GUIA LGPD:
Como adequar sua Empresa à Lei Geral de Proteção de Dados

STEPHANNIE MICHAELIS
ADVOCACIA

ÍNDICE

Olá, eu sou a **Stephannie Michaelis**.

Descomplicar o direito, tornando a informação e o conhecimento acessíveis é o meu propósito!

Foi por isso que fundei o escritório **SMichaelis**, e nós trabalhamos sempre visando a inovação. Dispensamos práticas ultrapassadas e estamos sempre em busca de soluções tecnológicas, mais seguras e personalizadas às necessidades de cada mercado e cliente. Nosso compromisso é otimizar processos e trazer resultados alinhados com as melhores práticas de cada setor.

Ético, transparente e seguro. Nosso foco é a construção de relacionamentos confiáveis e duradouros. Para isso, nos adaptamos à realidade de cada mercado, fazendo uma imersão em sua cultura, para aprender com a experiência do cliente e construir, em parceria, a solução ideal às necessidades legais e comerciais, sem perder a essência do negócio.

Através de um trabalho consultivo, auxiliamos empresas a adequarem suas atividades à LGPD, com projetos de adequação, monitoramento e gestão de crise. Possuímos um método exclusivo de organização de documentos e informações, agindo sempre de acordo com as melhores práticas na área de segurança da informação.

Hoje, minha missão é compartilhar com você um pouco sobre a Lei nº13.709/18, a Lei Geral de Proteção de Dados Pessoais (LGPD). Você já deve ter ouvido falar sobre ela, mas talvez ainda não saiba o que realmente deve ser feito para se adequar e cumprir com o novo regulamento. Espero que você termine essa leitura sabendo exatamente o que é a Lei, quais os benefícios que ela traz para as relações trabalhistas e comerciais, e o que você precisa fazer para que sua empresa não sofra nenhuma penalidade.

Então, sem enrolação, vamos juntos nessa!

1.
O que é a LGPD?

A **Lei Geral de Proteção de Dados** (Lei nº13.709/18) foi sancionada em 14 de agosto de 2018 e entrou em vigor em setembro de 2020.

O principal objetivo da LGPD é regulamentar o tratamento de dados pessoais feito pelas empresas, em meio físico ou digital.

Garantir a transparência no uso de dados pessoais, empoderando o titular dos dados para que ele conheça e decida o que pode ou não ser feito com suas informações pessoais. A Lei visa resguardar os direitos fundamentais de liberdade e privacidade dos titulares dos dados, razão pela qual ela **se aplica a toda operação realizada com dados pessoais.**

A partir da vigência da lei, todo o relacionamento entre a empresa e seus clientes, parceiros e colaboradores muda. Agora as empresas precisam, por exemplo, solicitar o consentimento na hora de coletar dados em cadastros e formulários. É preciso ter um motivo válido para querer tais dados e, também, passa a ser necessário informar a finalidade de armazená-los.

A seguir, listei alguns exemplos de motivos que levam uma empresa a coletar e armazenar dados pessoais de seus clientes e funcionários:

- Para envio de ações promocionais ou alertas sobre oportunidades de negócio;
- Com o objetivo de vender produtos ou serviços;
- Para analisar o comportamento e perfil de clientes e, assim, sugerir conteúdo ou produtos específicos;
- Personalizar a comunicação e oferecer manutenção e/ou serviços de pós-venda;
- Realizar pagamentos de salários de seus funcionários.

Com prazo de cumprimento definido, é esperado que todas as organizações atingidas pelo escopo da lei demonstrem conformidade a partir de agosto de 2021. As advertências e multas foram adiadas para agosto de 2021 com a sanção da lei 14010/2020 por causa da pandemia da Covid-19.

Mas, apesar das sanções ainda não estarem valendo, **ninguém deve deixar para se adequar à Lei no último instante**, afinal a LGPD já está em vigor e os direitos dos titulares dos dados pessoais já estão valendo!

Atenção!

- Dados de crianças e adolescentes gozam de proteção diferenciada.
- Para empresas cujos clientes são Pessoas Jurídicas, também há o tratamento de dados pessoais, tendo em vista que a empresa está na cadeia de suprimentos e o simples acesso ou visualização implica no tratamento do dado pessoal.

Para que fique ainda mais simples de entender, vamos esclarecer alguns dos principais conceitos que envolvem a Lei:

Dados:

- **Dados Pessoais:** são os dados que permitem identificar uma pessoa (por exemplo: nome, CPF ou endereço) ou torná-la identificável, através de associações de informações (por exemplo: geolocalização, hábitos de consumo ou perfil socioeconômico);
- **Dados Sensíveis:** são os dados relacionados à intimidade do ser humano, e que, a depender de sua utilização, podem causar discriminação ao seu titular (por exemplo: origem racial ou étnica, convicção religiosa, opinião política, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural);
- **Titular dos Dados Pessoais:** é toda pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- **Tratamento de Dados:** diz respeito a toda operação realizada com dados pessoais, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados.

Agentes de Tratamento e o Encarregado (DPO):

- **Controlador:** aquele a quem compete as decisões referentes ao tratamento de dados pessoais. Ou seja, é quem define os parâmetros e toma as decisões sobre o que deve ser feito;

- **Operador:** aquele que realiza tratamento, conforme instruções do controlador;

- **Encarregado (ou DPO):** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

É fundamental que a empresa nomeie agentes de tratamento e forneça treinamento adequado a eles. Essas pessoas serão as responsáveis pelos dados dentro da empresa.

O Encarregado (DPO) pode ser alguém externo à empresa. Esse cargo é estratégico, pois cria uma ponte de comunicação entre a empresa, os titulares de dados e o Poder Público. Ele precisa conhecer o ciclo de vida dos dados pessoais dentro da empresa, orientando-a sobre a implementação da gestão do Programa de Privacidade e garantindo assim que todas as atividades que envolvam o uso de dados estejam adequadas à LGPD.

Além deles, é importante destacar o papel da **Autoridade Nacional de Proteção de Dados (ANPD)**, que é o órgão do Poder Público responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

2.
Por que a Lei foi criada?

Atualmente, **os dados são considerados um importante ativo das empresas**. Saber usá-los tornou-se um diferencial estratégico dentro do mundo econômico.

Com o imenso volume de informações e a velocidade com que são geradas, as estruturas regulatórias existentes deixaram de ser capazes de lidar com novas demandas do mercado. Surgiu então a necessidade de um novo modelo de gestão e cuidado com os dados.

Motivada pela vigência da GDPR (General Data Protection Regulation), regulamentação europeia que usa os direitos fundamentais de liberdade e de privacidade como base para estabelecer regras quanto à coleta, armazenamento e compartilhamento de dados.

O Brasil criou a LGPD (Lei Geral de Proteção de Dados) para **organizar e formalizar regulações setoriais para proteção de dados já vigentes no país**, obrigando organizações públicas e privadas, nacionais e internacionais, a cumprirem alguns padrões de segurança.

A Lei 13.709/2018 é um marco legal e, com sua aprovação, o Brasil se une ao grupo de mais de 120 países com legislação sobre o tema. A regulamentação traz princípios, direitos e obrigações relacionadas ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas.

Em resumo, **a base da LGPD é o consentimento**. Isso significa que é **necessário solicitar a autorização do titular dos dados**, antes de realizar qualquer tipo de tratamento de seus dados. Como veremos nos próximos capítulos, existem casos de exceção previstos na lei, mas, em geral, precisa haver o consentimento, que deve ser recebido de forma explícita. O usuário pode ainda revogá-lo ou solicitar a remoção de suas informações do banco de dados da empresa a qualquer momento.

Assim, a lei destaca 10 princípios que devem ser observados na hora de tratar dados pessoais. São eles:

1. **Finalidade:** específica e explicitamente informada ao titular;
2. **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular;
3. **Necessidade:** limitação do tratamento ao mínimo que for necessário para a realização de suas finalidades;
4. **Livre Acesso:** acesso livre, fácil e gratuito do titular à forma como seus dados são tratados;
5. **Qualidade dos Dados:** mantendo os dados sempre atualizados e exatos, segundo a real necessidade do tratamento;
6. **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis;
7. **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
8. **Prevenção:** garantia de medidas contra danos ao titular;
9. **Não Discriminação:** impossibilidade de tratamento para fins discriminatórios, ilícitos ou abusivos;
10. **Responsabilização:** do agente, que deve ser capaz de demonstrar a eficácia de seu trabalho e das medidas adotadas;

Como já vimos, **o titular dos dados é a pessoa a quem se referem os dados pessoais que são objeto de tratamento**.

Conhecendo os princípios definidos pela lei, é preciso levar em consideração quais são os direitos que o titular possui em referência a seus dados. Destaquei aqui alguns que devem ser considerados:

1. Confirmação de que existe um tratamento sendo realizado;
2. Acesso aos dados que lhe dizem respeito;
3. Correção de dados que estejam desatualizados ou incorretos;
4. Eliminação de dados desnecessários ou em caso de tratamentos não autorizados;
5. Portabilidade de dados a outro fornecedor de serviço ou produto;
6. Eliminação de dados do banco da empresa;
7. Informação sobre compartilhamento dos seus dados;
8. Informação sobre o não consentimento e quais as decorrências dessa decisão;
9. Revogação do consentimento, nos termos da lei;
10. Reclamação contra o controlador de dados, nos termos da lei.

3.

Como a LGPD pode impactar sua empresa?

A LGPD tem grande impacto nas relações internas e externas da empresa. Pra começo de conversa, vamos falar sobre os impactos da lei dentro da própria empresa.

Todos os departamentos que coletem ou utilizem dados, como o Departamento Jurídico e o de Marketing, devem se adequar.

Destaco aqui a área de gestão de pessoas (Recursos Humanos e/ou Departamento Pessoal), que precisa se adequar às recomendações previstas em lei, visando um melhor uso e manutenção do banco de dados com as informações de seus colaboradores e candidatos.

Nos próximos tópicos vamos explorar alguns dos principais impactos da legislação no funcionamento da empresa. Vamos nessa?

3.1.

Repensando as relações de trabalho

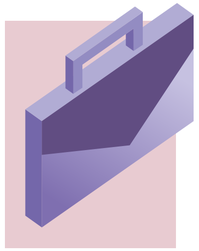
O RH passa a precisar solicitar o consentimento do uso dos dados de todo colaborador ou candidato, onde conste a finalidade da utilização dos dados e o período de armazenamento.

As modificações começam logo na porta de entrada: para manter um banco de currículos atualizado, os recrutadores precisam manter os candidatos informados sobre os processos seletivos e o uso e armazenamento das informações. **A lei exige que só podem ser coletadas informações relevantes e necessárias para as atividades da empresa**, tome cuidado com “curiosidades”, pois o processo de recrutamento e seleção deve se ater ao que for realmente necessário.

Além disso, caso queira manter um banco de currículos, é preciso ter autorização expressa de cada candidato e, caso contrário, um procedimento seguro e efetivo que garanta o descarte das informações.

Já **com os colaboradores ativos e inativos, os cuidados são diversos**. É preciso armazenar de forma segura e usar apenas para os fins pré estabelecidos os dados pessoais como: endereço, dados bancários, informações de saúde, contatos emergenciais, entre outros.

É preciso ter atenção às informações compartilhadas com outros setores, ou com empresas parceiras, como a seguradora do plano de saúde ou a contabilidade responsável pelo fechamento da folha de pagamento. Lembre-se, os dados são de responsabilidade da sua empresa, que os coletou e armazenou, e que **toda coleta e tratamento de dados depende de uma finalidade**.



Assim, **a LGPD requer uma revisão nos contratos de trabalho**, uma vez que solicita o consentimento expresso dos colaboradores acerca de seus dados pessoais. Quando for criá-lo, avalie a real necessidade de pedir dados como: estado civil, gênero, orientação sexual, política ou religiosa. Enfim, qualquer tipo de informação que não esteja diretamente ligada com o propósito da contratação ou com a manutenção do vínculo empregatício.

Se atente também aos dados sensíveis como atestados médicos e informações da utilização do plano de saúde. Dados como estes, requerem respeito e sigilo e é sempre responsabilidade da empresa garantir isso.

Com isso, fica clara a necessidade não apenas de adquirir softwares seguros para armazenar as informações, mas também de **treinar e capacitar os colaboradores, especialmente a equipe de RH** que, além de ser quem lida diretamente com os dados, é a responsável pela manutenção e propagação da cultura empresarial. É fundamental que cada um se conscientize sobre a importância da lei, já que garantir a segurança da informação é responsabilidade de todos.

A empresa deve ter um encarregado para garantir a aplicação e funcionamento da legislação nos procedimentos internos. Além do alinhamento do RH com esse encarregado, é preciso estabelecer uma parceria com as áreas jurídica e de tecnologia da empresa.

Estar dentro das normas da lei e seguir boas práticas no tratamento de dados elimina irregularidades que poderiam gerar ações trabalhistas no futuro.

Na prática!

Um caso de vazamento de dados de um atestado médico que indicava que o colaborador era portador de HIV.

A impressora utilizada pelo RH era compartilhada com o restante da empresa, algo aparentemente simples e cotidiano, não é mesmo? Acontece que o setor lida com informações sigilosas da equipe de colaboradores. Assim que o atestado foi impresso, foi visto por um dos colegas de trabalho do colaborador em questão. Essa informação foi vazada, gerando impacto em suas interações sociais dentro da empresa, ele foi vítima de preconceitos em decorrência de uma informação pessoal sobre sua saúde, um dado sensível que estava sob confiança da empresa.

Como resolver isso? Realizando um mapeamento de dados em cada setor da empresa, um Programa de Conformidade à LGPD poderia ter mitigado tal risco, evitando a ocorrência de uma situação constrangedora que comprometeu o ambiente de trabalho e o desempenho do colaborador.

3.2.

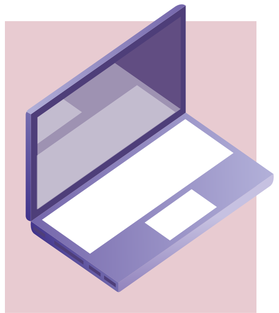
O caso do Teletrabalho ou Home Office

A pandemia da Covid-19 transformou nossas vidas em muitos níveis, mudamos hábitos de consumo e nossa relação com o trabalho. Colaboradores de diversos setores foram enviados para suas casas por medidas de segurança e passaram a **trabalhar em um modelo de Home Office, ou trabalho remoto.**

As empresas precisaram se adaptar às pressas para aderir a essa transformação que só foi possível devido às tecnologias que temos à disposição hoje, como ferramentas de reunião online ou VPN's usadas para garantir a segurança dos dados.

Com o modelo de trabalho remoto, surge a necessidade de registrar as comunicações entre o RH e os colaboradores ou candidatos, coletar e armazenar autorizações dos colaboradores sobre o tratamento de seus dados pessoais, além de estabelecer políticas de segurança da informação para as equipes que estão trabalhando de suas casas, a fim de evitar perdas ou vazamentos de dados.

Também é preciso **rever as políticas de uso dos dados** pelos colaboradores, explicitando o que pode ou não ser feito, dado que o modelo de trabalho é diferente do realizado usualmente nos escritórios. Deve-se realizar treinamentos com cada equipe, para conscientizar e preparar para melhores práticas durante esse período.



3.3.
Relações Comerciais e Consumo

Os impactos externos à empresa se darão principalmente em suas relações comerciais e de consumo.

Com o aumento na velocidade da captação e do processamento da informação, algumas grandes empresas começaram a mascarar os reais motivos para coletarem os dados de seus clientes e, com maior conhecimento de mercado, passaram a influenciar nas escolhas feitas pelas pessoas.

A **política de transparência no uso de dados** surge para proteger os usuários, empoderando o titular dos dados. Isso modifica não apenas a maneira como os clientes e parceiros se relacionam com a empresa, mas também quais suas expectativas em relação a ela.

Hoje, sabemos que as empresas analisam histórico de compras e hábitos de consumo para traçar perfis, oferecer ofertas personalizadas e condições financeiras e de crédito. Porém, tais tratamentos devem ser feitos com o consentimento do cliente ou usuário. Ou seja, ele deve estar ciente e ter a opção de autorizar ou não tais procedimentos, podendo, a qualquer momento, revogar o consentimento.

Agora, o consumidor está protegido e ciente de seus direitos, por isso, mais do que a aquisição de um software, **a lei vem para provocar uma mudança estrutural nas empresas**, exigindo modificações na cultura e comportamento de cada colaborador, já que todos são responsáveis por exercer práticas éticas e seguras com a informação confiada à empresa.

3.4.
Segredo Comercial e Industrial

Segredo Industrial é o nome dado a uma proteção que visa g**arantir a confidencialidade de informações que possam proporcionar alguma vantagem competitiva para a empresa.**

Apesar de não existir um padrão pré-definido, existem técnicas utilizadas pelas empresas para garantir o sigilo das informações. O que costuma ser feito é um contrato de confidencialidade dentro da própria empresa, entre os colaboradores que terão acesso às informações em questão. Normalmente, poucas pessoas têm acesso a essas informações privilegiadas, como forma de minimizar riscos de seu vazamento.

Também é possível contratar uma empresa especializada em segurança da informação, que garantirá a proteção de informações no meio digital. Além disso, pode ser feita ainda uma análise de risco para avaliar a necessidade de oferecer garantias, seguros e técnicas de compliance.

O direito ao segredo industrial está preservado pela LGPD como um instrumento de desenvolvimento tecnológico, que assegura às empresas seu direito de realizar pesquisas e desenvolver um material, produto ou ferramenta inovador.

Utilizando ferramentas de proteção, as empresas **evitam casos de vazamento ou sequestro de dados**, que podem ter consequências desastrosas, como veremos a seguir.

3.5.

Vazamento de Dados e Incidentes de Segurança

Um vazamento ou violação de dados é um incidente de segurança que expõe informações sensíveis e confidenciais a uma pessoa não autorizada. Informações estas que podem ser visualizadas, copiadas, transmitidas, roubadas ou deletadas sem acesso autorizado.

Vazamento de dados são um sinal de alerta para as empresas e para os consumidores, portanto, tome cuidado: é sua reputação que está em risco!

Um vazamento ocorre quando *hackers* conseguem acessar o banco de dados da empresa, acessando informações como senhas, e-mails, CPFs, números de cartão de crédito ou informações bancárias, dados de saúde, entre outros, de seus clientes.

Esses dados, por lei, devem ser mantidos em sigilo. A LGPD exige que a empresa informe os clientes em casos de vazamento e procurem remediar os eventuais prejuízos, já que é ela a responsável pela segurança da informação.

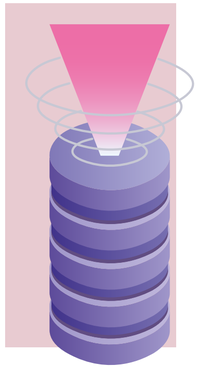
Apesar de associarmos incidentes de vazamentos a ações criminosas de *hackers*, existem diversas situações que propiciam a quebra de sigilo e o vazamento de informações sensíveis, tais como:

- **Um acidente entre colaboradores:** quando um colega vê o material de outro ou lê um arquivo sem permissão;
- **Um colaborador mal-intencionado:** quando um colaborador compartilha intencionalmente uma informação que não lhe diz respeito, com a intenção de prejudicar a empresa ou um colega de trabalho;
- **Dispositivo emprestado, perdido ou roubado:** quando um *notebook* ou celular que contenham informações sensíveis da empresa cai na mão de terceiros.

A adequação à lei, visa não apenas remediar, mas prevenir esse tipo de incidente. Além de evitar prejuízos financeiros, como indenização aos titulares ou penalidades e multas diretamente aplicadas pelo poder público, estar de acordo com a lei gera valor à empresa, pois demonstra sua genuína preocupação com seus clientes, aumentando a confiança na marca e melhorando o relacionamento entre as partes.

Segundo pesquisas realizadas pela IBM Security e pelo Instituto Ponemon, somente no Brasil, em 2020, houve um crescimento de 10,5% desse tipo de ataque a redes empresariais. O roubo de dados tem se tornado cada vez mais comum e uma violação pode custar até 5,8 milhões de reais para a empresa que for alvo de ataques.

Além dos prejuízos financeiros diretos, empresas que sofreram vazamentos relatam danos à reputação da marca e da credibilidade no mercado, resultando em queda nos lucros e dificuldades para recuperar a imagem da empresa.



Assim, **é imprescindível que as empresas adotem um programa de gestão de segurança da informação**, como veremos nos próximos capítulos.

3.6.

Penalidades

A lei prevê penalidades severas para empresas que não se adequarem. A omissão na hora de adotar medidas preventivas de riscos de incidentes com dados pessoais poderá ser punida de forma a servir de exemplo a outras empresas.

As possíveis penalidades são:

- Advertência e prazo para adoção de medidas corretivas;
- Publicização da infração após confirmada sua ocorrência;
- Multa simples, de até 2% do faturamento bruto, limitado a 50 milhões de reais por infração e multa diária;
- Bloqueio dos dados pessoais até a regularização;
- Eliminação dos dados pessoais referentes à infração;
- Suspensão do exercício da atividade de tratamento de dados pessoais por 6 meses, prorrogável por igual período;
- Suspensão parcial do banco de dados por 6 meses, prorrogáveis por igual período, até a regularização da atividade;
- Proibição parcial ou total do exercício da atividade de tratamento de dados.

Para a aplicação das penalidades, serão levados em conta fatores como a gravidade e a natureza das infrações, boa-fé do infrator e sua condição econômica, reincidência e grau de cooperação do infrator. Além, é claro, da existência de política de boas práticas e governança. Por isso, apesar de não existir nenhum tipo de blindagem que elimine completamente os riscos, **é fundamental demonstrar preocupação e cuidado com o tratamento de dados.**

O que fazer para se preparar?

4.

Bases Legais

A LGPD estabelece dez bases legais, ou hipóteses, nas quais é permitido realizar o tratamento de dados pessoais. Veja a lista a seguir:

1. **Consentimento do titular:** o titular dos dados deve concordar com o tratamento de seus dados para uma finalidade determinada;

2. **Cumprimento de obrigação legal pelo controlador:** mesmo sem o consentimento do titular, o controlador deve armazenar, processar e transmitir dados pessoais, por força de lei ou de algum regulamento normativo do interesse público;

3. **Pela administração pública, para a execução de suas finalidades:** quando tratamento de dados pessoais, pela administração pública, se justifica, para possibilitar a execução de políticas promovidas pelo setor público;

4. **Para a realização de estudos por órgão de pesquisa:** garantida, sempre que possível, a anonimização dos dados pessoais;

5. **Para execução de contrato ou de procedimentos preliminares a este, quando solicitado pelo titular:** quando o tratamento de dados pessoais é indispensável para o cumprimento dos próprios objetivos do próprio contrato;

6. **Exercício regular de direitos em processo judicial, administrativo ou arbitral:** quando o tratamento de dados pessoais se legitima para fins de operacionalização e execução de processos;

7. **Proteção da vida do titular ou de terceiros:** quando o titular ou terceiros estiverem expostos a riscos, perigo de morte ou suscetíveis a danos físicos graves;

8. **Tutela da saúde, exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária:** ou seja, cuidados a serem empregados visando proteger, preservar ou restabelecer a saúde;

9. **Atendimento aos interesses legítimos do controlador ou de terceiros:** os dados pessoais podem ser tratados, desde que não se contraponham aos direitos e liberdades fundamentais do titular e sejam somente os dados, estritamente, necessários e relacionados com as atividades praticadas pelo controlador dos dados;

10. **Proteção do crédito:** por fim, dispensa o consentimento do titular de dados pessoais em situações em que a coleta é realizada para pesquisa e análise de riscos relacionados à concessão de crédito.

Toda vez que for necessário fornecer uma justificativa de uso de um determinado dado pessoal dentro da empresa, essa justificativa deverá se enquadrar em uma dessas dez situações. Caso contrário, o tratamento dos dados será considerado indevido ou ilegal.

4.1
Framework de Segurança de Dados

Pra facilitar, criei um Framework que ajuda a atender às necessidades previstas na LGPD:

1. **Gestão e Governança:** os processos de governança devem possibilitar que todos aqueles que têm acesso aos dados contem com um conjunto definido de princípios, políticas e procedimentos que estabeleçam claramente o modo como os dados pessoais podem ser processados e tratados;

2. **Coleta, Armazenamento e Uso dos Dados:** gerenciar os dados pessoais de acordo com um ciclo de vida, relacionado com a classificação do dado, desde a coleta inicial até o arquivamento e eliminação do banco de dados;

3. **Consentimento e Transparência:** a empresa precisa informar ao usuário a finalidade da coleta de dados e este deve concordar com ela. Para isso, é essencial que seja transparente quanto às suas intenções e procedimentos. Somente assim conseguirá estabelecer uma relação de confiança com seus clientes e parceiros;

4. **Exercícios de Direitos do Titular:** a empresa precisa ter procedimentos estabelecidos que visem garantir aos titulares que suas requisições serão atendidas;

5. **Compartilhamento:** ao compartilhar dados pessoais com terceiros, a empresa deve garantir que os mesmos sejam autorizados e validados previamente, evitando o uso indevido destes dados;

6. **Segurança:** obviamente, os dados precisam ser tratados de forma segura. Para isso, a empresa precisa ter um programa de segurança da informação que garanta a aplicação das medidas de segurança necessárias, alinhadas aos riscos identificados;

7. **Gerenciar Incidentes:** Além das boas práticas no armazenamento e tratamento de dados, a empresa deve estar pronta para manejar situações de crise e reparar possíveis danos causados ao titular dos dados em caso de incidentes;

8. **Avaliação de Riscos:** os possíveis riscos devem ser identificados, avaliados e tratados de forma adequada. O processo de gerenciamento de riscos visa a melhoria das normas e a mitigação de possíveis danos;

9. **Monitoramento:** é necessário conferir se todas as regras, políticas, processos, procedimentos estão sendo aplicados na prática, no dia a dia das operações da empresa;

10. **Treinamento:** é preciso criar uma cultura empresarial forte, onde todos os colaboradores se percebam como agentes de privacidade e ajudem a manter a segurança da informação.

4.2

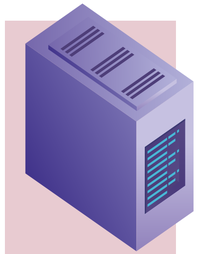
Governança de Dados

Governança, nada mais é do que administrar. Quando usamos essa palavra, estamos nos referindo a um **sistema de gestão e monitoramento** que envolve todos os níveis da empresa. Nele, todos os princípios e valores básicos da empresa são convertidos em recomendações objetivas e expressas, de modo a alinhar seus interesses e otimizar o seu valor econômico de longo prazo.

Tendo a LGPD e a Privacidade como foco, **um programa de governança deve garantir que a empresa esteja adequada à legislação e de acordo com os princípios e valores de sua cultura, ou seja, com sua razão de ser**.

No Programa de Governança em Privacidade devem constar o regime de funcionamento da empresa, seus procedimentos, as reclamações dos titulares, as normas de segurança e os padrões técnicos, as obrigações para os envolvidos no tratamento, as ações educativas e os mecanismos internos de análise e diminuição de riscos.

As regras de privacidade de uma empresa devem ser criadas em parceria com a direção e as lideranças, para que estejam de acordo com o propósito da empresa e para que haja uma verdadeira transformação cultural, uma vez que as regras estabelecidas devem ser seguidas por todos os colaboradores no dia a dia de suas atividades.



5.

Por onde começar?

A LGPD requer que as empresas atualizem seus procedimentos de tratamento de dados, garantindo transparência e segurança no uso da informação, respeitando sempre o titular dos dados.

Nesse ponto da leitura, você deve estar se perguntando *“Por onde eu começo?”*. Calma, para tudo há uma solução!

Eu sei que parece muita coisa, mas, como qualquer projeto, o segredo é traçar um plano de ação estratégico e começar. Para te ajudar, preparei um guia com **8 Passos para começar a se adequar à LGPD**:

1. **Conhecer a Lei:** Parabéns! Esse passo você já está realizando com a leitura desse e-Book que eu preparei pra você. Conhecer a lei e saber como ela impacta o seu mercado é o primeiro passo em direção a uma verdadeira transformação;

2. **Analisar as bases legais para o tratamento de dados:** leia o material novamente, vá além e estude. Você precisa identificar em qual caso sua empresa se enquadra, que tipo de dado é coletado e com qual finalidade. Os processos devem estar claros para você e sua equipe;

3. **Obter os consentimentos necessários:** se preciso, reformule contratos de trabalho com seus colaboradores ou contratos de prestação de serviços com os clientes, lembre-se que é necessário informar ao titular dos dados tudo o que será feito com suas informações, ele deve estar ciente e autorizar previamente o uso de tais dados;

4. **Revisar a Política de Privacidade e os contratos de sua empresa:** junto ao setor jurídico ou consultoria especializada, revise detalhadamente todos os termos de sua política de privacidade;

5. **Nomeie o encarregado de proteção de dados (DPO):** defina quem será o responsável por garantir o monitoramento dos processos e cumprimento da legislação. Lembre-se da importância e responsabilidade deste cargo;

6. **Identifique possíveis riscos no tratamento de dados:** contrate profissionais de segurança da informação que façam um diagnóstico de sua rede e digam quais as reais necessidades da empresa para estar apto a cumprir com a lei;

7. **Implemente as medidas necessárias para garantir a segurança dos dados:** faça as modificações necessárias em termos de maquinário, softwares e treinamentos de equipe;

8. **Implemente políticas para lidar com eventuais incidentes:** esteja pronto para lidar com qualquer anormalidade de procedimentos. A capacidade de gerenciar uma crise diz muito sobre uma empresa.

Se você chegou até aqui, já deve ter percebido que não existe outra alternativa: **é preciso se adequar à LGPD**.

As boas práticas estabelecidas pela legislação não são apenas uma questão de evitar sanções e punições. Estar adequado é se mostrar atualizado, digital e seguro. É consolidar sua marca e passar segurança ao público.

É fundamental que a mudança comece pelo olhar da gestão e se espalhe dentro de cada área da empresa, provocando mudanças comportamentais na atuação de cada membro. Para não esquecer nenhum ponto e minimizar riscos, é aconselhável a contratação de uma consultoria especializada que ajudará no diagnóstico, implementação de práticas e treinamentos de colaboradores. Um profissional também poderá reelaborar os contratos de trabalho, de serviços, os termos de consentimento e a Política de Privacidade vigentes.

Apesar de não existir nenhuma forma de eliminar completamente os riscos, a adequação minimiza a exposição da empresa e garante uma melhoria considerável de seu posicionamento no mercado. Ter assessoria jurídica é a melhor forma de diminuir os riscos de problemas e danos como indenizações a titulares de dados ou ações trabalhistas.

Conte conosco nessa jornada!

(11) 97484-6813

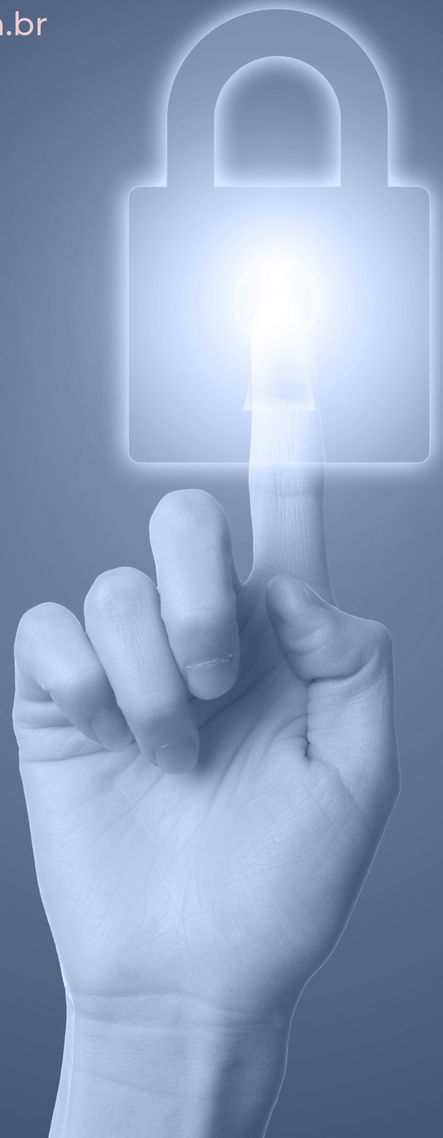
stephannie@smichaelis.com.br

www.smichaelis.com.br

/smichaelisadv

/smichaelisadv

Clique nos ícones ou nos links para ser direcionado



STEPHANNIE
MICHAELIS
ADVOCACIA