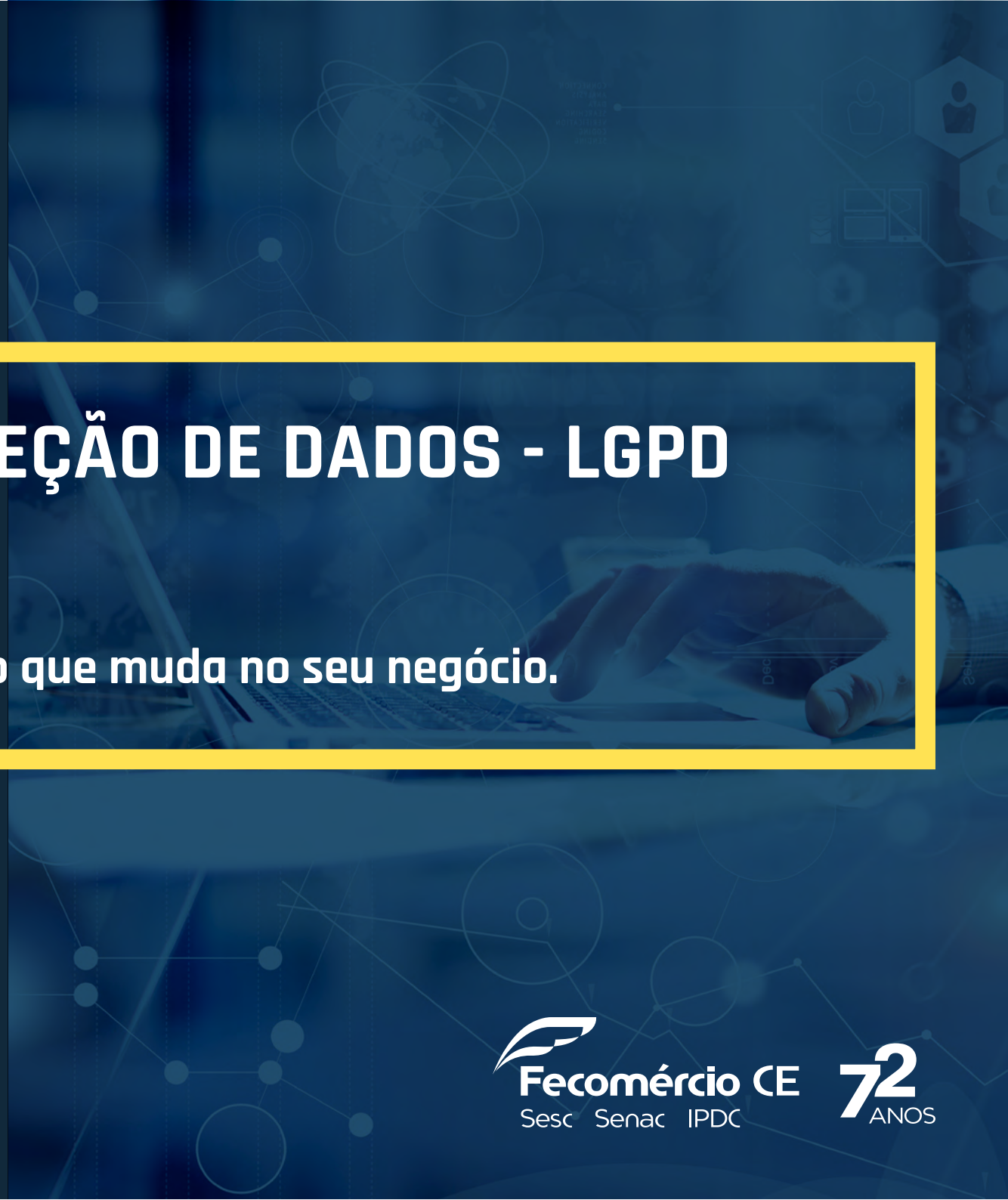
LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

Lei 13.709/2018

Conheça os detalhes da lei e o que muda no seu negócio.



Fecomércio CE
Sesc Senac IPDC

72 ANOS

INTRODUÇÃO

A Lei Geral de Proteção de Dados, sancionada em agosto de 2018, entrou em vigor em setembro de 2020. A lei determina as obrigações que empresas e organizações possuem diante da coleta, armazenamento, tratamento e compartilhamento de dados pessoais, tanto online quanto offline.

O Brasil agora faz parte dos mais de 120 países que possuem lei específica para a proteção de dados pessoais. O objetivo da lei é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A lei prevê multas e penalidades consideráveis no caso de não cumprimento dos requisitos impostos na lei.

Neste e-book você conhecerá as principais características da Lei Geral de Proteção de Dados e o que muda no seu negócio.

SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Carta de Direitos Fundamentais da União Europeia reconheceu em seu Art. 8º a Proteção de Dados como um direito autônomo, destacado do Direito à Privacidade (Art. 7º).

Modelo europeu de proteção de dados: Tutela da privacidade no sentido de proteção dos dados pessoais é um direito fundamental (Regulamento Geral de Proteção de Dados – GPDR).

Modelo norte-americano de proteção de dados: Tutela da privacidade no sentido de proteção dos dados pessoais não configura um direito fundamental. A abordagem norte-americana tem um aspecto mais prático, mais voltado para a solução e proteção de situações específicas, que culminam em legislações separadas para cada uma delas.

Modelo brasileiro de proteção de dados: A proteção dos dados pessoais no sistema jurídico brasileiro se aproxima do modelo europeu, pois reconhece seu status de direito fundamental.

DO QUE DISPÕE A LEI GERAL DE PROTEÇÃO DE DADOS?
Tratamento de dados pessoais por pessoas naturais ou jurídicas (públicas e privadas).

QUAIS SEUS PRINCIPAIS OBJETIVOS?

- Proteção à privacidade;
- Assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais;
- Transparência;
- Estabelecer regras claras sobre tratamento de dados pessoais.

DESENVOLVIMENTO
Fomentar o desenvolvimento econômico e tecnológico.

PADRONIZAÇÃO DE NORMAS
Estabelecer regras únicas e harmônicas sobre tratamento de dados pessoais, por todos os agentes e controladores que fazem tratamento e coleta de dados.

SEGURANÇA JURÍDICA
Fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo.

FAVORECIMENTO À CONCORRÊNCIA
Promover a concorrência e a livre atividade econômica, inclusive com portabilidade de dados.

DEFINIÇÕES RELEVANTES

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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;

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;

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

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

DEFINIÇÕES RELEVANTES

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem 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;

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).

DIREITOS DO TITULAR

- 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 o disposto na LGPD;

- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD;

- 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.

DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E SUAS COMPETÊNCIAS

- Zelar pela proteção dos dados pessoais, nos termos da legislação;

- Zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º da LGPD;

- Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

- Apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

- Solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento da LGPD;

- Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais;

- Ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E SUAS COMPETÊNCIAS

- Realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

- Comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

- E muitas outras mais...

FISCALIZAÇÃO E SANÇÕES

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

- Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

- Multa diária;

- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;

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

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

- Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

- Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dado.

BASICAMENTE, O QUE A EMPRESA DEVE FAZER?

Due Diligence sobre dados pessoais:
Identificação dos dados (pessoal, sensível, criança, público, anonimizado), departamentos, meios (físico ou digital), operadores internos e externos para mensuração de exposição da empresa à LGPD.

Auditoria sobre o tratamento de dados:
Aderência das 20 atividades de tratamento (art. 5º, X) de dados (coleta, controle, eliminação, etc.) aos princípios gerais previstos no Art. 6º da LGPD, mediante revisão e criação de documentos (contratos, termos, políticas) para uso interno e externo.

Gestão do consentimento e anonimização:
Controle do consentimento e anonimização para atender possível solicitação do titular e da futura agência.

Gestão dos pedidos do titular:
Criação de banco de dados para controle dos pedidos dos titulares dos dados (acesso, confirmação, anonimização, consentimento, portabilidade etc).

BASICAMENTE, O QUE A EMPRESA DEVE FAZER?

Relatório de impacto:
Atendimento à ANPD e demais órgãos do Sistema Nacional de Proteção do Consumidor que poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais.

Segurança dos dados:
Adoção das medidas de segurança da informação aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas.

Governança do tratamento:
Criação de regras de boas práticas e de governança que estabeleçam procedimentos, normas de segurança, ações educativas e mitigação de riscos no tratamento de dados pessoais.

Plano de comunicação – Incidente de segurança:
Comunicação aos órgãos fiscalizatórios (Autoridade Nacional de Proteção de Dados - ANPD, Programa de Proteção e Defesa do Consumidor - Procon, Conselho Administrativo de Defesa Econômica - Cade) e à imprensa sobre incidente de segurança que acarrete risco ou dano.

BASICAMENTE, O QUE A EMPRESA DEVE FAZER?

Validação do término do tratamento:
Adoção das providências necessárias à eliminação dos dados tratados e verificação de eventual conservação dos dados com a elaboração de documentos que evidenciem a eliminação.

Certificação:
Certificação por auditoria especializada das práticas relacionadas à LGPD.

Data Protection Officer (Encarregado):
Identificação do encarregado (Pessoa Física ou Jurídica) e sua capacitação para exercer as atividades previstas na LGPD.

Prevenção de conflitos:
Inclusão de uma cláusula compromissória de mediação vinculada à câmara privada online cadastrada no CNJ (ou similar) para mitigação do contencioso judicial

COMO NÓS ESTAMOS?

- 85% das empresas declararam que não estão prontas para a LGPD (Serasa Experian, 2019);

- 69% dos indivíduos consultados na América Latina dizem estar preocupados com a segurança de seus dados pessoais (Unisys Security Report, 2019);

- O Brasil foi o segundo colocado no aumento do nível de preocupação mundial com segurança de dados de 2018 para 2019 (Unisys Security Report, 2019);

- 43% é a probabilidade, no Brasil, de se enfrentar violações de dados, sendo o mais provável dos países pesquisados (IBM, 2019);

- O impacto financeiro sobre uma empresa que sofre vazamento de dados pode chegar a um custo médio total de US$ 1,24 milhão no Brasil (IBM, 2019).

A LGPD SE APLICA À MINHA EMPRESA?

A LGPD impacta diretamente todos os negócios independentemente do seu tamanho ou do segmento em que atuam - que acessam, coletam ou tratam dados de pessoas físicas, tanto no meio digital quanto no meio físico.

Independe:

- Do setor econômico
- Do tamanho da base de dados
- Se a base de dados é digital ou física

Implica a rotina e práticas de governança de diversos setores do negócio:

- Jurídico
- Tecnologia da Informação
- Contabilidade
- Recursos Humanos
- Marketing
- Comercial
- Compliance

Envolve relações com:

- Clientes
- Prestadores de serviços
- Fornecedores de produtos
- Funcionários, colaboradores, terceirizados
- Parceiros de negócios

INSTRUMENTOS PARA ADEQUAÇÃO

- Assessment para empresas já em operação: submeter a uma avaliação técnica e jurídica que localize os pontos que estão gerando desconformidade à proteção de dados;
- Testes, providências, revisões, auditorias e conformidades técnicas.
- Cláusulas de NDA que prevejam proteção de dados.
- Contratos com fornecedores.
- Contratos com clientes.
- Contratos de RH.
- Capacitação interna de equipe com Código de Conduta.
- Medidas a serem adotadas em caso de vazamento de dados.
- Políticas de privacidade para usuários.
- Políticas tratamento de dados para serem seguidas por terceirizados (integrantes do contrato).
- Termos de uso.
- Manual de Boas práticas e governança em proteção de dados.

PILARES

Jurídico

Consultoria Jurídica
Análise de Privacidade (Situação Atual)
Legislação de Privacidade
Impacto da Privacidade no Negócio
Análise de Contratos, Termos de Consentimento
Treinamentos

Processos

Entrevista com as áreas
Mapeamento dos processos
Mapeamento das aplicações
Mapeamento dos dados pessoais digitais

Tecnologia da Informação

Plataforma Onetrust
Firewall – Segurança de Perímetro
Proteção de Endpoint (Desktop, Notebook e Mobile)
Firewall de Banco de Dados
Firewall de Aplicação – WAF
Cofre de Senhas
Gestão de Acesso
Analise de Vulnerabilidade
Pentest
SOC – Security Operation Center
PSI – Política de Segurança da Informação

www.fecomercio-ce.com.br