítimos para tratar os dados pessoais que se sobrepõem à objeção do titular, como, por exemplo, nos casos em que o tratamento for essencial para registrar o vínculo do titular com a empresa ou para prevenir fraudes
Explicação	Direito de entender os motivos que levaram o titular a ser submetido a um determinado tratamento, inclusive no caso de decisões automatizadas
Portabilidade	Requisitar o fornecimento de seus dados pessoais, em um formato estruturado e interoperável, para outra empresa. Diferente do direito de acesso, neste caso a própria empresa é responsável por transferir os dados para a outra, inclusive se esta for concorrente
Retirar o Consentimento	Trata-se do direito de o titular revogar o seu consentimento

5 Ajude na conscientização dos colaboradores

A realização de treinamentos e ações de conscientização para colaboradores serve para reforçar as políticas e práticas de privacidade e proteção de dados da empresa e é essencial para a criação e sedimentação de uma cultura de privacidade. Algumas dessas ações podem incluir:

- realizar treinamentos internos periódicos, trazendo exemplos e relatos de experiências;
- incentivar a participação em cursos sobre o tema;
- desenvolver campanhas com cartazes e panfletos espalhados na empresa.

Importante também que a empresa crie documentos que possam ajudar na formalização de políticas internas, orientando os funcionários e estabelecendo as diretrizes corporativas. Podem ser documentos simples, como uma política de dados e de segurança da informação, que apresentem as principais obrigações às quais os colaboradores estão sujeitos, de modo a proteger a privacidade e o uso adequado dos dados dos demais colaboradores e dos clientes. Importante também que isso seja bem alinhado com um termo de confidencialidade, que conscientize os colaboradores sobre a importância de manter as informações sobre a empresa – sejam dados pessoais ou não – sempre sob sigilo e em segurança.

6 Avalie seus fornecedores e parceiros

Para estar em conformidade com a LGPD, sua empresa precisa garantir que seus fornecedores e parceiros também estejam em conformidade. Pela lei, o controlador dos dados também pode ser responsabilizado caso seus operadores (ou seja, as pessoas que são contratadas pela empresa para tratar os dados) infrinjam as obrigações previstas na LGPD.

Nesse sentido, é preciso orientar colaboradores a questionarem também os parceiros comerciais da empresa (como agências de publicidade, escritórios de contabilidade etc.) a respeito de como eles fazem para proteger dados pessoais. Fique atento para os seguintes pontos:

- **investigue se a empresa já foi multada ou já sofreu investigações que ainda não foram resolvidas;**
- **verifique a política de privacidade e práticas de seguraça da informação;**
- **questione sobre certificações de segurança da informação que são utilizados;**
- **confira se os contratos possuem obrigações de proteção de dados.**

Ainda, sob esta ótica, se adequar pode vir a ser um diferencial competitivo. Uma vez que as empresas somente poderão contratar outras empresas que também estejam adequadas, aquelas que saírem na frente poderão estar em vantagem enquanto as demais organizações ainda estiverem adequando-se.

7 Tome cuidado com a segurança da informação

Para que sua empresa esteja em conformidade com a LGPD, é necessário adotar medidas para proteger a segurança dos dados pessoais, independentemente do seu tamanho. Algumas dicas podem ser úteis, inclusive na instrução de seus colaboradores:

- Bloqueie os computadores quando estiver fora de seu ambiente de trabalho;
- Utilize senhas em seus computadores e celulares de trabalho, guardando-as em sigilo e alterando-as periodicamente;
- Tenha um controle de quem acessa as informações nos seus sistemas, quando estas são acessadas, definindo responsabilidades e privilégios de acesso. Ou seja, quem pode acessar o que e quando pode acessar;
- Quando estiver trabalhando fora da empresa, fique atento ao seu redor: certifique-se de que o objeto do seu trabalho não esteja visível a outras pessoas e tome cuidado ao falar nomes de clientes, colaboradores e sobre casos específicos;
- Utilize criptografia em todos os computadores, celulares e tablets;
- Descarte documentos confidenciais em papel utilizando um triturador ou rasgando-os em pequenos pedaços;
- Tome cuidado ao abrir e-mails e seus anexos, principalmente de desconhecidos;
- Certifique-se de que documentos físicos que contenham dados pessoais estejam armazenados em locais seguros (gavetas com chaves e cadeados, por exemplo);
- Registre a identificação dos visitantes de entrada e saída do seu estabelecimento, acompanhando-os sempre que forem transitar em áreas reservadas aos colaboradores da empresa;
- Sempre que possível, e viável, utilize e armazene dados anonimizados;
- Somente utilize redes Wi-Fi seguras e confiáveis;
- Limite o acesso aos dados pessoais àqueles que realmente precisem tê-lo;
- Diminua o fluxo de documentos de papel levados para fora de seu estabelecimento

8 Relate eventuais incidentes

Outra obrigação muito importante trazida pela LGPD é relatar eventuais ocorrências de incidentes desegurança da informação. Se houver um incidente envolvendo dados pessoais (e isso significa não só o vazamento de dado, mas todo e qualquer acesso indevido ou não autorizado a um dado pessoal, por exemplo), que possa acarretar risco ou dano relevante aos titulares, a LGPD exige que em alguns casos esse incidente seja comunicado à Autoridade Nacional de Proteção de Dados e, eventualmente, aos titulares

Portanto, se houver qualquer ocorrência envolvendo dados pessoais, não especule se se trata de um incidente; entre em contato com o seu advogado ou o encarregado indicado pela sua empresa para que esta questão seja avaliada e as medidas corretas sejam tomadas.

CONCLUSÃO

Tornar-se compatível com a LGPD não precisa ser uma tarefa assustadora. Para micro e pequenas empresas, a adequação pode levar uma boa quantidade de tempo, e é importante começar logo. Não procure um modelo único para ficar em conformidade com a LGPD: cada organização deve ter seu jeito de fazer as coisas. **Apenas dê o primeiro passo.**

Crie um plano de trabalho para traçar quais são as questões mais relevantes para a empresa, com base no seu próprio cenário. Estabelecidas as prioridades, faça a implementação aos poucos, siga o plano de trabalho ao longo do tempo, até que a empresa esteja em nível avançado de conformidade.

E lembre-se: **este guia é apenas um ponto de partida e não substitui qualquer aconselhamento jurídico**. Possivelmente, você precisará se aprofundar em cada área da sua empresa e ver como você coleta, processa, divulga, armazena e exclui dados. Proteger os dados dos seus clientes, colaboradores e parceiros deve ser mais um processo importante para qualquer empresário. Independentemente de qualquer penalidade, talvez o maior dano para a empresa seja em relação à sua reputação, à sua credibilidade perante o mercado e à perda de confiança. Uma vez perdida a confiança, o custo e o tempo para recuperá-la pode ser muito maior do que qualquer multa.

Por último, fica a dica: proteger dados pessoais também pode ser uma **oportunidade de negócio.** Garantir a privacidade de clientes e colaboradores é fundamental para a construção de uma imagem de confiança. A capacidade de transmitir segurança, antecipar-se a riscos e gerenciar eventuais problemas pode **afetar positivamente a reputação das empresas** - enquanto o resto do mercado estiver correndo para se adaptar, quem se antecipar às mudanças poderá já oferecer seus serviços e produtos de forma mais adequada e eficiente.

RECURSOS ÚTEIS

Além desta cartilha, você pode acessar outros recursos que podem ser úteis para o processo de adequação da sua empresa:

Guia LGPD
Um guia completo produzido pela IdWall, com a LGPD comendada artigo por artigo;
https://guialgpd.com.br/lgpd-comentada/

Publicidade Online e LGPD
Um guia publicado no site do IAB Brasil sobre como adequar suas práticas de marketing digital
https://iabbrasil.com.br/wp-content/uploads/2019/10/MP_guia_LGPD.pdf

Proteção de Dados e Startups
Um guia publicado no site do IAB Brasil sobre como adequar suas práticas de marketing digital
https://www.dinamo.org.br/blog/a-lei-geral-de-protecao-de-dados-lgpd-e-os-pontos-de-atencao-para-as-startups

Espaço Startup
Focado em pequenas empresas, esse blog mantido pelo Baptista Luz Advogados e outros parceiros possui vários artigos sobre LGPD
https://guialgpd.com.br/lgpd-comentada/

Publicações do Data Privacy
O Data Privacy promove cursos sobre proteção de dados e possui vários materiais bacanas em seu site
https://dataprivacy.com.br/publicacoes/

Google

PROTESTE
ESCOLHA DIFERENTE