INTE
GRI
DADE

PROTEÇÃO
DE DADOS

LGPD NA PRÁTICA
DO PLANEJAMENTO À EXECUÇÃO

O QUE É E QUAL IMPACTO GERA NAS ORGANIZAÇÕES

Pratique integridade, faça a diferença.

ICTS protiviti

FIEMG

1. Introdução

Nos últimos anos, os modelos de negócio têm enxergado o dado pessoal como um ativo de grande potencial econômico e, com isso, os dados têm sido cada vez mais explorados pelas organizações. Assim, a privacidade e a proteção de dados surgiram da necessidade de resguardar os direitos de liberdade, intimidade e privacidade das pessoas.

Não se trata de uma necessidade específica do Brasil, pois a proteção de dados é um movimento mundial que, impulsionado pelo regulamento europeu (GDPR – General Data Protection Regulation), culminou na regulamentação sobre o tema em vários países mundo afora. Por conta desses regulamentos, multas (muitas vezes milionárias) já foram aplicadas por diferentes motivos, tais como vazamento, acessos ou utilização indevida de dados pessoais.

Dessa maneira, vamos entender um pouco sobre essa nova regulamentação e saber como ela pode impactar seus negócios.

2. O que é LGPD?

A Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018 é a lei brasileira que tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento das pessoas.

A LGPD estabelece que toda empresa, independentemente de seu porte, que trate dados pessoais por meio de suas atividades deverá adotar medidas técnicas e administrativas para protegê-los em meio físico ou digital. Para tanto, essa lei define princípios e fundamentos, bem como bases legais que permitem a utilização do dado pelas organizações em harmonia com os direitos dos titulares também estabelecidos na LGPD. Os titulares são as pessoas identificadas ou identificáveis, às quais os dados se referem.

3. Quais os benefícios da LGPD?

A LGPD traz diversos benefícios para o titular, para as organizações e para o Brasil.

Para o titular, o respeito à sua privacidade e a maior segurança no tratamento de seus dados pessoais permitirão uma relação mais transparente e mais adequada junto às organizações.

Para as organizações, a necessidade de adequação à LGPD exigirá que sejam realizados os mapeamentos de todos os seus processos que tratam dados pessoais, promovendo uma análise geral de todas as suas atividades e possibilitando a implementação de melhorias e aumento da eficiência operacional. As organizações que acelerarem o processo de adequação poderão ter vantagens competitivas diante de seus clientes e terceiros, além de um impacto positivo em sua imagem.

Para o Brasil, uma vez que vários países que integram os principais blocos econômicos do mundo já têm regulamentação sobre proteção de dados pessoais, a sua regulamentação agiliza as relações estratégicas e de negócios que envolvam dados pessoais.

4. Como a LGPD impactará as organizações?

A LGPD se baseia em 10 princípios, sendo estes a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização.

Desta maneira, considerando os princípios de segurança e prevenção, as organizações deverão implementar medidas para avaliação e gerenciamento dos riscos a elas relacionados:

Vazamento dos dados pessoais - as organizações terão que adotar medidas protetivas para garantir que não ocorram vazamentos de dados pessoais em seu ambiente.

Tratamento indevido dos dados pessoais - as organizações deverão utilizar os dados pessoais com responsabilidade e transparência, de modo a atender aos princípios e às bases legais estabelecidos na LGPD.

5. Quais são os dados protegidos pela LGPD (art. 5º)?

Dados pessoais são aqueles que identificam ou que permitem identificar uma pessoa, tais como:

NOME SOBRENOME	**CPF RG**	**CARTEIRA DE TRABALHO**
TÍTULO DE ELEITOR	**E-MAIL TELEFONE**	**COOKIES ENDEREÇO IP**

Alguns dados são considerados sensíveis, porque podem, em caso de vazamento, divulgação, utilização indevida etc., gerar situações de discriminação e danos ao titular. Por isso tais dados requerem grande proteção. São eles:

ORIGEM RACIAL OU ÉTNICA	**CONVICÇÃO RELIGIOSA**	**OPINIÃO POLÍTICA**
FILIAÇÃO SINDICATOS/ORGANIZAÇÃO FILOSÓFICA, RELIGIOSA OU POLÍTICA	**SAÚDE OU VIDA SEXUAL**	**GENÉRICO OU BIOMÉTRICO**

6. Quem são os titulares dos dados pessoais?

São as pessoas físicas a quem se referem os dados, sejam clientes, colaboradores, parceiros etc.

- A pessoa é o titular, o detentor dos direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da LGPD.

- É o motivo pelo qual o dado existe, já que, quando não vinculado a uma pessoa física, o dado deixa de ser considerado pessoal.

- É aquele que deve ser informado sobre o uso dos dados e suas finalidades com informações claras, precisas e facilmente acessíveis.

7. O que é "tratamento de dados pessoais" segundo a LGPD (art. 5º)?

São as operações realizadas com os dados pessoais, desde o momento em que eles são coletados até seu armazenamento e destruição. Segundo a LGPD, essas operações consistem em atividades 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.

Por isso devemos avaliar as atividades que realizamos, os dados aos quais temos acesso, os usos para os quais eles são necessários e, quando preciso, ajustar nossas atividades para garantir a proteção dos dados pessoais.

(LGPD, Art. 5º)

8. Quais são os riscos relativos ao tratamento dos dados pessoais?

As organizações devem conhecer suas atividades, assegurar que os dados pessoais sejam utilizados somente para a finalidade devida e, quando necessário, adotar medidas protetivas adicionais para minimizar a exposição aos riscos relacionados ao tratamento.

O tratamento de dados de forma não adequada pode expor os dados pessoais a incidentes de segurança que são capazes de colocar em risco os titulares dos dados e a própria organização. Os riscos são, basicamente:

Vazamento de dados - está relacionado à ausência ou insuficiência de proteção de documentos físicos e arquivos eletrônicos, bem como à comunicação ou transferência de dados (interna ou externa) sem proteção lógica ou segurança adequada etc.

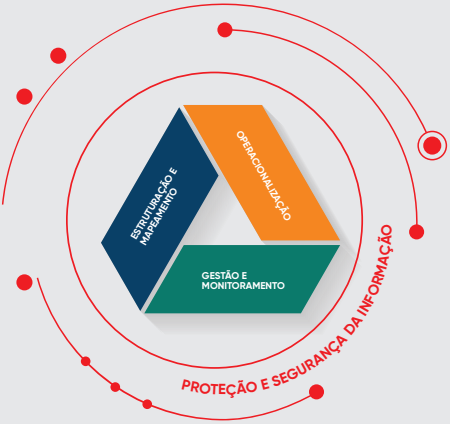
Tratamento indevido de dados - está relacionado à utilização indevida do dado pessoal, ausência ou coleta inadequada de consentimento, utilização desnecessária de dados pessoais etc.

9. Como garantir a proteção dos dados pessoais nas organizações (art. 50)?

Para a implementação da proteção de dados pessoais nas organizações, recomenda-se a estruturação de um Programa de Privacidade e Proteção de Dados, que deverá envolver três setores fundamentais: Tecnologia, Jurídico e Processos/Gestão.

O Programa de Privacidade e Proteção de Dados tem como objetivo estabelecer boas práticas de governança que estruturem a organização para atendimento aos princípios e fundamentos estabelecidos na LGPD, bem como aos requisitos de segurança, às solicitações de titulares e às ações educativas direcionadas aos colaboradores e parceiros.

As ações para estabelecimento do Programa de Privacidade iniciam-se com a Estruturação e Mapeamento dos processos com fluxos de dados pessoais, além da elaboração de Políticas de Privacidade e Proteção de Dados. Na sequência, a Operacionalização instrumentaliza a organização para atender ao direito dos titulares de dados, avaliar impacto, assim como gerir incidentes, terceiros e consentimentos. Então, a Gestão e o Monitoramento prosseguem com o ciclo de planejamento, ação, avaliação contínuos, garantindo o tratamento adequado e seguro dos dados pessoais.



10. Como as organizações podem se preparar para atender a LGPD?

Entenda como a LGPD afeta o seu negócio – conhecer a LGPD, os conceitos e exigências nela estabelecidos e entender os impactos nas organizações e nos seus negócios.

Conscientize e engaje sua organização – orientar e instruir a alta administração, os colaborados e os terceiros sobre as obrigações estabelecidas na LGPD. Os riscos e os impactos do tratamento de dados pessoais, com a finalidade de adequação dos processos às exigências da lei e à criação de cultura de proteção de dados e privacidade nas organizações, devem, da mesma forma, ser abordados.

Avalie o seu nível de adequação - entender o nível de adequação em que a organização se encontra é o primeiro passo para definir um plano consistente de adequação.

Defina seu plano de ação – estruturar um plano para adequação e manutenção das ações necessárias para atendimento à LGPD é fundamental para a sustentabilidade no longo prazo. Esse plano deve conter ações estruturantes, que são necessárias para manter de maneira ampla o programa, tais como o Estabelecimento de canal de atendimento dos titulares de dados (pessoa física), as Medidas de proteção e segurança física e cibernética, a Nomeação de um encarregado (DPO) e o Estabelecimento de uma política de privacidade e proteção de dados pessoais. Além disso, são necessárias ações específicas e direcionadas para áreas e posições que tratam dados pessoais, tais como a adequação de contratos/cláusulas contratuais junto a colabores e terceiros, a segregação de acessos a dados pessoais e a aplicação de controles em atividades críticas.

Coloque as ações em prática – implantar o plano de ação estruturado na etapa anterior, estabelecendo prazos e responsáveis para colocar as ações definidas em prática. Para isso será necessário engajar não apenas os responsáveis pela execução das ações, mas todas

as pessoas da organização: desde a alta administração (responsável pelo patrocínio do programa) até todas as áreas de negócios (responsáveis por implantar os controles e comunicar mudanças nas atividades de tratamento de dados pessoais).

Sustentação do programa – garantir a manutenção do Programa de Privacidade e Proteção de Dados, proporcionando o atendimento aos direitos dos titulares e reduzindo riscos relacionados ao tratamento indevido e vazamento de dados pessoais. Para isso, é importante que a empresa tenha definido uma matriz de responsabilidades, por exemplo, a matriz RACI (Responsável, Autoridade, Consultado e Informado).

Sobre a ICTS Protiviti

A ICTS Protiviti é uma empresa brasileira que combina a segurança, eficiência e independência da plataforma tecnológica de serviços especializados da ICTS (canal de denúncias, diligência de terceiros, monitoramento de fraudes e de comportamentos antiéticos e treinamentos on-line) com o alcance global e o conhecimento e inovação em gestão de riscos, compliance, auditoria interna, investigação e proteção e privacidade de dados da Protiviti. A união de especialidade com capacidade de transformação e excelência operacional proporciona aos seus clientes um portfólio abrangente de soluções que endereçam os principais riscos, problemas e desafios de negócio, protegendo e maximizando o valor das organizações e ajudando seus líderes a encararem o futuro com confiança e alcançarem resultados extraordinários num mundo dinâmico. Reconhecida como Empresa Pró-Ética desde 2015, conta no Brasil com aproximadamente 400 profissionais em 4 escritórios – São Paulo, Barueri/Alphaville, Rio de Janeiro e Belo Horizonte – que atendem cerca de 600 empresas de diferentes portes e segmentos. No mundo, são mais de 4.500 profissionais atuando por meio de uma rede de subsidiárias e firmas-membro independentes. Empresa reconhecida como Great Place to Work e com faturamento anual superior a USD 1 bilhão, opera 85 escritórios em 27 países, que atendem a 60% das empresas da FORTUNE 1000®.

Sobre a FIEMG

A Federação das Indústrias do Estado de Minas Gerais (FIEMG) representa o setor industrial do estado de Minas Gerais e atua na defesa de seus interesses locais e nacionais. A instituição oferece às empresas mineiras assessoria e apoio em áreas vitais, como crédito e financiamento, tributária, meio ambiente e trabalhista. A FIEMG trabalha para que a indústria mineira se torne cada vez mais competitiva, inovadora e sustentável, capaz de gerar novos negócios, riqueza e desenvolvimento. Uma indústria que se destaque no Brasil e no exterior, e que seja o motor para o crescimento econômico e social de todo o estado de Minas Gerais. É por meio de suas áreas de negócios e das entidades que a compõem que a FIEMG atende as demandas da indústria e da sociedade. Fazem parte da composição

da federação as seguintes entidades: Centro Industrial e Empresarial de Minas Gerais (CIEMG), Serviço Social da Indústria (SESI), Serviço Nacional de Aprendizagem Industrial (SENAI) e Instituto Euvaldo Lodi (IEL). Juntas, essas empresas oferecem à indústria mineira estratégias para o desenvolvimento industrial e formação da força de trabalho, inclusive preparando novas gerações para a indústria do futuro.

Autores

André Bottecchia Cilurzo é Diretor Associado da ICTS Protiviti, onde trabalha desde 2002, atuando em projetos de Privacidade de Dados, Cibersegurança, Prevenção de Perdas e Gestão de Riscos em diversas indústrias, tais como bens de consumo, bancos e varejo. É formado em Administração pela EAESP-FGV, com pós-graduação em Business Economics pela EESP-FGV.
Áreas de conhecimento especializado
Privacidade de Dados / Segurança de Informações / Redução de riscos de negócios
Prevenção de perdas e fraudes / Inteligência preventiva

Ana Paula Bicalho Brandão é Gerente de Proteção de Dados da FIEMG, onde trabalha desde 2003, atuando na Gestão de Pessoas e de Projetos, com foco em melhoria constante de processos. Membro da ANPPD® - Associação Nacional dos Profissionais de Privacidade de Dados, formada em Tecnologia da Informação e pós-graduada em Gestão de Pessoas e Gestão de Projetos.

Marcos Roberto Oliveira de Souza é Advogado de Proteção de Dados e Privacidade da FIEMG, membro da ANPPD® - Associação Nacional dos Profissionais de Privacidade de Dados, membro da Comissão de Proteção de Dados da OAB/MG e especialista em Direito Público pela PUC Minas. MBA em Proteção de Dados no CEDIN (em curso). Atuou como auditor e gestor nas áreas de corregedoria e compliance no serviço público estadual e como gestor na área de ciência da informação no setor privado.

Referências

LEI N° 13.709, DE 14 DE AGOSTO DE 2018

protiviti.com.br

fiemg.com.br