SUMÁRIO

1. INTRODUÇÃO

LEI Nº 13.709

A aprovação da Lei Geral de Proteção de Dados, aprovada em 14 de agosto de 2018, e com vigência a partir de agosto de 2020, marcou o início de uma nova cultura tanto no setor privado como setor público: uma cultura de transparência centrada na pessoa física, na minimização do impacto e no aumento da segurança aplicada ao tratamento dos dados pessoais.

A legislação brasileira em vigor se fundamenta em diversos valores, como o respeito à privacidade, à liberdade de expressão, e aos direitos humanos de liberdade e dignidade das pessoas.

Dentro desse contexto de preocupação crescente com a proteção de dados pessoais no Brasil e para se adequar aos requisitos exigidos na lei, a Administradora desenvolveu este manual, para que de forma objetiva e simplificada, possa apresentar aos seus colaboradores e parceiros, as principais informações sobre a LGPD, com o objetivo de avaliar sua forma de atuação, planejar mudanças e adequações.

2. OBJETIVOS

A Lei Geral de Proteção de Dados Pessoais (LGPD) 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. Trata-se de uma normativa com características extraterritoriais, de interesse nacional, que deve ser observada pela União, Estados, Distrito Federal e Município, visando garantir maior segurança em relação aos dados pessoais que podem ser coletados e tratados no Brasil de maneira legítima e segura.

3. FUNDAMENTOS

A disciplina da proteção de dados pessoais tem como fundamentos:

I - Respeito à privacidade;

II - Autodeterminação informativa;

III - Liberdade de expressão, de informação, de comunicação e de opinião;

IV - Inviolabilidade da intimidade, da honra e da imagem;

V - Desenvolvimento econômico e tecnológico, e a inovação;

VI - Livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII – Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

4. ABRANGÊNCIA

A LGPD atinge todos os setores da economia e todas as empresas, independentemente do porte.

Assim, qualquer operação de tratamento de dados pessoais realizada no território nacional, por pessoa natural ou pessoa jurídica de direito público ou privado, cujos titulares estejam localizados no Brasil, ou que tenha por finalidade a oferta de produtos ou serviços no Brasil, estão sujeitos à LGPD, que passa a exigir o consentimento expresso do usuário para esta operação.

A responsabilidade de cumprir a Lei se estende a todos que lidam com a informação, inclusive subcontratantes como fornecedores e seus parceiros.

As únicas exceções à aplicação da Lei são as hipóteses de tratamento de dados pessoais realizado por pessoa natural, para fins exclusivamente particulares e não econômicos;

Além daqueles realizados exclusivamente para fins:

I. Jornalístico, artístico ou acadêmico (neste caso, não se dispensa o consentimento);

II. De segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; e

III. Dados em trânsito, ou seja, aqueles que não tem como destino Agentes de Tratamento no Brasil.

5. PRINCIPAIS CONCEITOS

Para os fins desta Lei, considera-se:

I - Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - 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;

III - Dado Anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - Banco de Dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

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

VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

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

VIII – 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);

IX - Agentes de Tratamento: o controlador e o operador;

X - Tratamento: 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;

XI - Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

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

XIII - Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

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

XV - Uso Compartilhado de Dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados (na Lei está apresentada no inciso XVI);

XVI - Relatório de Impacto à Proteção de Dados Pessoais: 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 (na lei está apresentada no inciso XVII);

XVII - Autoridade Nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (na lei está apresentada no inciso XIX).

6. PRINCÍPIOS PARA O TRATAMENTO DE DADOS

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - Finalidade: Considerado um dos mais relevantes para a interpretação da lei, pois não será mais possível tratar dados pessoais com finalidades genéricas ou indeterminadas. O tratamento de cada informação pessoal deve ser feito para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - Adequação: Esse princípio exige que haja compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - Necessidade: O tratamento de dados deve ser limitado 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. De acordo com esse princípio, não é possível coletar dados sem uma finalidade específica, apenas com a justificativa de que eles poderão ser úteis no futuro;

IV - 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. De acordo com esse princípio, a pessoa física titular dos dados tem o direito de consultar, todos os dados que a empresa detenha a seu respeito. Além disso, devem ser especificadas questões como: o que a empresa faz com as suas informações, de que forma o tratamento é realizado e por quanto tempo.

V - Qualidade dos Dados: Nesse princípio é exigido 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;

VI - Transparência: Esse princípio garante aos titulares, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. Além disso, a Administradora não pode compartilhar dados pessoais com terceiros, inclusive com operadores que sejam essenciais para a execução do serviço, sem que o titular tenha conhecimento;

VII - Segurança: É de responsabilidade da Administradora a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, como nos casos de invasões por hackers, e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - Prevenção: Esse princípio se refere a adoção de medidas prévias para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - Não Discriminação: Este princípio se refere a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivo, e busca assegurar que os dados pessoais não serão usados para finalidades que envolvam segregação social, racial ou de gêneros;

X - Responsabilização e Prestação de Contas: O princípio da responsabilização e prestação de contas envolve 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.

7. TRATAMENTO DE DADOS

7.1. Tratamento de Dados Pessoais

O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

Segundo o art. 7º da LGPD, o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I. Mediante o fornecimento de consentimento pelo titular, exceto nas hipóteses previstas na Lei, sendo que o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular;

II. Para o cumprimento de obrigação legal ou regulatória pelo controlador;

III. 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;

IV. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V. 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;

VI. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, este último nos termos da Lei nº 9.307/1996 - (Lei de Arbitragem);

VII. Para a proteção da vida ou da incolumidade física do titular ou de terceiros;

VIII. Para a tutela da saúde, exclusivamente, em serviços de saúde e autoridade sanitária;

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

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

Vale ressaltar que é dispensada a exigência do consentimento para os dados tornados, manifestamente, públicos pelo titular. Porém a eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos.

7.2. Tratamento de Dados Sensíveis

O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

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

7.2.2. Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307/1996 - (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiros;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei, e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

8. AGENTES DE TRATAMENTO

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.

8.1. Controlador

O Controlador é pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

8.1.1. Compete ao Controlador:

I. Manter registro das operações de tratamento de dados pessoais que realize, especialmente quando baseado no legítimo interesse;

II. Elaborar, quando determinado pela autoridade nacional, relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados;

III. Decidir as questões referentes ao tratamento de dados pessoais;

IV. Expedir normas administrativas;

V. Deliberar sobre recursos administrativos relativos à proteção de dados pessoais.

A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

O relatório 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.

8.2. Operador

O operador é pessoa natural ou jurídica, de direito público ou privado que realiza o tratamento dos dados.

8.2.1. Compete ao Operador:

I. Processar os dados coletados para que sejam tratados de acordo com a LGPD, mantendo registros de suas atividades de processamentos, e disponibilizá-los ao controlador.

O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Responde pelos danos decorrentes da violação da segurança dos dados, o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas na LGPD, der causa ao dano.

O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

8.3 Encarregado/ DPO

O Encarregado, também chamado de Data Protection Officer (DPO), é a pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

8.3.1. Atribuições do Encarregado:

I. Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II. Receber comunicações da autoridade nacional e adotar providências;

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

IV. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

9. SEGURANÇA E BOAS PRÁTICAS

A Lei Geral de Proteção de Dados Pessoais também determina que o agente de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento é responsável por garantir a segurança dos dados pessoais, mesmo após o fim do tratamento.

A Segurança da Informação para garantir a proteção de dados pessoais não se trata apenas de uma boa prática, mas também é um requisito de conformidade da LGPD.

A Lei estabelece a segurança como um de seus dez princípios básicos, determinando que 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.

Na LGPD, a segurança norteia-se pelos seguintes princípios:

I. **Confidencialidade:** informação conhecida apenas por quem necessita conhecê-la;

II. **Integridade:** informação mantida íntegra, inalterada indevidamente;

III. **Disponibilidade:** informação disponível quando necessária.

Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade, a probabilidade, a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

9.1. Classificação dos Níveis de Informação

A classificação tem o objetivo de definir os níveis da informação e assegurar adequada proteção contra eventuais vazamentos e/ou acessos indevidos, levando-se em consideração seu valor e grau de criticidade e confidencialidade.

Nesse sentido, as informações do Consórcio são classificadas em:

▪ **Pública:** informações que podem ser livremente utilizadas e compartilhadas, na medida em que são públicas.

▪ **Interna:** informações de caráter restrito que devem ser mantidas no ambiente interno e não devem ser divulgadas a terceiros.

▪ **Confidencial:** informações que devem ser acessadas somente por pessoas devidamente autorizadas, mediante o estabelecimento de restrições e controle de acesso.

Importante ressaltar que a classificação acima, para fins da aplicabilidade da Lei Geral de Proteção de Dados, limita-se às hipóteses de tratamento e proteção de dado pessoal e dado pessoal sensível.

9.2. Controles de acesso à informação

Trata-se de medida de segurança que visa garantir que o acesso a todo e qualquer dado pessoal coletado e armazenado pela Administradora, incluindo-se aqueles contidos em documentos físicos, arquivos eletrônicos/digitais e qualquer pasta da rede interna, somente seja efetivado por pessoas efetivamente autorizadas.

Para tanto, é de fundamental importância a definição prévia e informada dos níveis de permissão de acesso aos usuários, assim entendido como:

I. Colaboradores em geral;
II. Gestores; e
III. Corpo diretivo com suas respetivas atribuições e autorizações de acesso, levando-se em conta a estrita necessidade para o regular exercício da atividade profissional.

A partir da definição dos perfis, acima mencionado, os usuários receberão login e senha, de uso pessoal e intransferível, destinados exclusivamente ao exercício das atividades profissionais, nos termos da sua função e respectivas atribuições, ficando o usuário integralmente responsável por suas ações.

Ademais, há que se assegurar que o controle de acesso contemple as seguintes etapas do processo:

▪ **Autenticação:** identificação do usuário que acessou;

▪ **Autorização:** estabelece o que o usuário pode acessar e fazer;

▪ **Auditoria:** registro do que foi efetivamente realizado pelo usuário.

Na hipótese de arquivos/pastas físicas, deverá o controle de acesso seguir as mesmas premissas acima. Recomenda-se, no caso, que os acessos sejam monitorados e controlados pelo gestor da área, por exemplo, mediante formulário próprio de autorização de acesso, contendo:

- data de acesso;
- nome do usuário;
- Identificação dos motivos do acesso;
- prazo de devolução; e
- visto do gestor da área.

9.3. Gerenciamento de login/senha dos usuários

Fica o usuário responsável por adotar as atualizações de login e senha, no prazo e periodicidade previamente estabelecidos pelos gestores da Administradora, observados os critérios aplicáveis para geração de novas senhas, sem prejuízo de autenticação.

9.4. Uso de equipamentos e dispositivos móveis

Os equipamentos e recursos tecnológicos disponibilizados são de propriedade da Administradora, devendo os usuários utilizá-los exclusivamente para fins profissionais, sendo expressamente vedada a sua utilização para interesses privados, exceto na hipótese de expressa autorização do gestor da área.

É terminantemente proibido aos usuários a realização de procedimentos nos equipamentos e recursos tecnológicos, tais como alterar configurações, instalar/desinstalar programas e/ou promover quaisquer alterações, sem o prévio conhecimento, aprovação e acompanhamento do gestor da área e do responsável pela área técnica.

Caso o usuário identifique qualquer ocorrência suspeita e/ou atípica no funcionamento dos equipamentos sob sua responsabilidade, deverá comunicar o gestor da área imediatamente para a verificação e tratamento da ocorrência.

Aplicam-se, na íntegra, as disposições deste Manual, na hipótese do exercício remoto da atividade profissional, sem prejuízo da aplicabilidade do respectivo Contrato de Trabalho ou Contrato de Prestação de Serviços.

Recomenda-se que os colaboradores que exercerem suas atividades remotamente, se utilizem de equipamentos (ex. celulares, notebooks) de propriedade da Administradora, vedada a utilização para fins pessoais, visando a proteção, confidencialidade e integridade de todos os dados neles contidos.

Considerando que dispositivos móveis podem ser mais facilmente comprometidos em caso de perdas, furtos/roubos, o que poderá colocar em risco a guarda dos dados pessoais, recomenda-se que a empresa avalie e implemente funcionalidades que permitam apagar remotamente os dados pessoais

relacionados à sua atividade de tratamento, devendo tal procedimento estar descrito no plano de resposta a incidentes.

10. SEGURANÇA DAS COMUNICAÇÕES

No que se relaciona à segurança das comunicações, destaca-se a relevância de se utilizar conexões cifradas, com uso de protocolos seguros, como TLS/HTTPS, ou aplicativos com criptografia fim a fim. Isso se aplica também ao uso de e-mails, de dispositivos de trocas de mensagens e de redes sociais. Recomenda-se, também, a utilização de sistemas de proteção de perímetro que monitorem, detectem, bloqueiem e previnam ameaças cibernéticas, incluindo firewalls de aplicação, sistemas de proteção a serviços de e-mail, com antivírus, anti-spam e filtros de e-mail integrados.

11. SERVIÇOS EM NUVEM

A Administradora mantém a contratação de serviços em nuvem, com empresa idônea, e em seu contrato, existe cláusula que contemple a segurança dos dados armazenados, além da avaliação do serviço oferecido pelo provedor em nuvem que atende aos requisitos, e se está em conformidade com os requisitos da LGPD.

São exigidos requisitos para o acesso da pessoa usuária a cada serviço em nuvem relacionados a dados pessoais, além da utilização das técnicas de autenticação multifator (MFA), por exemplo, aplicativos autenticadores ou short message service (SMS).

12. POLÍTICA DE BACKUP

A Administradora adotou sistema de agendamento automatizado de suas operações de backup, as quais são executadas diariamente, após o horário regular de expediente, no formato completo em nuvem. Os testes de restauração de backup devem ser realizados periodicamente.

13. GERENCIAMENTO DE VULNERABILIDADE E TESTES DE INTRUSÃO

Um dos pontos centrais na prevenção a vulnerabilidades é a manutenção de sistemas e aplicativos sempre atualizados, bem como a instalação de todas as correções de segurança disponíveis lançadas pelos desenvolvedores do sistema operacional, e de aplicativos.

Uma medida adicional de segurança e detecção de comprometimentos consiste na adoção e atualização de softwares de antivírus ou anti-malwares, que detectam, impedem e atuam na remoção de programas maliciosos, como vírus.

Esses mecanismos são mantidos em funcionamento e atualizados, e realizam varreduras periódicas nos dispositivos, e que não possam ser desativados ou alterados pelas pessoas usuárias.

O teste de intrusão é um método que avalia a segurança de um sistema de computador ou de uma rede, simulando um ataque de uma fonte maliciosa e apresenta um resumo das possíveis vulnerabilidades para checagem da efetividade desse sistema, e dicas de correção.

14. CANAL DE COMUNICAÇÃO COM OS TITULARES

Para o exercício dos direitos dos titulares (alteração, consulta, exclusão, portabilidade e revogação), recomendamos implantar canal para a gestão das requisições, conforme modelo, além da expressa informação dos dados do Encarregado nomeado, com indicação do nome, telefone e e-mail: lgpd@motoasaconsocios.com.br

15. FISCALIZAÇÃO

A Autoridade Nacional de Proteção e Dados (ANPD) é o órgão da administração pública federal responsável por zelar pela proteção de dados pessoais, implementar, fiscalizar e orientar a população sobre o cumprimento da LGPD no Brasil, bem como aplicar as penalidades cabíveis no caso de desrespeito à Lei de tratamento de dados. Além de receber denúncias, anônimas ou não, sobre práticas irregulares das instituições com os dados pessoais.

As principais Competências da ANPD são:

I. Zelar pela proteção dos dados pessoais, nos termos da legislação;
II. Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
III. 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;
IV. Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; e
V. Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis.

De acordo com o art.3º da LGPD, estão sujeitas à aplicação da lei todos os tratamentos de dados pessoais:

- Que envolvam a oferta de bens ou serviços para titulares que se encontram no Brasil, seja de modo gratuito ou oneroso, independentemente do país em que o tratamento ocorra; e

- Que envolvam dados pessoais coletados no Brasil.

Para estar em conformidade com a Lei, é necessário que a empresa tenha todos os registros de consentimento armazenados. A regra também é válida para leads e clientes adquiridos antes da Lei entrar em vigor.

O não cumprimento da Lei, pode gerar advertências e multas de até 2% sobre o faturamento da empresa, com um limite estabelecido de R$ 50 milhões por infração cometida.

Além disso, a inconformidade com a LGPD pode culminar na obrigatoriedade de fornecer relatórios periódicos para a ANPD, que é o órgão criado para a fiscalização da Lei.

O Ministério Público e o Procon também podem entrar com ações judiciais para a apuração de dados coletivos.

16. SANÇÕES ADMINISTRATIVAS

A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.

As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - Gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - Boa-fé do infrator;

III - Vantagem auferida ou pretendida pelo infrator;

IV - Condição econômica do infrator;

V - Reincidência;

VI - Grau do dano;

VII - Cooperação do infrator;

VIII - Adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados;

IX - Adoção de política de boas práticas e governança;

X - Pronta adoção de medidas corretivas; e

XI - Proporcionalidade entre a gravidade da falta e a intensidade da sanção.

As penalidades da LGPD ocorrem de diversos modos, cada uma com um grau diferente, variando entre, mínimo, moderado e máximo. São elas:

1. Advertência

Notificação para a empresa se atentar às novas normas de tratamento de dados, com um prazo estipulado.

2. Multas

Podem ser aplicadas em até 2% sobre o faturamento da empresa e até 50 milhões de reais por infração cometida. A multa também pode ser cobrada diariamente.

3. Bloqueio de Dados Pessoais

Com essa penalidade, a empresa fica proibida de utilizar, seja por qualquer finalidade, os dados pessoais coletados, até a regularização das infrações cometidas.

4. Eliminação Total da Base de Dados

Dependendo do número de infrações e do grau de risco de cada uma delas, a empresa poderá ter que apagar todos os dados pessoais coletados da base.

5. Impacto na Imagem

Outro impacto perigoso para quem não está em conformidade é a notoriedade da infração. Empresas que não acatarem as normas previstas na LGPD, poderão ter o ato infracional divulgado para conhecimento geral da população. Isso afeta diretamente na reputação e autoridade de uma organização, que terá a sua imagem manchada por irregularidades que poderiam ter sido evitadas.

17. CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados instituiu novos conceitos, princípios, direitos e obrigações que, em conjunto, traduzem uma nova cultura de mercado nas operações com dados pessoais, de maior transparência e segurança.

A LGPD determina qual o processo correto para a coleta e utilização dos dados de consumidores obtidos pelas empresas através de bancos de dados, páginas de cadastro, automações de serviços ou marketing, e qualquer outra estratégia de aquisição de leads.

Além disso, a Lei também determina as devidas penalizações em caso de vazamento ou má utilização das informações, garantindo ao cliente um maior respaldo jurídico e uma melhor experiência de consumo.

Existe um outro fator: a administração de riscos e falhas precisa ser revista. Isso quer dizer que quem gere base de dados pessoais deve redigir normas de governança, adotar medidas preventivas de segurança, replicar boas práticas e certificações existentes no mercado. Além de elaborar planos de contingência, fazer auditorias e resolver incidentes com agilidade.

Outro ponto importante é que todos os agentes de tratamento se sujeitam à Lei. Isso significa que as organizações e as subcontratadas para tratar dados respondem, em conjunto, pelos danos causados.

Sendo assim, é preciso ressignificar a sua relação com os clientes e a forma de prospectar, sendo mais transparentes sobre a finalidade do uso de dados em seus formulários de consentimento.

18. GLOSSÁRIO

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

2. **Agentes de Tratamento:** representados pelo Controlador, Operador e o Encarregado/ DPO.

3. **Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

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

5. **Banco de Dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

6. **Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

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

8. **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

9. **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.

10. **Dado Pessoal:** qualquer informação relacionada a uma pessoa natural identificada ou identificável, como por exemplo, nome e sobrenome, endereço, telefone de contato, e-mail, ID profissional etc.

11. **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.

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

13. **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).

14. **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

15. **LGPD:** Lei Geral de Proteção de Dados – Lei nº 13.709/2018;

16. **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.

17. **Não Discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

18. **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.

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

20. **Órgão de Pesquisa:** órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário, a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

21. **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.

22. **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

23. **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.

24. **Relatório de Impacto:** 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.

25. **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.

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

27. **Transferência Internacional de Dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

28. **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.

29. **Tratamento:** 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.

30. **Uso Compartilhado de Dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.