



CRIANDO CULTURA DE PRIVACIDADE E PROTEÇÃO DE DADOS

SOB O OLHAR DA LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

APRESENTAÇÃO

A entrada em vigor da Lei Geral de Proteção de Dados - LGPD, cria uma gama de responsabilidades para todos os tratamentos de dados pessoais, sejam eles realizados por pessoas físicas ou pessoas jurídicas.

Desta forma, se torna eminente a adequação de todos os meios de tratamentos de dados pessoais para o que é observado na lei, seus princípios, suas bases legais e os direitos adquiridos pelos titulares dos dados.

Esta cartilha tem como objetivo o repasse de conhecimentos, informações e interpretações dos autores sobre a Lei Geral de Proteção de Dados - LGPD, bem como a sua relação no tratamento de dados pessoais nas empresas.

Esperamos que as informações aqui contidas despertem a luz que guiará o caminho de todos a um melhor tratamento e respeito no que diz a lei.

1 - LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (lei nº 13.709/2018), criada em 2018 no Brasil, tem como objetivo regular o tratamento dos dados pessoais de cidadãos brasileiros, seja na sua forma física (documentos impressos) ou digital (sistemas ou documentos eletrônicos).

Após sua criação em 2018, determinou-se que todas as empresas ou pessoas físicas que tratam dados pessoais, teriam um período de 02 anos para realização da adequação do tratamento com a lei, observando seus princípios, bases legais e itens relacionados às tratativas de dados.

Com as discussões e reviravoltas sobre a sua vigência, no dia 18/09/2020 a lei entrou em vigor, porém sem a possibilidade de aplicação das sanções disciplinares previstas nos Artigos 52, 53 e 54, visto que a vigência sobre a aplicação destas medidas foi alterada para iniciar apenas no dia 01 de agosto de 2021, por meio da lei nº 14.010/2020.

Entretanto, a partir da sua vigência, a necessidade de adequação aos tratamentos é imediata, uma vez que os titulares dos dados já podem exercer seus direitos, inclusive com abertura de processo ou acionamento a outros órgãos fiscalizadores.

Para o melhor entendimento da lei e suas tratativas, considera-se (Art. 5):

Dado Pessoal: Informação relacionada a pessoa natural identificada ou identificável;

Dado Pessoal Identificado: Um dado pessoal no qual é possível identificar de maneira direta uma pessoa natural (exemplo: CPF, RG, Biometria);

Dado Pessoal Identificável: Um dado pessoal no qual é possível identificar uma pessoa natural de maneira indireta (exemplo: Endereço, Placa de Carro, Número de Telefone);

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;

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;

ANPD - Autoridade Nacional de Proteção de Dados: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

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

Encarregado de Dados: 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);

Tratamento de Dados Pessoais: O tratamento de dados pessoais é toda e qualquer operação realizada com um dado pessoal, incluindo a sua própria coleta, seu armazenamento e também o descarte.

2 - A QUEM SE APLICA

Conforme descrito nos Art. 3º da lei, a LGPD 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 operação de tratamento seja realizada no território nacional;
- 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;
- os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

Desta forma, é preciso observar que a LGPD se aplica também em empresas estrangeiras que realizam o tratamento conforme itens supracitados, mesmo que os dados sejam armazenados fora do território nacional.

3 - OS SUJEITOS E RESPONSABILIDADES

Na observância da lei podemos avaliar que, nos tratamentos de dados realizados, existem alguns sujeitos relacionados que irão possuir responsabilidades específicas de acordo com a legislação. São sujeitos da lei:

Titular: Conforme já mencionado, o titular é aquele que detém e repassa os dados pessoais, considerado o dono dos dados pessoais produzidos e manipulados.

Principais Direitos: Como o principal objetivo da lei é proteger e tratar de maneira adequada os dados pessoais dos titulares, este sujeito possui alguns direitos específicos, conforme pode ser visto no item 6 desta cartilha.

Controlador: O controlador é o primeiro responsável pelo tratamento de dados pessoais. Geralmente é o sujeito que coleta e trata os dados e, por isso, este sujeito tem

responsabilidades específica para com a lei. Em caso de sanções ou investigações, este sujeito será o principal responsabilizado, cabendo a ele o ônus da prova, quando necessário.

Principais Responsabilidades: O controlador tem o dever de regular todo o tratamento de dados pessoais da sua competência, criando regras, processos, treinamentos e quaisquer dispositivos necessários para que os dados dos titulares em seu poder estejam sendo tratados de acordo com a lei. É dele a responsabilidade por fornecer regras de tratamento claras ao operador, eleger um encarregado de dados de forma obrigatória, bem como responder em caso de violações sobre o tratamento de dados pessoais.

Operador: É o sujeito que opera dados em prol de um controlador. Este sujeito possui basicamente as mesmas responsabilidades do controlador no que tange ao tratamento de dados, não podendo ser omissos em caso de violações. No entanto, o operador deve seguir as regras de um controlador, devidamente estipuladas e repassadas por ele e não possui obrigatoriedade inicial de eleição de um encarregado de dados (salvo exceções).

Principais Responsabilidades: Tratar os dados pessoais do controlador de acordo com as regras repassadas pelo mesmo, oferecendo os mecanismos necessários para os dados dos titulares sejam tratados de acordo com a lei.

Encarregado de Dados: O encarregado de dados pessoais é um papel/função, elegido pelo controlador ou pelo operador, o qual deve ter o nome e contato divulgados no site da empresa.

Principais Responsabilidades: Tem como responsabilidade a garantia dos tratamentos de dados nos agentes de tratamento, bem como servir como principal ponto de contato com a ANPD e com o Titular.

ANPD: É a Autoridade Nacional de Dados, o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Principais Objetivos: Fiscalizar o tratamento de dados realizados pelos agentes de tratamento, bem como servir de ponto de coleta de denúncias e sobre a garantia dos direitos dos titulares perante ao tratamento de dados.

4 - OS PRINCÍPIOS

A partir da vigência da lei todo o tratamento de dados pessoais deve observar 10 princípios, os quais servem para proteger e garantir sobretudo o tratamento adequado dos dados dos titulares, bem como sua proteção e transparência.

Deste modo, como é possível verificar no Art. 6º da lei, para que seja possível tratar dados pessoais a partir de então, se torna obrigatório que cada tratamento (considera-se tratamento desde a coleta do dado até a sua eliminação) obedeça todos os princípios previstos, conforme abaixo:

Finalidade: Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

Livre Acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

Qualidade dos Dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

Segurança: 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;

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.



Finalidade:
Propósitos legítimos
específicos e
explícitos



Adequação:
Compatível com
as finalidades



Necessidade:
Utilizar apenas
Os dados
necessários



Livre acesso:
Acesso ao
tratamento e à
integralidade dos
dados



Qualidade:
Dados claros,
exatos, atualizados
e relevantes.



Transparência:
Dados claros e
precisos ao titular



Segurança:
Processos e técnicas
para proteção de
dados



Prevenção:
Adoção de
medidas para
mitigar danos ao
titular



Não discriminação:
Não utilizar de
dados para fins
discriminatórios



**Responsabilização e
prestação de contas:**
Prestar contas do
cumprimento da
legislação

5 - AS BASES LEGAIS

A lei também é clara quando informa que a partir da sua vigência, todo o tratamento de dados pessoais, além de observar os princípios mencionados no item 4, deve possuir um base legal para tratamento dos dados.

Portanto, em seu Art. 7º, a lei informa 10 bases legais na qual os dados podem ser tratados. Caso não exista uma base legal vinculada ao tratamento dos dados pessoais, a partir da vigência da lei, eles não poderão mais ser tratados.

Deste modo, observa-se como opções para tratamento as seguintes bases legais:

Consentimento: Quando o titular fornece seu consentimento para a tratativa dos seus dados pessoais. Apesar de parecer simples, essa é uma das bases legais mais complexas, visto que o titular pode negar-se a fornecer consentimento e revogá-lo a qualquer momento;

Cumprimento de Obrigação Legal: Quando existir uma outra lei que solicite que os agentes de tratamento façam a devida tratativa (geralmente armazenamento) dos dados pessoais, sempre observando que apenas os dados necessários e pelo período determinado descritos na lei em questão podem ser tratados;

Estudo de órgão de Pesquisa: para a realização de estudos exclusivo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

Exercício Regular de Direitos: para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307/1996;

Tutela da Saúde: para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

Execução de Políticas Públicas: 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 contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da lei;

Execução de Contrato: 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;

Proteção à Vida: para a proteção da vida ou da incolumidade física do titular ou de terceiro;

Proteção ao Crédito: para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente;

Interesse Legítimo: 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;



No caso do tratamento de dados sensíveis, a lei informa em seu Art. 11º e Art. 12º que o tratamento dos dados pessoais só se darão em 7 bases legais existentes. São elas: O Consentimento, Estudo por órgão de pesquisa, Proteção da Saúde, Prevenção a Fraude e a Segurança do Titular, Execução de Políticas Públicas, Proteção da vida, Exercício regular de direitos e Cumprimento de obrigação legal.

6 - OS DIREITOS DOS TITULARES

Em observância com o Art. 18 da lei, que tem em sua essência apoiar que o titular se empodere de seus dados pessoais, a LGPD fornece alguns direitos que os titulares dos dados pessoais poderão exercer perante a seus controladores e operadores.

Desta forma, é necessário que todo controlador e operador de dados, ao realizar o tratamento, garanta que os direitos dos titulares possam ser exercidos, conforme descrito abaixo:

Confirmação do Tratamento: Direito de acionar os agentes de tratamento para confirmar se existe tratamento de seus dados pessoais;

Acesso aos Dados: O titular tem a garantia de ter acesso aos seus dados que são tratados por um agente de tratamento;

Correção de Dados: O direito de pedir a correção de dados incompletos, inexatos ou desatualizados;

Eliminação de Dados: Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no Art. 16º da Lei;

Eliminação de Dados Excessivos: Direito de solicitar anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

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

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

Informações de Consentimento: Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

Revogação do Consentimento: O direito a revogação do consentimento que foi realizado, caso esta seja a base legal utilizada para o tratamento;

Acionamento aos Agentes e a ANPD: O titular possui o direito de acionar qualquer agente de tratamento sobre as questões supracitadas, mediante a figura do Encarregado de Dados, bem como realizar reclamação a Autoridade Nacional caso for necessário;

Oposição ao tratamento: Poderá se opor ao tratamento de seus dados quando julgar que o tratamento é incorreto ou ilegal.

7 - A SEGURANÇA DOS DADOS

A existência de um capítulo específico na lei para questões de segurança dos dados (Capítulo VII), remete que a proteção dos dados pessoais dos titulares que são confiados aos agentes de tratamento de dados deve ser muito observada.

Portanto, cabe aos agentes de tratamentos a adoção de medidas técnicas e administrativas para proteger os dados pessoais que estão sendo tratados em nome do titular dos dados, principalmente para evitar vazamento de dados ou possíveis acessos não autorizados.

Neste ponto, é importante observar os seguintes artigos da lei:

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Além desses itens, no Art. 48º da lei, é informado que o controlador de dados deve comunicar à ANPD e aos titulares dos dados quaisquer ocorrências de incidentes de segurança envolvendo dados pessoais que possam acarretar em riscos ou danos relevante aos titulares. Esta comunicação é obrigatória, e deverá ser realizada com o repasse das seguintes informações:

- Descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos;
- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata; e
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Por esses e outros motivos, é muito importante que todos os agentes de tratamentos possuam avaliações periódicas de segurança e proteção de dados pessoais, com a devida observância de padrões mínimos de segurança na manipulação física ou digital dos dados, bem como a atuação nas frentes de Pessoas, Processos e Tecnologias, conforme pode ser visto na imagem abaixo:



8 - A RELAÇÃO COM O MEIO EMPRESARIAL

Entendido de maneira simples e objetiva o que envolve a LGPD, a pergunta que fica é, qual a relação desta lei com as empresas?

Tendo nossas empresas diversas bases de dados pessoais, estes dados pessoais, assim como todos os outros, também são regidos pela lei.

Deste modo, se faz necessária que a Cultura de Privacidade também recaia sobre o meio empresarial, sendo que cada empresa terá o dever de realizar a adequação de seus tratamentos de dados pessoais em observância com a lei.

Isso quer dizer que a empresa será prejudicada?

A nossa interpretação sobre esta pergunta é absolutamente não! Assim como a evolução realizada ao longo dos anos, processos e até mesmo a própria informatização, assim será com a adequação a tratativa correta de dados pessoais.

9 - A ADEQUAÇÃO MÍNIMA DAS EMPRESAS

Observando os conceitos da lei e a sua relação com as empresas, elencamos abaixo uma série de medidas e dicas para que as empresas realizem a devida adequação sobre o tratamento de dados pessoais, preservando sua essência, mas também fazendo com que a adequação seja realizada:

1 - Criação de um Comitê de Privacidade: Acreditamos que a primeira ação para o tratamento de dados seja adequação é a criação de uma comissão formal. É muito importante que esta comissão seja envolvida ativamente nos processos de adequação e que seja formada por pessoas que tratam dados físicos e digitais, profissionais de informática e também do âmbito Jurídico;

2 - A escolha das bases legais: Um assunto muito importante para a lei e também para o tratamento correto das adequações dentro da empresa será a escolha das bases legais. Cada tratamento de dados terá que ser vinculado a uma ou mais bases legais específicas, conforme o documento de registro de tratamento. Se porventura, não existir base legal para tratamento dos dados, estes dados pessoais não devem ser tratados.

3 - Dados pessoais sensíveis: Perante a lei, os dados pessoais sensíveis só podem ser tratados em oito bases legais aplicáveis, por isso é recomendado que os tratamentos destes dados sejam separados dos demais, a fim de observar os tratamentos corretos;

4 - Criação de Políticas de Privacidade: Observando o princípio da transparência previsto em lei, é obrigação das empresas a criação de documentos de Política de Privacidade, os quais servirão para informar aos titulares o que é feito com seus dados que são entregues aos controladores, se são compartilhados, consultados ou transferidos.

5 - Aviso de Cookies: Caso a sua empresa possua coleta de cookies nos sites, é necessário adicionar um aviso e permitir que o titular realize gerenciamento dos cookies que são coletados. A equipe de TI deve ser acionada para avaliação do aviso e controle;

6 - Tratamento com fornecedores: É importante também avaliar bem quem são os fornecedores, terceiros e operadores que realizam tratamento de dados em nome da sua empresa. Para estes, é necessário enviar um checklist de perguntas aferindo a adequação da LGPD e até mesmo a revisão das cláusulas de contrato para adição de aditivos relacionados caso for necessário;

7 - Relatório de Impacto: Ao realizar os registros de tratamento e evidenciar tratamentos de alto risco, principalmente ligado a base legal de interesse legítimo, é importante realizar um relatório de impacto anterior ao tratamento, para que possa ser apresentado a autoridade nacional, caso for necessário;

8 - Resposta a incidentes: Por fim, a lei prevê que todo o vazamento de dados ou incidentes de segurança que envolvam dados pessoais, tenham uma comunicação aos titulares e a ANPD, por isso, é necessário utilizar o modelo com os itens previstos na lei, caso ocorra.



CRIANDO CULTURA DE PRIVACIDADE E PROTEÇÃO DE DADOS
DECLARO QUE RECEBI DE UMA VIA DESTA CARTILHA EM FORMATO DIGITAL

- 1 –
- 2 –
- 3 –
- 4 –
- 5 –
- 6 –
- 7 –
- 8 –
- 9 –
- 10 –
- 11 –
- 12 –
- 13 –
- 14 –
- 15 –