Cartilha Entenda a Lei Geral de Proteção de Dados

Fecomércio RS
Sesc | Senac

Introdução

A LGPD (Lei Geral de Proteção de Dados) é a lei nº 13.709, aprovada em agosto de 2018 mas que entrou em vigência em agosto de 2020. Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Mas por que a LGPD é tão importante para as empresas? Porque todos os negócios e organizações terão que atender às exigências da Lei, que prevê a aplicação de penalidades a partir de agosto de 2021 a quem não cumpri-la. Em suma, a LGPD irá afetar a forma como as empresas captam, armazenam e utilizam os dados de seus clientes. Por isso, preparamos esta cartilha para você entender tudo sobre a Lei Geral de Proteção de Dados, e como a sua empresa pode se adaptar a ela.

O que é?

A Lei Geral de Proteção de Dados, conhecida como LGPD, foi publicada no dia 14 de agosto de 2018. Inscrita sob o número 13.709, a lei é baseada na GDPR, lei europeia, e uma das precursoras do tratamento de dados pessoais no mundo.

**Lei publicada para proteger os dados das pessoas (ex. nome, telefone, endereço, CPF...).*

Objetivo

O objetivo da LGPD é o de proteger os direitos fundamentais de liberdade e de privacidade e o livre-desenvolvimento da personalidade da pessoa natural, mediante a disposição sobre o tratamento de dados pessoais.

**Fazer com que as empresas utilizem os dados pessoais unicamente para a finalidade que foram solicitados.*
**Evitar vazamento e venda de dados.*

Conceitos

A LGPD trouxe novos conceitos para o arcabouço legislativo brasileiro que serão abordados abaixo, além de outros que são relevantes para o tema:

- **Dados pessoais:** informação relacionada à pessoa natural identificada ou identificável;
- **Dados pessoais sensíveis:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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;
- **Tratamento:** toda operação realizada com dados pessoais;
- **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

• **Dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

• **Banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

• **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

• **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais;

• **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

• **Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

• **Encarregado:** 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);

• **Privacy by Default (privacidade como padrão):** Assim que um produto ou serviço for lançado ao público, as configurações mais seguras de privacidade deverão ser aplicadas por padrão, sem nenhuma entrada manual do usuário final. Além disso, todos os dados pessoais fornecidos pelo usuário para permitir o uso ideal de um produto devem ser mantidos apenas pelo tempo necessário para fornecer o produto ou serviço. Se mais informações do que o necessário para fornecer o serviço forem divulgadas, esse conceito será violado.

• **Privacy by Design (privacidade desde a concepção):** Qualquer projeto de uma empresa que envolva o processamento de dados pessoais deve ser realizado mantendo a proteção e a privacidade dos dados a cada passo. Isso inclui o desenvolvimento de produtos, desenvolvimento de software, sistemas de TI, etc.

Princípios

A LGPD baseia-se em vários princípios, importando frisar, dentre eles:

• Respeito à privacidade;

• À autodeterminação informativa;

• À liberdade de expressão, de informação à inviolabilidade da intimidade, da honra e da imagem;

• Ao desenvolvimento econômico e tecnológico e a inovação;

• Livre-iniciativa, livre-concorrência, dentre outros;

Quando a LGPD não se aplica

Importante referir que a LGPD não é aplicável a todo e qualquer tratamento de dados pessoais, havendo algumas exceções constantes na lei, quando:

• Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

• Realizado para fins exclusivamente: jornalístico e artísticos ou acadêmicos;

• Realizado para fins exclusivos de: segurança pública; defesa nacional; segurança do estado; ou atividades de investigação e repressão de infrações penais; ou

• Provenientes de fora do território nacional e não usados e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou com outro país que não possua adequado nível de proteção de dados.

Possibilidades de tratamento

Já os casos em que se pode tratar dados pessoais, a lei exemplifica dez possibilidades (também chamadas de bases legais), sendo essa lista taxativa, cabendo destacar os seguintes:

• Consentimento do titular;

• Cumprimento de obrigação legal ou regulatória pelo controlador;

• Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

• Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

• Para a proteção da vida ou da incolumidade física do titular ou de terceiro;

• Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

• Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

• Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

• Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contrato, convênios ou instrumentos congêneres.

• Para a realização de estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

Importa frisar que os agentes de tratamento devem coletar e processar os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida.

Dados sensíveis

Aquele que precisar tratar de dados pessoais sensíveis deverá ter o dobro de atenção em seus processos, pois eles são tratados de forma excepcional pela LGPD, que restringe o seu tratamento apenas quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas ou então sem consentimento, quando para:

• Cumprimento de obrigação legal ou regulatória pelo controlador;

• Exercício regular de direitos;

• Proteção da vida ou da incolumidade física do titular ou de terceiro;

• Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

• Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

• Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

• Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

• Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoas sensíveis.

Término do Tratamento

A LGPD define em quais ocasiões o tratamento terminará:

• Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

• Fim do período de tratamento;

• Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento; ou

• Determinação da autoridade nacional, quando houver violação à LGPD.

Ainda, permite a manutenção desses dados nos seguintes casos:

• Cumprimento de obrigação legal ou regulatória pelo controlador;

• Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

• Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta lei; ou

• Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Direitos do Titular

O titular dos dados tem seus direitos definidos dentro da LGPD, podendo obter junto ao controlador, a qualquer momento e mediante requisição:

• Confirmação da existência de tratamento;

• Acesso aos dados;

• Correção de dados incompletos, inexatos ou desatualizados;

• Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;

• Portabilidade dos dados a outro fornecedor de serviço ou produto;
• Eliminação dos dados pessoais tratados com o consentimento do titular;

• Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

• Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

• Revogação do consentimento.

A partir do requerimento do titular dos dados, a empresa demandada providenciará a confirmação ou acesso a dados pessoais, em formato simplificado de modo imediato, ou então por meio de declaração clara e completa, observado o segredo comercial, em até quinze dias contados da data do requerimento.

Obrigações do Controlador

Conforme já apontado anteriormente, o controlador é a pessoa física ou jurídica a quem importa tomar decisões referentes ao tratamento de dados. É ele que tem obrigações perante os titulares dos dados e ao poder público e precisará se adaptar à LGPD. Dentre as obrigações contidas na Lei, cabe destacar:

• Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

• As medidas referidas acima deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução;

• Qualquer pessoa que intervenha em uma das fases de tratamento obriga-se a garantir a segurança da informação, mesmo após o término do tratamento;

• Comunicação à Autoridade Nacional de Proteção de Dados (ANPD) de incidentes de segurança que possam ac arretar risco ou dano relevante aos titulares de dados;

O Encarregado (DPO)

O Encarregado, também conhecido pela sigla em inglês “DPO”, será indicado pelo controlador e deverá ter sua identidade e informações para contato divulgadas publicamente, de forma clara e objetiva.

É o Encarregado quem:

• Aceitará reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

• Receberá comunicações da autoridade nacional e adotar providências;

• Orientará os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

• Executará as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

O Encarregado pode ser tanto um profissional interno da empresa, como uma pessoa jurídica de consultoria contratada exclusivamente para tal cargo, por exemplo. Independentemente da escolha, sugere-se que o Encarregado possua conhecimento multidisciplinar e acesso a todas as áreas da empresa, especialmente na etapa de implantação da LGPD.

Além das atribuições legais, o Encarregado deve gerenciar e acompanhar a implementação da Lei, bem como garantir a conformidade em todo o período de sua vigência. Para tanto, deverá elaborar plano de gestão de riscos à proteção de dados pessoais, gerenciar os incidentes que envolvam dados pessoais, administrar todo o ciclo de vida dos dados, entre outras.

Boas Práticas e Governança

A implementação de um guia de boas práticas e governança de dados pessoais é altamente aconselhada e deve seguir algumas diretrizes, especificadas na própria LGPD:

• Demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

• Seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

• Seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

• Estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

• Tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

• Esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

• Conte com planos de resposta a incidentes e remediação; e

• Seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Importante deixar claro que a adoção de um guia de boas práticas e governança será levada em consideração na hora de aplicação de sanção administrativa.

Sanções Administrativas

As sanções contidas na LGPD são nove e podem variar desde uma advertência até a proibição do exercício de atividades relacionadas a tratamentos dados ou multa em valor de até R$ 50.000.000,00 (cinquenta milhões de reais).

Para a aplicação das sanções, serão observados alguns requisitos, tais como:

• A gravidade e a natureza das infrações e dos direitos pessoais afetados;

• A boa-fé do infrator;

• A vantagem auferida ou pretendida pelo infrator;

• A condição econômica do infrator;

• A reincidência;

• O grau do dano;

• A cooperação do infrator;

• A adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto na LGPD;

• A adoção de política de boas práticas e governança;

• A pronta adoção de medidas corretivas; e

• A proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Neste ponto, é importante frisar que as sanções administrativas passaram a vigorar a partir de 01º de agosto de 2021.

Autoridade Nacional de Proteção de Dados (ANPD)

A Autoridade Nacional de Proteção de Dados (ANPD) foi criada junto à LGPD mas sofreu veto presidencial e só retornou ao texto da lei com a publicação da Medida Provisória nº 869/2018, posteriormente convertida na Lei 13.853/2019. Ela teve, no dia 26 de agosto de 2020, seu regimento interno publicado. É ela quem vai zelar pelo cumprimento e fiscalização da LGPD, bem como quem aplicará as sanções administrativas em casos de infração à lei.

Vigência

A LGPD passou a viger no dia 17 de setembro de 2020, após sanção tácita da lei nº 14.010/2020 pelo Presidente da República. A entrada em vigor das suas sanções administrativas, entretanto, foram adiadas até o dia 01º de agosto de 2021.

Política de Privacidade (PP)

É o principal documento informativo ao titular dos dados, devendo atender ao princípio da transparência, com informações claras, precisas e de fácil acesso. O mínimo é a confecção de uma política de privacidade geral, mas é possível que seja necessário fazer políticas específicas, a depender da situação.

Sugere-se que a PP contenha, no mínimo, os seguintes pontos:

- Identificação do controlador e DPO (encarregado), com suas respectivas informações de contato;
- Apresentação de todos os direitos e as garantias individuais do Titular de Dados;
- Descrição das responsabilidades dos agentes que realizarão o tratamento;
- Descrição sobre o uso compartilhado de dados pelo controlador e a finalidade;
- Indicação relativa à privacidade de crianças e adolescentes, considerando a legislação pertinente, observando o Art. 14 da LGPD;
- Especificação da política de segurança da informação adotada para os dados pessoais sensíveis;
- Finalidade do tratamento;
- Forma e duração do tratamento.

Importa frisar que esse documento é volúvel, ou seja, pode – deve – ser constantemente reavaliado e atualizado, de acordo com as novas possibilidades de tratamento de dados pessoais que surjam no decorrer do tempo. Eventuais alterações devem ser informadas aos titulares de dados, em tempo hábil, levando em consideração um tempo razoável para que o titular possa se adaptar às novas diretrizes ali constantes.

Sugestões de Ações

A LGPD é um arcabouço jurídico complexo e que ainda está dando os seus primeiros passos em solo brasileiro. Logo, é muito provável que novas regras alterem algumas das disposições aqui constantes e, até mesmo, criem novas obrigações ou direitos envolvendo o tratamento de dados. Logo, sugere-se sejam tomadas algumas ações:

• Nomear um Encarregado (DPO – Data Protection Officer) que responderá em nome da empresa por questões que envolvam o tratamento de dados pessoais;

• Revisar procedimentos para constatar quais deles envolvem tratamento de dados pessoais e, a partir daí, reformular atividades internas a fim de se adequar à legislação;

• Após essa revisão, pegar cada base de dados e tentar adequar elas à legislações ou contratos, visando evitar o uso da autorização pelo titular do dado;

• Ainda, após essa revisão, verificar quais dados coletados pela empresa são realmente necessários para a execução dos processos internos, lembrando que quanto menos acesso a dados, menor a chance de incorrer em violação à LGPD;

• O assunto envolve situações jurídicas e de tecnologia da informação, sendo aconselhado mesclar os conhecimentos;

• Criar um manual contendo políticas de boas práticas e governança exclusivo ao tratamento de dados pessoais (será considerado em caso de imposição de alguma penalidade);

• Utilizar o método de "Privacy by Default", que significa pensar na privacidade de dados pessoais sempre que se criar um novo processo dentro da empresa;

• Criar a Política de Segurança da Informação (PSI), que consiste em um conjunto de diretrizes e regras que tem por objetivo possibilitar o planejamento, a implementação e o controle de ações relacionadas à segurança da informação;

• Assinatura de termos de confidencialidade (NDA – non-disclosure agrément) com os funcionários, comprometendo todos a não divulgar informações confidenciais que envolvam dados pessoais;

• Contratação de um serviço de armazenamento em nuvem, visando maior garantia na proteção de dados pessoais;

• Criação de um modelo de relatório de impacto à proteção de dados pessoais, documento que pode ser requerido pela ANPD;

Plano de Ação

Além das sugestões contidas no ponto anterior, sugere-se um plano de ação para implantação da LGPD, baseado no plano de ação sugerido pelo Departamento Nacional do Sesc, conforme segue abaixo.

GESTÃO DE PROTEÇÃO DE DADOS

- Indicar DPO;
- Definir Grupo de Trabalho para implantação da LGPD;
- Alinhar serviços compartilhados;
- Indicar pontos focais da LGPD;
- Realizar inventário de dados;
- Implementar canal de comunicação para gerir requisições dos titulares de dados;
- Analisar segurança e vulnerabilidade dos dados.

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

- Elaborar política de privacidade geral;
- Elaborar política de privacidade específica;
- Elaborar política para tratamento das requisições;
- Elaborar política de arquivamento e descarte dos dados;

- Elaborar Matriz de Risco da lei;
- Atualizar política e norma de Segurança da Informação;
- Criar relatório de impacto à proteção de dados pessoais.

GESTÃO DE PROCESSOS

- Definir processos críticos;
- Revisar processos críticos;
- Elaborar processos de apoio ao DPO;
- Elaborar mapa de ciclo de vida dos dados.

COMUNICAÇÃO INTERNA

- Elaborar plano de comunicação interna.

COMUNICAÇÃO EXTERNA

- Elaborar plano de comunicação externa.

GESTÃO DE CONTRATOS E CONVÊNIOS

- Comunicar fornecedores acerca do cumprimento da lei;
- Identificar instrumentos que necessitam de aditivação;
- Criar cláusula geral de privacidade para contratos e convênios;
- Aditivar instrumentos vigentes.

AÇÕES DE CAPACITAÇÃO INTERNA

- Estruturar plano de capacitação;
- Realizar palestra inicial;
- Elaborar curso de boas práticas.

AÇÕES DE RECURSOS HUMANOS

- Definir cláusula geral de privacidade;
- Ajustar regulamento de pessoal;
- Revisar novos contratos de trabalho;
- Aditivar contratos de trabalho existentes.

Versão 02 - Novembro de 2021.

Fecomércio RS · Sesc · Senac

Sistema Comércio