COMO PREPARAR AS EMPRESAS **PARA LGPD**

CNC · Fecomércio MG · Sesc · Senac · Sindicatos Empresariais

Sistema Comércio

Mais segurança para empresários e consumidores

Nadim Donato Filho
Presidente do Sistema Fecomércio MG, Sesc e Senac em Minas

A boa compra é a boa venda e vice-versa, esta é uma verdade que não muda com o passar do tempo. Contudo, o relacionamento comercial mudou substancialmente nos últimos tempos. Como sabemos, o contato entre comerciante e cliente se torna cada vez mais rápido e, em grande parte das vezes, é intermediado por uma ferramenta tecnológica.

Como a relação de confiança continua sendo fundamental para as trocas comerciais, a Lei Geral de Proteção de Dados (LGPD) de 2018 veio para assegurar proteção e privacidade aos dados pessoais. Ao conhecer e utilizar a Lei Federal 13.709 de 2018, que se encontra em vigor, o empresário do comércio trabalha com a segurança necessária para estabelecer um relacionamento de confiança com seu cliente.

É para assegurar o acesso e o conhecimento à LGPD aos empresários do comércio que a Federação do Comércio de Bens Serviços e Turismo de Minas Gerais - Fecomércio MG – publica a presente cartilha. De maneira bem simples, o texto traz os principais pontos da Lei, desde os cuidados necessários à sua aplicação até os procedimentos para a correta manutenção dos dados pessoais da clientela. A LGPD de fato é complexa e impõe penalidades em caso de violação, mas é possível trabalhar com segurança desde que os procedimentos exigidos sejam atendidos.

Desejamos que esta cartilha venha a contribuir com sua empresa com esclarecimentos que permitam a adoção das melhores práticas no cuidado com os dados pessoais dos clientes. A Fecomércio MG acredita que este é o caminho mais seguro para gerar a tranquilidade necessária ao bom atendimento do cliente, seja ele feito presencialmente ou no ambiente virtual.

Boa leitura!

SUMÁRIO

1. Apresentação

No âmbito jurídico nacional, a Lei Geral de Proteção de Dados (LGPD) vigora em um cenário de constante evolução tecnológica e crescente volume de informações compartilhadas no mundo digital. Em meio a tantos desafios, a Lei Federal nº 13.709/2018 – como foi sancionada – visa facilitar o controle e a segurança sobre os dados pessoais, ao exigir o consentimento explícito para a coleta, a manutenção e o uso desse material.

Para facilitar o cumprimento da lei, evitar penalidades e garantir os benefícios de sua adaptação às empresas, a Fecomércio MG elaborou esta cartilha. O material aborda os principais pontos da LGPD, como a sua aplicação, o tratamento de dados, as boas práticas e os direitos do titular dos dados pessoais.

Embora sirva de guia para os negócios, especialmente aqueles enquadrados no comércio de bens, serviços e turismo, esta cartilha deve ser interpretada de acordo com a realidade de cada estabelecimento. Por isso, estude as mudanças necessárias e adapte os processos conforme as rotinas da sua empresa.

2. Introdução

Acessar as redes sociais, baixar um *e-book*, participar de promoções ou realizar uma compra on-line. Essas ações, comuns à rotina de milhões de cidadãos, são geralmente habilitadas a partir do cadastro de dados pessoais. Na prática, ao dar aceite em um termo e/ou fornecer informações desse teor, as pessoas nem sempre eram comunicadas sobre o armazenamento, sigilo ou uso desses dados.

Neste contexto, começou a vigorar, no dia 18 de setembro de 2020, a Lei Geral de Proteção de Dados (LGPD). Regulamentada como a Lei nº 13.709/2018, esse marco legal visa garantir direitos individuais, assegurar transparência por parte de empresas públicas e privadas, além de conferir mais previsibilidade jurídica. O tratamento de dados pessoais, instituído pela nova legislação, também contribui para reduzir custos operacionais das organizações e elevar a segurança do titular desses dados.

3. Aplicação da LGPD

3.1 A quem se aplica

A Lei Geral de Proteção de Dados (LGPD) se aplica a qualquer operação de tratamento realizada por pessoa natural (pessoa física) ou por pessoa jurídica de direito público ou privado. Ela abrange todos os setores da economia e da administração pública que realizam tratamento de dados pessoais no meio físico e/ou digital, seja no país de sua sede ou onde estejam localizados os dados pessoais.

Desta forma, é necessário que as empresas fiquem atentas à lei, nos casos em que haja: (I) a coleta de dados pessoais para ações de marketing em promoções, site ou anúncios, diante da análise do comportamento do público para criação e envio de conteúdo específico; (II) a manutenção de dados pessoais de colaboradores ou a terceirização da coleta, armazenamento e/ou tratamento de dados pessoais.

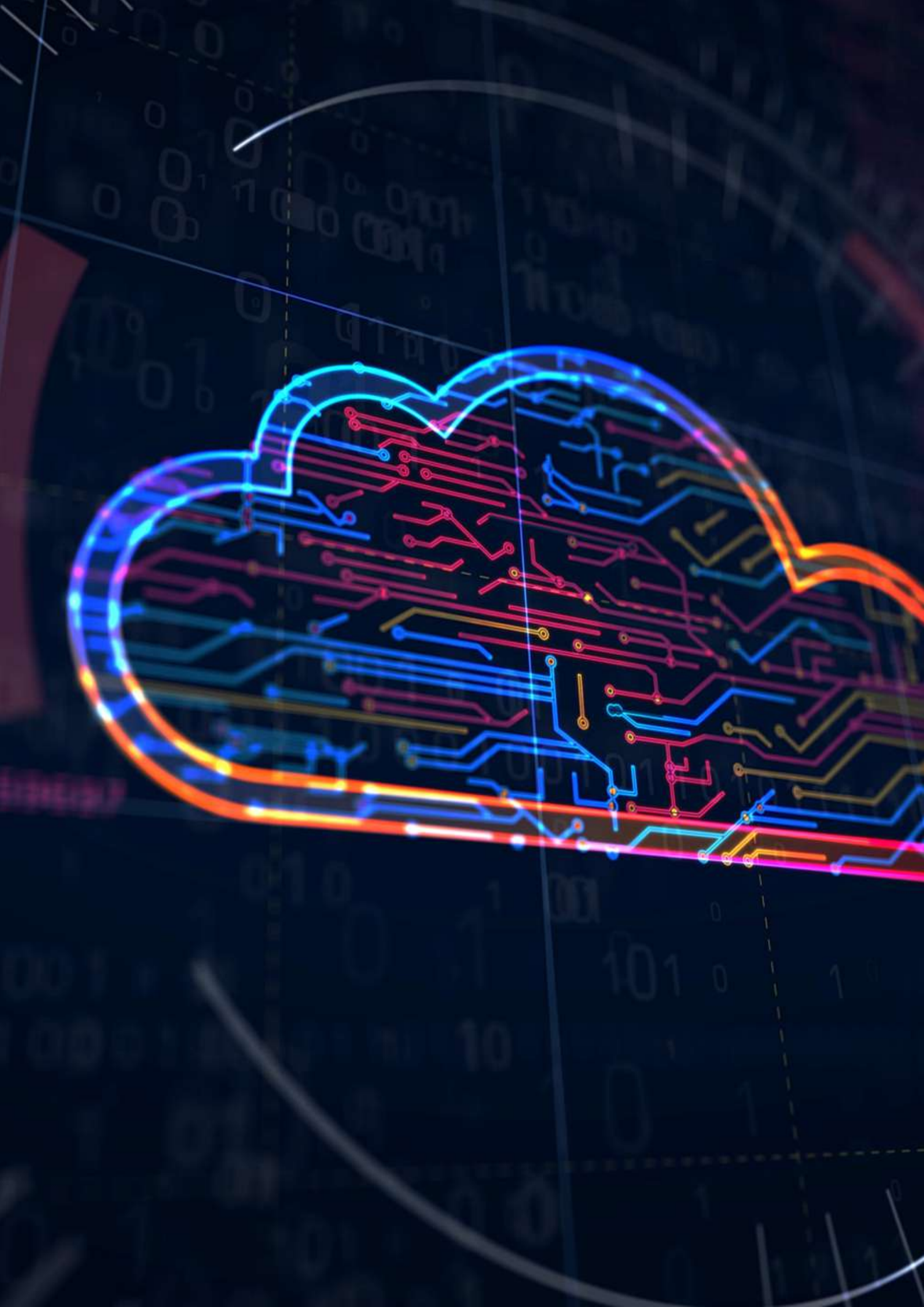
Assim como o regulamento europeu (GDPR), a LGPD obriga as organizações públicas e privadas, sejam brasileiras ou multinacionais, a cumprirem padrões de segurança. O objetivo é prevenir crimes cibernéticos, bem como o vazamento ilegal de dados pessoais.

3.2. Abrangência extraterritorial

Todas as empresas com atuação no Brasil devem seguir a Lei Geral de Proteção de Dados. No entanto, também estão sujeitas às regras os negócios em que: (I) a operação de tratamento seja realizada no território nacional; (II) a atividade de tratamento vise a oferta ou o fornecimento de bens ou serviços, bem como o tratamento de dados pessoais de indivíduos localizados no Brasil; ou (III) os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

3.3. Exceções

A lei não se aplica ao tratamento de dados pessoais: (I) realizado por pessoa natural para fins exclusivamente particulares e não econômicos; (II) para fins exclusivamente jornalísticos, artísticos e acadêmicos; (III) para fins exclusivos de segurança pública e de Estado, defesa nacional ou atividades de investigação e repressão de infrações penais; ou (IV) provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que essa nação proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.



4. Principais pontos da LGPD

4.1. Objetivo

As normas dispostas pela Lei Geral de Proteção de Dados visam a proteção dos direitos fundamentais de liberdade e privacidade, além do livre desenvolvimento da personalidade da pessoa natural. Considerada lei de interesse nacional, a LGPD deve ser observada pela União, Estados, Distrito Federal e Municípios.

4.2. Fundamentos

A disciplina da proteção de dados pessoais tem como alicerces: (I) o respeito à privacidade; (II) a autodeterminação informativa; (III) a liberdade de expressão, de informação, de comunicação e de opinião; (IV) a inviolabilidade da intimidade, da honra e da imagem; (V) o desenvolvimento econômico e tecnológico e a inovação; (VI) a livre iniciativa, a livre concorrência e a defesa do consumidor; e (VII) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

4.3. Categorias

Os dados relativos às pessoas naturais (também denominadas pessoas físicas) podem ser divididos em três segmentos:

- **Dados pessoais:** são relacionados à pessoa natural, sendo identificados ou identificáveis, como: nome, endereço, documentos (RG, CPF, título de eleitor), foto, localização, e-mail e características pessoais.

- **Dados pessoais sensíveis:** são aqueles relacionados à origem racial ou étnica; à convicção religiosa; à opinião política; à filiação a sindicato ou organização de caráter religioso, filosófico ou político; à saúde ou à vida sexual e à genética ou biometria, quando vinculados a uma pessoa natural.

- **Dados anonimizados:** são dados que não possibilitam a identificação de seu titular. Neste caso, a LPGD não é aplicada, salvo quando a reversão do processo seja possível, por meios técnicos razoáveis.

Atenção! Menores de idade possuem proteção diferenciada

A Lei Geral de Proteção de Dados (LGPD) também protege crianças e adolescentes na internet. As normas se baseiam nos mesmos princípios gerais: por exemplo, se o menor de idade fica on-line para jogar, não será permitido pedi-lo que forneça acesso à lista de contatos, à localização, à câmera e ao microfone. Porém, o sigilo de alguns dados dos pais poderá ser quebrado para alertá-los sobre contatos inconvenientes na *web*.

Desta forma, é imprescindível obter o consentimento de um dos responsáveis pelo menor de idade e solicitar apenas os dados pessoais estritamente necessários para a atividade em questão; sendo ainda vetado o repasse desses dados a terceiros. Sem o consentimento, pode-se coletar apenas os dados para contato urgente com os responsáveis, garantindo a proteção da criança e do adolescente.

4.4. Princípios

A LGPD estabelece os seguintes princípios a serem considerados, além da prática da boa-fé, para as atividades de tratamento de dados pessoais:

- **Finalidade:** ações firmadas em propósitos legítimos, específicos, explícitos e informados ao titular dos dados.

- **Adequação:** compatibilidade do tratamento com as finalidades informadas.

- **Necessidade:** limitação do tratamento ao mínimo necessário para suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos.

- **Livre acesso:** consulta facilitada e gratuita, pelos titulares, sobre a forma e a duração do tratamento, além da integralidade dos dados pessoais.

- **Qualidade dos dados:** garantia de exatidão, clareza, relevância e atualização dos dados.

- **Transparência:** informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial, caso existentes.

- **Segurança:** utilização de medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

- **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

- **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

- **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.

4.5. Fiscalização

A fiscalização, regulamentação e aplicação das sanções da LGPD ficará a cargo da Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública direta, ligado à Presidência da República.

4.6. Penalidades

Os agentes de tratamento de dados ficam sujeitos às sanções administrativas aplicáveis pela autoridade nacional a partir do dia 1º de agosto de 2021.

- Advertência, com indicação de prazo para adoção de medidas corretivas.

- Multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no seu último exercício no Brasil, excluídos os tributos e limitada a R$ 50 milhões por infração.

- Multa diária, observado o limite a que se refere o inciso II.

- Tornar pública a infração após devidamente apurada e confirmada a sua ocorrência.

- Bloqueio dos dados a que se refere a infração até a sua regularização.

- Eliminação dos dados pessoais a que se refere a infração.

- Suspensão parcial do banco de dados a que se refere a infração por até seis meses, prorrogável por igual período, até a sua regularização pelo controlador.

- Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração por até seis meses, prorrogável por igual período.

- Proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.

5.Titular dos dados

Conforme disposto na LGPD, o titular dos dados é a pessoa natural a quem se refere os dados pessoais, objeto de tratamento. Como o próprio nome da lei já evidencia, os dados relacionados à pessoa jurídica não estão no escopo desta nova legislação brasileira.

5.1. Direitos determinados

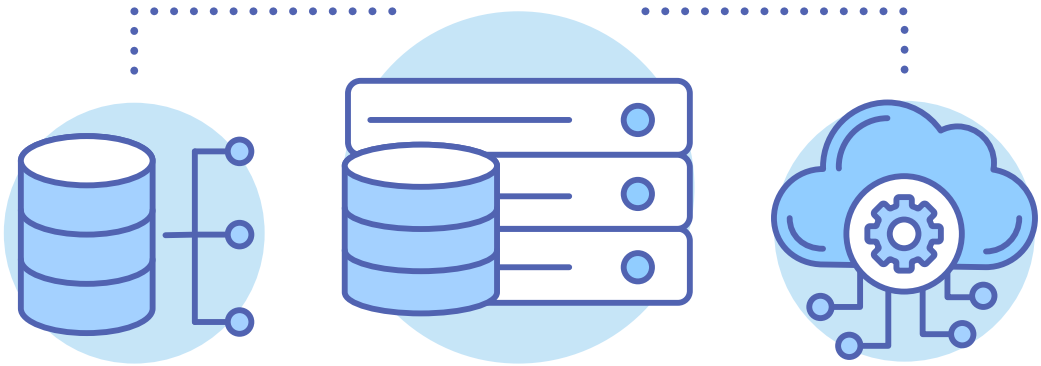
Para garantir os direitos fundamentais de liberdade, intimidade e privacidade das pessoas físicas, a Lei Geral de Proteção de Dados prevê um conjunto de direitos aos titulares dos dados pessoais tratados:

I. confirmação da existência de tratamento de dados.
II. acesso aos dados pessoais.
III. correção de dados incompletos, inexatos ou desatualizados.
IV. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei.
V. direito à portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, desde que sejam observados os segredos comercial e industrial – caso existentes.
VI. eliminação de dados pessoais tratados com o consentimento do titular, exceto para o cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida – sempre que possível – a anonimização dos dados; transferência a terceiro, desde que sejam respeitados os requisitos de tratamento desta lei; ou uso exclusivo do controlador, vedado acesso por terceiro, desde que os dados sejam anonimizados.
VII. informação sobre os dados compartilhados com outras organizações.
VIII. informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
IX. revogação do consentimento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento manifestado anteriormente.

6. Tratamento de dados

6.1. O que é?

São consideradas atividades de tratamento de dados todas aquelas que utilizem um dado pessoal em sua operação, como as ações de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.



6.2. Agentes de tratamento nas empresas

O controlador e o operador são responsáveis por manter registro das operações de tratamento de dados pessoais que realizarem, especialmente em situações de legítimo interesse. O controlador deverá, ainda, indicar um encarregado pelo tratamento de dados pessoais.

- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados pessoais realizado pela empresa.

- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que, conforme instruções do controlador, realiza o tratamento de dados pessoais.

- **Encarregado:** pessoa indicada pelo controlador para atuar como um canal de comunicação entre os representantes da empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Em países que fazem parte da Área Econômica Europeia, esta função é conhecida como Data Protection Officer (DPO).

6.3. Responsabilidade legal

A Lei Geral de Proteção de Dados considera tanto o controlador quanto o operador responsáveis por eventuais danos patrimonial, moral, individual ou coletivo, em caso de violação à respectiva legislação.

Sendo assim, para assegurar a indenização ao titular dos dados, o operador responde solidariamente quando descumprir as obrigações da lei ou caso não tenha seguido as instruções do controlador. Por sua vez, o controlador envolvido em tratamento de dados do qual decorreram os danos também responderá solidariamente.

Caso não haja violação à LGPD ou o dano seja de culpa exclusiva de terceiros ou do titular dos dados, nenhum dos agentes será responsabilizado.

7. Adequação à Lei Geral de Proteção de Dados

7.1. Aplicação no âmbito empresarial

Para cumprir a missão de proteger os dados de pessoas físicas, a LGPD impõe que as empresas públicas e privadas realizem o tratamento de dados pessoais dos cidadãos. Com isso, torna-se imprescindível adaptar processos e procedimentos para garantir segurança e evitar multas e penalidades dispostas pela lei.

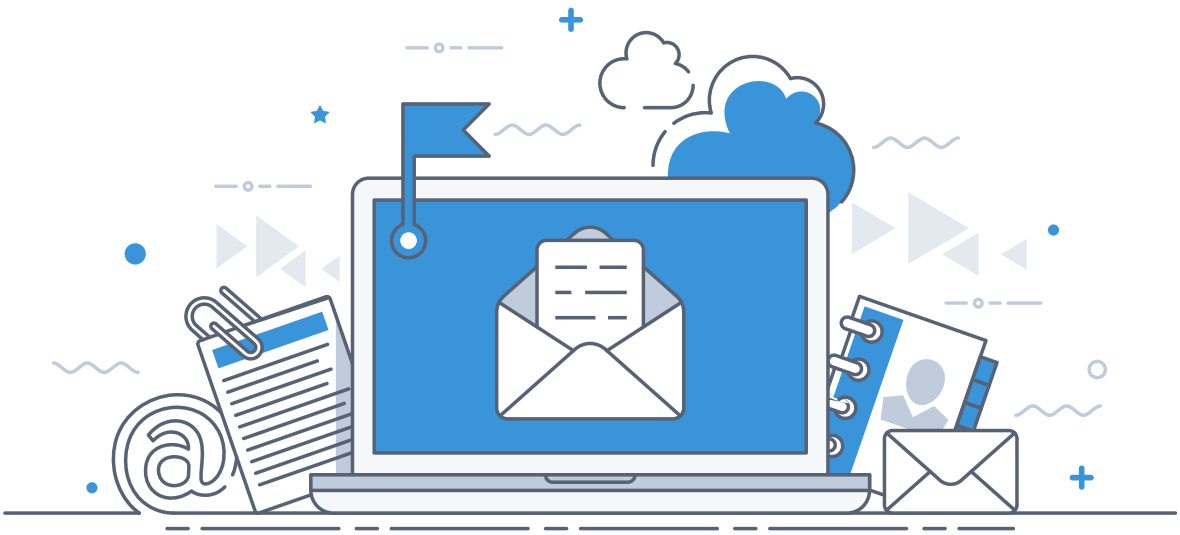
Neste cenário, é preciso envolver todas as áreas da empresa, principalmente Jurídico, Recursos Humanos e Tecnologia da Informação, formando um comitê de "Governança de Dados". Essa estrutura permite analisar como a LGPD irá impactar o negócio, além de levantar questões sobre como, porque e quais categorias de dados pessoais deverão ser tratados. Com a lei, é preciso entender e mapear o tratamento de dados, buscando identificar sua finalidade.

O empresário também precisa ficar atento à definição de regras ligadas às boas práticas e à governança, o chamado *compliance*, incluindo ainda o regime de funcionamento do negócio e os procedimentos corporativos, como a gestão de contratos e normas internas. Mas, para agir em conformidade com a lei, as empresas devem investir, ainda, no treinamento de suas equipes.

7.2. Fases para adaptação à LGPD

A implantação da Lei Geral de Proteção de Dados pode variar conforme o porte da empresa, o fluxo de tratamento de dados pessoais e o nível de procedimentos relativos a cada departamento. No entanto, é possível dizer que os processos de adaptação à lei seguem, em geral, as seguintes fases: (I) sensibilização; (II) diagnóstico e preparação; (III) avaliação e organização; (IV) mapeamento; (V) políticas; (VI) processos; (VII) treinamentos; (VIII) monitoramento.

Para exemplificar os processos de adaptação à LGPD, a Fecomércio MG apresenta um caso real de planejamento de ações, produzido para uma empresa de grande porte, onde as etapas foram devidamente detalhadas.



	1. Sensibilização
1	Conscientização da alta liderança.

	2. Diagnóstico e preparação
1	Nomeação, ratificação e divulgação do Comitê de Governança de Dados Pessoais.
2	Atribuição e manutenção das responsabilidades de cada membro do comitê (Matriz RACI).
3	Nomeação do Encarregado de Proteção de Dados (EPD).
4	Reunião com o comitê para alinhamento dos trabalhos – o EPD (encarregado) precisa estar presente.
5	Treinamento do Comitê de Governança de Dados Pessoais.
6	Levantamento das regras, regulamentos, leis e normas de proteção de dados e privacidade em nível nacional e internacional que impactam ou podem impactar a empresa: ● LGPD (Lei Geral de Proteção de Dados); ● GDPR (Regulamento Geral sobre a Proteção de Dados); ● Código Civil; ● Resoluções; ● Marco Civil da Internet; ● Lei nº. 12.737/2012 (Lei Carolina Dieckmann) ● Código de Defesa do Consumidor; ● Lei de Acesso à Informação.
7	Levantamento e listagem dos contratos existentes que, de alguma forma, podem incidir em infrações relativas à LGPD. Na fase seguinte, serão realizadas ações sobre esses contratos, como a inclusão de cláusulas relativas à proteção de dados.
8	Inventário e verificação do fluxo de quem envia os dados pessoais para a organização, como clientes, fornecedores, funcionários e fontes de pagamentos. Estudo sobre como a organização recebe os dados pessoais: - Para quem são transmitidos; - Que tipo de dados pessoais são coletados em cada ponto de entrada. Ex.: cadastro de um novo cliente. Registro dos locais onde são mantidos os dados pessoais: ● Servidor local – fica em *data center* local ou em *colocation*? ● São armazenados dados pessoais em nuvem? Caso seja, qual é a solução utilizada: Amazon, Azure, ou outra infraestrutura de nuvem? ● São armazenados dados pessoais em *laptops*? ● São armazenados dados pessoais em *smartphones*? ● Quem possui acesso aos dados pessoais (áreas e líderes da empresa)?
9	Identificação dos sistemas utilizados (digital e físico): ● Tipo de sistemas utilizados (papel ou digital); ● Quem os utiliza (dentro da estrutura da empresa); ● Tipos de dados tratados (normais ou sensíveis); ● A forma como os dados são gerenciados; ● Como os dados são transmitidos (interna e externamente – inclusive se forem transmitidos para outros órgãos ou reguladores, dentro e fora do país).

10	Levantamento dos processos existentes relativos ao tratamento de dados pessoais.
11	Parte documental de Tecnologia da Informação (TI): o Estrutura do site; ● Onde está hospedado (internamente ou em nuvem)? ● No site, ocorre coleta de dados pessoais? Caso aconteça, onde? ● Quais *cookies* são utilizados? ● Há alguma política de privacidade? o Topologia de rede; o Como funcionam os *backups* (documentação da estrutura).
12	Análise do impacto da privacidade e da realização de auditorias, somadas à avaliação dos dados iniciais.
13	Instauração de Programa de Proteção de Dados e Privacidade.
14	Promoção de ações de comunicação e marketing – divulgação das atividades realizadas pela empresa e conscientização das equipes para o cumprimento da lei.

	3. Avaliação e organização
1	Avaliação do cenário de fornecedores, prestadores de serviço e parceiros (operadores).
2	Avaliação de riscos e gaps: com o diagnóstico do levantamento de dados pessoais, deve-se analisar inicialmente a proteção de dados e a privacidade para verificar as ações da organização em relação ao tema e mapear possíveis riscos para o negócio e para os indivíduos.
3	Avaliação e correlacionamento de quais direitos dos titulares dos dados estão ou não sendo devidamente atendidos.
4	Análise, revisão e entendimento do impacto das documentações, regras, regulamentos e normas de proteção de dados e privacidade nas atividades da empresa.
5	Avaliação sobre o orçamento da empresa para investimento em recursos de marketing, sistemas, ferramentas tecnológicas.
6	Definição do plano de ação para as demais etapas – Programa de Proteção de Dados e Privacidade.
7	Criação de um código de conduta a ser assinado por todos os funcionários da empresa.
8	Promoção de ações de comunicação e marketing – divulgação das atividades realizadas pela empresa e conscientização das equipes para cumprimento da lei.

	4. Mapeamento
1	Correlacionamento dos tratamentos atuais com princípios e bases legais.
2	Identificação dos responsáveis pelas operações de tratamento.
3	Identificação e avaliação das medidas de segurança existentes.
4	Conhecimento de todo o ciclo de vida dos dados pessoais (criação → uso → compartilhamento → armazenamento → exclusão).
5	Confecção de relatórios e *checklist* (inventário de dados) demonstrando a existência de dados pessoais na organização, divididos por setores e categorias.
6	Desenvolvimento e implementação de estratégias, planos e políticas de privacidade e proteção de dados pessoais – Sistema de Classificação de Dados Pessoais: "disponível publicamente", "confidencial", "sensível".
7	Promoção de ações de comunicação e marketing – divulgação das atividades realizadas pela empresa e conscientização das equipes para o cumprimento da lei.

	5. Políticas
1	Realização de ajustes e/ou desenvolvimento de políticas/manuais relacionadas à privacidade e à proteção de dados: • Política de Privacidade; • Política de Proteção de Dados; • Políticas para fornecedores, clientes, terceiros, prestadores de serviços; • Políticas de segurança da informação; • Política de Segurança Cibernética; • Adequação jurídica do Departamento de Recursos Humanos; • Cláusulas de confidencialidade; • Manual de boas práticas.
2	Desenvolvimento e implementação de um sistema de transferência internacional de dados pessoais (dados para operadores "nuvens").

3	Execução de um plano que atenda aos titulares dos dados sobre solicitações, reclamações e retificações, a ser gerenciado pela organização, e contenha: • Procedimentos de acesso a dados pessoais; • Procedimentos de reclamações de dados pessoais; • Procedimentos de retificação de dados pessoais; • Procedimentos de objeção de dados pessoais; • Procedimentos de portabilidade de dados pessoais; • Procedimentos de eliminação de dados pessoais; • Procedimentos de manipulação de dados pessoais.
4	Instauração e manutenção de um plano de resposta de violação de privacidade de dados, cujas as funções são: • Estabelecer o procedimento de notificação de violação para os titulares afetados; • Reportar, no tempo exigido, os incidentes de privacidade de dados para os órgãos reguladores; • Manter os *logs* que registram detalhes dos incidentes; • Apresentar relatório de métricas para gestores estratégicos; • Obter cobertura de seguro para os custos associados à violação.
5	Estabelecimento de um cronograma de retenção de dados que defina o período no em que eles serão armazenados – Política de Retenção de Dados.
6	Criação de um modelo de Relatório de Impacto sobre Proteção de Dados Pessoais (RIPD).
7	Inclusão de tarefas relacionadas às medidas de *compliance* 'anticorrupção'.
5	Promoção de ações de comunicação e marketing – divulgação das atividades realizadas pela empresa e conscientização das equipes para o cumprimento da lei.

6. Processos

1	Criação de mecanismos para efetivação das práticas de *compliance*, resguardando a organização e seus gestores de responsabilização cível, administrativa e criminal. Inclusão de formulários de consentimento dos titulares dos dados, de consentimento dos pais ou responsáveis, avisos de privacidade e outros aceites.
2	Conscientização sobre *privacy by design* (privacidade desde a concepção) e *privacy by default* (privacidade por padrão).
3	Desenvolvimento de uma estratégia de prevenção de perda de dados pessoais.
4	Realização de testes de segurança da informação (*pentest*).

5	Aconselhamento em relação à implementação de sistemas de computadores para a proteção de dados e privacidade: ● *Backup*; ● *Criptografia*; ● *Data Loss Prevention* (DLP); ● *Web Application Firewall* (WAF); ● *Next Generation Firewall* (NGFW); ● *Intrusion Prevention System* (IPS).
6	Promoção de ações de comunicação e marketing – divulgação das atividades realizadas pela empresa e conscientização das equipes para o cumprimento da lei.

7. Treinamentos

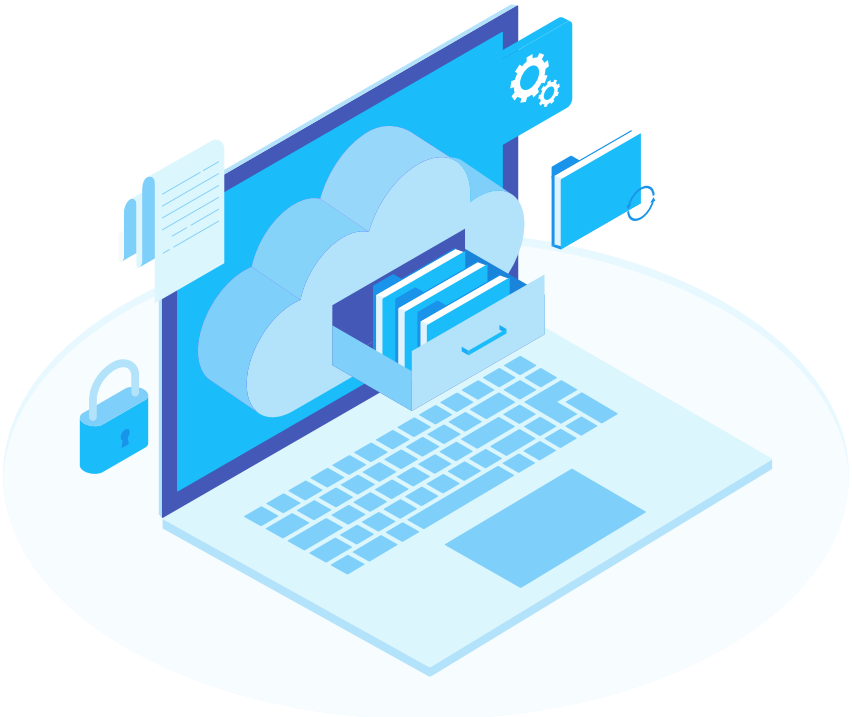
1	Realização de um treinamento básico sobre a proteção de dados e privacidade com os colaboradores da empresa, que inclua: ● Informações sobre o programa implementado; ● O que é privacidade; ● O que são dados pessoais e dados sensíveis; ● Quais são os direitos dos titulares dos dados; ● Quais são as responsabilidades do controlador da empresa; ● Quais são as responsabilidades de cada colaborador no processo de implementação do programa de privacidade e proteção de dados; ● Conscientização sobre os avisos explícitos para o cliente sobre a coleta, uso, tratamento e manutenção dos dados na base.
2	Inclusão do treinamento sobre privacidade em outras capacitações, como no momento de admissão de um novo funcionário.
3	Definição de um plano de comunicação que explicite o uso dos dados pessoais dentro de cada departamento e integre a proteção de dados para toda a empresa, permitindo aos funcionários coletar apenas as informações necessárias e redobrar os cuidados em relação aos dados compartilhados.
4	Realização de testes de segurança da informação (*pentest*).

	8. Monitoramento
1	Sugestão de contratação de auditoria externa entre períodos determinados para assegurar que a organização está em conformidade com os processos e as políticas de adequação estabelecidas. Realização de *benchmarks* para avaliação de resultados.
2	Conscientização sobre a atualização constante das políticas desenvolvidas, de acordo com as mudanças nas leis ou outros aspectos que venham impactar o negócio.
3	Manutenção das atividades de conscientização e treinamento sobre privacidade e proteção de dados (a cada seis meses ou um ano, promover um treinamento sobre mudanças impostas pela ANPD).
4	Monitoramento constante das leis e regulamentos.
5	Promoção de ações de comunicação e marketing – divulgação das atividades realizadas pela empresa e conscientização das equipes para o cumprimento da lei.


SysRq
Pause
Break
Backspace
Enter
Shift

8. Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

De responsabilidade do controlador, essa documentação serve para identificar os riscos específicos aos dados pessoais como resultado das atividades de processamento. O relatório deve ser elaborado antes da implementação de novos projetos, processos ou políticas. Dessa forma, o RIPD reúne informações coletadas, tratadas, usadas e compartilhadas, além de medidas adotadas para mitigar riscos que possam afetar os direitos fundamentais do titular dos dados pessoais.



8.1. Como elaborar o RIPD

O Relatório de Impacto à Proteção de Dados Pessoais deve ser elaborado na fase inicial do tratamento de dados, quando o projeto estiver sendo definido. Para tanto, a empresa precisa delimitar as seguintes etapas:

- **Identificação dos agentes de tratamento:**

nesta fase, deve-se nomear o controlador, o operador e o encarregado pelos dados pessoais. Além disso, é preciso registrar contatos de telefone e e-mail do encarregado, pois ele será o ponto focal entre a empresa, o titular dos dados e a ANPD.

- **Necessidade de elaboração do relatório:**

é preciso entender os casos específicos em que esse relatório poderá ser solicitado e, a partir disso, descrever as etapas do tratamento de dados pessoais.

- **Descrição do tratamento:**

nesta etapa, a empresa deve discriminar cada processo de tratamento de dados pessoais que possa gerar risco às liberdades civis e aos direitos dos titulares dos dados. Essa definição possibilita a visão de um cenário institucional, fornecendo subsídios para a avaliação e o tratamento de eventuais riscos.

- **Necessidade e proporcionalidade:**

deve-se entender e descrever como a empresa avalia a necessidade dos dados que serão solicitados para demonstrar que as operações limitam o tratamento ao mínimo necessário para a realização de suas finalidades.

- **Identificação e avaliação dos riscos:**

a Lei Geral de Proteção de Dados define que o RIPD deve conter medidas de mitigação de risco. No entanto, essas ações devem ser pensadas a partir da identificação dos riscos no processo de tratamento de dados. Assim, será possível identificar as medidas mais assertivas para tratar os riscos mapeados.

- **Aprovação do relatório:**

a próxima etapa consiste em formalizar a aprovação do RIPD. Para isso, é preciso obter as assinaturas do encarregado, das autoridades que representam o controlador e o operador e do responsável pela elaboração do relatório – o próprio encarregado ou pessoa designada pelo controlador para realizar a demanda.

- **Manutenção da revisão:**

nesta fase se estabelece que o relatório seja revisto e atualizado em caso de mudança que afete o tratamento de dados pessoais realizado pela empresa. Diante de possíveis transformações tecnológicas, políticas, normativas e institucionais, é imprescindível que o RIPD seja reanalisado, pelo menos, com periodicidade anual.

9. Término do tratamento

A conclusão da fase de tratamento de dados pessoais e a sua eliminação do banco de informações da empresa ocorrerá quando: (I) for constatada que a finalidade foi alcançada ou que os dados se tornaram desnecessários para a finalidade específica almejada; (II) quando o período de tratamento chegar ao fim; (III) caso o titular exerça o direito de revogação do consentimento, resguardado o interesse público; ou (IV) por determinação da autoridade nacional, quando houver violação desta lei.

No entanto, a LGPD autoriza a conservação dos dados em quatro hipóteses: (I) para o cumprimento de obrigação legal ou regulatória pelo controlador; (II) para o estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados; (III) para a transferência a terceiro, desde que respeitados os requisitos de tratamento de dados; ou (IV) para o uso exclusivo do controlador, vedado o seu acesso por terceiro, desde que os dados sejam anonimizados.

10. Ciclo de vida do tratamento de dados pessoais

Estratégica para o tratamento correto dos dados pessoais, esta etapa também é primordial para a adoção de medidas adequadas ao longo do seu ciclo de vida. Por isso, a empresa, seja ela pública ou privada, precisa entender os dados pessoais que gerencia, bem como os processos, projetos, serviços e ativos.

1.

Coleta

momento de obtenção, recepção ou produção de dados pessoais independentemente do meio utilizado.

2.

Retenção

fase em que ocorre o armazenamento de dados pessoais pela empresa, seja de forma física ou digital.

3.

Processamento

operação onde ocorre a classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.

4.

Compartilhamento

etapa que reúne a transmissão, distribuição, comunicação, transferência, difusão ou compartilhamento de dados pessoais.

5.

Eliminação

fase destinada à exclusão dos dados ou à eliminação de ativos organizacionais.

11. Conte com a Fecomércio MG

Capacitação e orientação

Para fortalecer o comércio de bens, serviços e turismo em Minas Gerais, a Fecomércio MG aborda em suas lives temas pertinentes à atuação de sindicatos e empresas representadas pela Federação. Ciente das responsabilidades trazidas pela LGPD, a entidade disponibilizou o webinar "LGPD na prática: o que muda para você?", em seu canal no YouTube.

O encontro, com participação do Coordenador de TI da Fecomércio MG, Dênis Zeferino, e da consultora de sistemas da ao3, Juliana Borsato, esclarece as principais dúvidas sobre o tema e demonstra, de forma prática, como essa norma afetará a rotina das empresas.

Clique aqui e assista!

Para auxiliar com mais conteúdo sobre o tema, a Fecomércio MG possui uma websérie de LGPD que começa com o vídeo "O que é a LGPD e qual seu objetivo?".

Clique aqui e assista!

Para mais informações, acesse o site: fecomerciomg.org.br

Curta nossas redes sociais!

Expediente
Produção de textos: Comunicação
Diagramação: Marketing
Corpo técnico: Comercial, Jurídico e Tecnologia da Informação

CNC · Fecomércio MG · Sesc · Senac · Sindicatos Empresariais

Sistema Comércio