COMO SE ADEQUAR À LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

GOUVÊA ADVOCACIA CONSULTORIA

Workplan GROUP

O que é a Lei geral de proteção de dados?

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet, sua vigência terá início a partir de agosto de 2020.

Qual a finalidade desta lei?

A lei tem como principal objetivo **garantir a privacidade de dados pessoais das pessoas.**

Através de um maior controle e transparência sobre a utilização destes dados a lei objetiva garantir direitos fundamentais relacionados à proteção da liberdade, privacidade e intimidade das pessoas.

A quem se aplica?

A qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

a) A operação de tratamento seja realizada no território nacional;

b) A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

c) Os dados pessoais objeto do tratamento tenha sido coletados no território nacional.

A lei estabelece que são considerados coletados no território nacional os dados pessoais **cujo titular nele se encontre no momento da coleta.**

Extraterritorialidade

A LGPD segue os princípios de extraterritorialidade. Assim, será aplicada para as empresas estrangeiras que tratem dados pessoais, com finalidade comercial, de indivíduos localizados em território nacional no momento da coleta.

O que são dados pessoais?

De acordo com a LGPD dados pessoais é toda informação relacionada a uma pessoa natural identificada ou identificável, ou seja qualquer informação que possa identificá-la, como nome, RG (registro geral), CPF (cadastro de pessoa física), gênero data e local de nascimento, telefone, endereço residencial, retrato em fotografia, localização via GPS entre outros.

O que são Dados pessoais sensíveis?

São aqueles que possuem um poder maior de causar dano ou discriminação ao cidadão. São taxativos e definidos pela lei: 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.

O que é tratamento de dados?

Tratamento é toda operação realizada com dados pessoais, como as que se referem 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;

Como realizar o tratamento de Dados Pessoais de Crianças e de Adolescentes?

Deverá ser realizado em seu melhor interesse, através de termo com consentimento de uso específico e com a garantia de que um dos responsáveis autorizou o tratamento dos dados.

As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Poderão ser coletados dados pessoais de crianças sem o termo de consentimento uma única vez e quando a coleta for necessária para contatar os pais ou o responsável legal, sem que haja o seu armazenamento.

Quem são os agentes de tratamento de dados:

Controlador: O texto define o controlador como uma pessoa natural ou jurídica, de direito público (governo) ou privado (empresa), a quem compete às decisões referentes ao tratamento de dados pessoais natural.

Operador: pode ser uma pessoa natural ou jurídica, de direito público ou privado, mas com uma diferença: ele realiza o tratamento de dados pessoais em nome do controlador.

Quem é o DPO (DPO- Data Protection Officer) ou Encarregado de proteção de dados?

É a pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de proteção de Dados (ANPD).

O que é titular dos dados e quais os seus direitos?

Titular de dados: informação relacionada a pessoa natural identificada ou identificável"

Direitos: Os titulares poderão requerer ao controlador:

a) **Confirmação da existência de tratamento e acesso**: Solicitar ao controlador informações sobre a existência do Direito de solicitar e acessar os dados pessoais coletados e tratados pelo controlador.

b) **Correção de dados incompletos, inexatos ou desatualizados:** Direito de requerer a correção de dados incompletos, inexatos ou desatualizados.

c) **Anonimização**, **bloqueio ou eliminação de dados desnecessários**, excessivos ou tratados em desconformidade com a lei de proteção de dados.

d) **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;

e) **Eliminação dos dados pessoais** tratados com o consentimento do titular, exceto disposição legal/ contratual diversa.

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

g) **Informação sobre a possibilidade de não fornecer consentimento** e sobre as consequências da negativa;

h) **Revogação do consentimento**: Direito de manifestar, por procedimento gratuito e facilitado, a revogação do seu consentimento em relação ao tratamento de seus dados pessoais.

i) **Oposição:** Direito de se opor ao tratamento de seus dados pessoais quando realizado em descumprimento à LGPD.

j) **Decisões automatizadas:** direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

k) **Reclamação à autoridade Nacional**

Relatório de Impacto

É a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

O que deve conter?

O relatório de impacto deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Violação De Dados

Em que pese a LGP não traga sua definição, vale lembrar que a nossa legislação foi adaptada à GDPR legislação Europeia que traz a dispõe: "violação de dados pessoais" (incidente de segurança), como: *"(...) uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento (...)".*

ANPD AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A Autoridade Nacional de Proteção de Dados, atuará para:

- Zelar pela proteção dos dados pessoais.
- Editar normas e procedimentos.

- Decidir sobre a interpretação da LGPD, inclusive sobre casos omissos. Requisitar informações às empresas que realizam tratamento de dados. Implementar mecanismos para o registro de reclamações.
- Fiscalizar e aplicar sanções.

Das Sanções Administrativas

Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

a) Advertência, com indicação de prazo para adoção de medidas corretivas;

b) 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;

c) Multa diária, observado o limite total a que se refere o inciso II;

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

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

f) Eliminação dos dados pessoais a que se refere a infração;

g) 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;

h) 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;

i) Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

ADEQUAÇÃO A LGPD

Após as orientações acerca dos principais pontos trazidos pela Lei Geral de Proteção de Dados, entre eles, **suas sanções**, que dependendo da violação ocorrida poderá comprometer o funcionamento parcial ou total do exercício de atividades relacionadas a tratamento de dados, o que em alguns casos implicará no funcionamento do negócio.

O ideal é que as empresas, **SEM EXCEÇÃO**, de acordo com a sua estrutura, se adeque antes do início de sua vigência em agosto de 2020.

Daremos algumas sugestões:

1. Efetuar análise de todos os procedimentos realizados pela empresa em seus negócios com o intuito de verificarem como os dados pessoais são tratados.

   Como são tratados os dados sensíveis? Estão de acordo com a finalidade para que foram coletados? Há consentimento de uso pelo titular?

2. Realizar um "*data mapping*", ou seja, um mapeamento de dados, incluindo todas as pessoas envolvidas no tratamento, seja funcionários, colaboradores ou terceiros.

3. Preparar as pessoas envolvidas no negócio de maneira eficaz para a proteção de dados pessoais, conscientizando da importância no tratamento destes dados e lembrando-as que são de propriedade de seus "titulares".

4. Elaborar ou ajustar o Regulamento Interno da empresa, ou Política de privacidade , bem como gerenciar o compromisso dos envolvidos com um documento assinado por todos (funcionários e terceiros), seja por meio de contrato (digital ou físico) ou recebimento de uma via da política de privacidade que deverá conter as sanções para caso de descumprimento.

5. Empresas com atuações em nível global devem adotar políticas de transferência de dados atribuindo as condições e regras para o tratamento.

6. Para atender aos titulares dos dados as empresas devem adotar um plano de solicitações, retificações e reclamações, deixar em evidência quem será o DPO ou encarregado para os esclarecimentos.
7. Realizar relatórios de impacto
8. Realize auditoria interna
9. Mantenha um programa constante de treinamento, orientações para que todos os envolvidos na operação da empresa estejam sempre atualizados
10. Mantenha uma política de coockies de forma transparente e contrate empresas de marketing que estejam preparadas para a legislação.

Caso, ainda, entenda que não há razões para preocupar-se, **FIQUE ATENTO!!**

1. **Sua empresa terceiriza a folha de pagamento dos funcionários?**

   O BPO (**Business Process Outsourcing**) - Terceirização de Processo de Negócios é uma prática comum adotada pela maioria das empresas para o processamento da folha de pagamento dos funcionários.

   Então, **os dados pessoais** são transferidos aos cuidados de terceiros.

   Portanto, certifique-se de que os envolvidos no processo estejam adequados a LGPD, **tanto tecnicamente, quando juridicamente.**

2. **O seu segmento é na área de saúde?**

   Cautela!! A vulnerabilidade em um arquivo físico ou digital poderá trazer riscos de violação de dados sensíveis.

3. **É do ramo Educacional?**

   Como estão armazenadas informações de seus alunos? Quem tem acesso? Há autorização dos pais? De que forma?

4. **Escritórios Contábeis?**

   O Escritório ou os seus funcionários já estão preparados para a lei? Já possui um Data Loss Prevention (DLP), "prevenção a perda de dados/violações". Em caso de arquivos físicos, como estão protegidos? Como é a Política de Governança na proteção de dados pessoais?

ADEQUEM-SE!!

Procurem profissionais com conhecimentos técnicos em Segurança da Informação e Jurídicos de modo que a empresa esteja em Compliance (conformidade) com as normas, regulamentos, leis e Políticas de Privacidade na proteção de dados pessoais.

Adriana Gouvêa, advogada, com expertise em Direito Empresarial, Contratos e certificada internacionalmente pela EXIN como **DPO (Data Protection Officer)**, Privacy and Data Protection Essentials, Privacy and Data Protection Foundation, ***Privacy and Data Protection Practitioner***, ISO 27001 Foundation, experiência em consultoria, treinamento, adequação e implantação GDPR e LGPD.

Contato:

adriana@gouveaadvocaciaconsultoria.com.br | 11 5087-8837 | 11 9 8220-4387

Workplan é uma consultoria especializada em soluções integradas de saúde, benefícios corporativos e segurança do trabalho atuando diretamente com o setor de Recursos Humanos em busca de resultados, eficiência e alcance das metas propostas.

Elaboramos um conjunto de ações para a correta implantação dos processos internos relacionados à nova LGPD com a eficiência e eficácia necessárias.

Contato:

contato@workplanbrasil.com.br | 11 2737.1964 |11 9.8291.7070 | 11 99307-2300

LGPD PORTAL BRASIL

Contato:

www.lgpdportalbrasil.com.br | contato@lgpdportalbrasil.com.br

---

Fonte: Lei nº 13.709/18 – Lei Geral de proteção de Dados