CARTILHA DE **PROTEÇÃO DE DADOS PESSOAIS**

LEI GERAL DE
PROTEÇÃO DE DADOS

(LGPD) | LEI 13.709/2018

GRUPO UMUARAMA

SUMÁRIO

1. O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS

Você já deve ter escutado a famosa frase que diz que os dados são “o novo petróleo”, ou DATA IS THE NEW OIL.

Essa frase está sendo muito falada no contexto mundial, mas muitas vezes já ouvimos, mas não entendemos o real significado.

A sociedade ao longo do tempo sofreu diversas formas de organização social. Em cada época, existiu um elemento central para o seu desenvolvimento. Com o avanço da tecnologia se consegue romper todos os padrões impostos durante milhares de anos, como por exemplo padrões geográficos, que faz com que estejamos vivenciando essa era da sociedade da informação. Atualmente a sociedade têm um elemento central que é a INFORMAÇÃO, sendo ela fundamental para o desenvolvimento da economia. É a partir do momento que a informação passa a ser o ponto central de desenvolvimento da sociedade e da economia, os dados que se transformam em informações, tomam esse lugar de importância, dentro do cenário mundial e passa ser os principais ativos das empresas.

Hoje, não existe empresas que não trabalham com dados pessoais. Isso demonstra que os dados são o novo petróleo, ou seja, o combustível para a movimentação da empresa. A coleta de informações pessoais por empresas alavanca a eficiência empresarial devido a transformação dessas informações em conhecimento, que são processadas e aplicadas através da inteligência de mercado, onde sua principal matéria prima são os dados coletados que ajudam a entender o cliente e seu comportamento. Esses dados devidamente processados geram valor para empresa.

Um grande exemplo da importância de transformar informação em conhecimento baseado em dados, é trazida pelo autor Tallis Gomes - em seu livro NADA EASY “o passo a passo de como combinei gestão, inovação e criatividade para levar minha empresa a 35 países em 4 anos”. Em um dos pontos relatados, ele diz que usou a estratégia de levar soluções de forma simples aos seus clientes. Uma das maneiras foi através dos feedbacks de seus consumidores a qual aplicou em seus produtos para serem aprimorados. Isso quer dizer que a informação dos feedbacks se transforma em conhecimento que gera uma melhoria dentro da empresa e consequentemente crescimento de mercado. Então, podemos observar que o tratamento de dados pessoais pelas empresas faz o consumidor sair de mero expectador para ter uma postura mais ativa. Ele entra no ciclo da produção empresarial.

Mas, na verdade qual a ligação da Lei Geral de Proteção de Dados com as empresas? LGPD e as empresas estão totalmente interligadas. A partir de 18 de setembro de 2020, as empresas estarão obrigadas a aplicarem a LGPD (assim chamada intimamente) dentro de seus modelos de negócios. A lei 13.709/2018 em seu - Art. 1º: Esta Lei 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.

Não é que as empresas e órgãos públicos não possam usar mais dados pessoais. Vemos que os dados são necessários para o desenvolvimento, inovação e empreendedorismo. Não há economia que se sustente sem uma eficiência empresarial. Mas ao mesmo tempo a lei veio para resguardar direitos e garantias fundamentais dos titulares de dados pessoais. A LGPD estabelece as “regras do jogo” para um ganho mútuo das empresas e dos titulares de dados. Quando há uma coerência na coleta de dados, há uma confiabilidade maior por parte do consumidor depositada naquela empresa. Dessa forma, um maior consumo daquele produto é impulsionado e uma relação de estreitamento de laços é delineada com o cliente. A lei, trata-se de uma oportunidade única, geradora de vantagens competitivas e estabelecedora de limites de segurança, transparência e confiança por parte do titular.

1.1. O QUE SÃO DADOS PESSOAIS E SUAS CLASSIFICAÇÕES

O legislador traz o conceito de dado pessoal no Art. 5°, I: dado pessoal - informação relacionada a pessoa natural identificada ou identificável. Conforme classificado pelo legislador, dado pessoal é toda informação relacionado a "pessoas" (eu e você), sendo informações que pode nos identificar diretamente, como RG, CPF, TITULO DE ELEITOR, ENDEREÇO entre outros. Esses dados são classificados como dados comuns, onde qualquer pessoa consegue em simples análise identificar alguém. Mas existem também informações pessoais que não nos identifica imediatamente, por exemplo: PLACA DE UM VEÍCULO, IP DO COMPUTADOR, COR DA PELE etc. Lembrando que o conceito de dados pessoais é expansionista. Vale ressaltar que dado pessoal é um conceito relacional, ou seja, será considerado dado pessoal a partir da relação e da análise de cada caso.

A lei traz também os dados considerados sensíveis, que é definido no ART. 5°,

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. Podemos afirmar que essa categoria de dados é protegida pela LGPD em função do seu caráter discriminatório, podendo trazer um dano muitas vezes irreparável ao titular. O tratamento de dados sensíveis deverá seguir o rol do ART 11 da lei.

Ligado ao conceito de dados pessoais, o tratamento de dados é o procedimento que envolve a utilização destes dados, tais como a coleta, classificação, utilização, processamento, armazenamento, compartilhamento, transferência, eliminação e outras funções relativas a esse tratamento. Então tratamento é toda operação feita com dado. A lei nos coloca como os verdadeiros donos dos dados, cujo os direitos estão elencados no art. 18, a qual falaremos no capítulo 5.

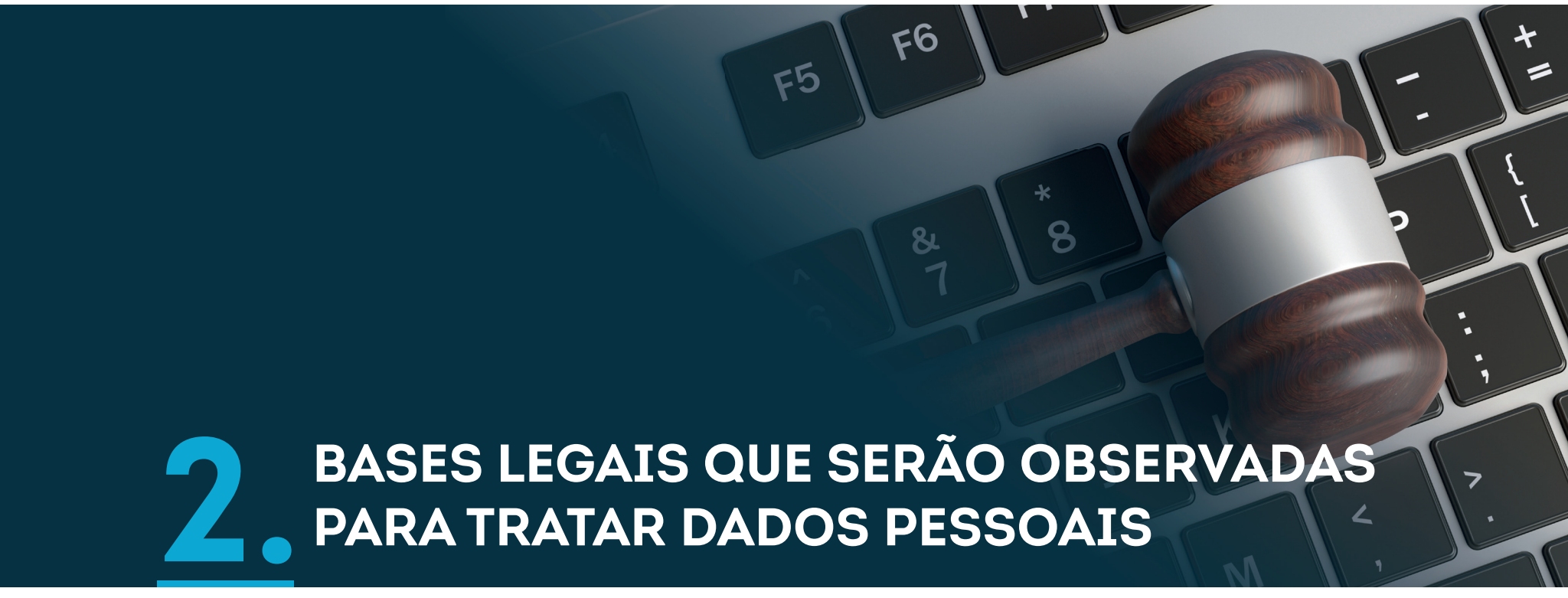
1.2. A IMPORTÂNCIA DOS DADOS PESSOAIS

A Lei Geral de Proteção de Dados tem como objetivo o desenvolvimento tecnológico e econômico, bem como a proteção de direitos e liberdades fundamentais. A LGPD quer ajudar a economia através da tecnologia, mas sem deixar de proteger os direitos dos consumidores, visando proteger dados pessoais e trazendo uma maior competitividade de mercado.

Para o Brasil do ponto de vista comercial e econômico é de grande importância termos uma lei de proteção de dados, sendo um dos requisitos estipulado pela OCDE (Organização de Cooperação e de Desenvolvimento Econômico), para que o Brasil possa fazer parte juntamente com outros países. Se trata de uma organização internacional, composta por 35 países, que tem por objetivo promover políticas que visem o desenvolvimento econômico.

Estamos diante de um mundo que dados pessoais são fontes de informações valiosas para inúmeras transações. Podemos afirmar que vivemos em uma era que nunca se compartilhou tantos dados. Dados esses captados por empresas de diversos segmentos. Os dados pessoais são os insumos das empresas, através deles podem fazer marketing direcionado para trazer maior efetividade em suas vendas. Afinal, quem não gosta de um atendimento personalizado! A empresa que entende a importância dos dados pessoais consegue levar aos seus possíveis clientes o produto ou serviços que realmente eles precisam. Um exemplo disso é a empresa Target, uma grande varejista Norte-Americana que a partir de uma grande base de dados formada pelo histórico de compras e, também, informações pessoais dos clientes, programou um algoritmo em seu sistema que tinha por finalidade predizer o que os consumidores gostavam de receber como anúncio e antever quais compras eles realizariam. O objetivo da empresa era alcançar seu público-alvo e promover ações de marketing específicos para cada segmento, fomentando as compras de itens de interesse do cliente.

Vale ressaltar que a Lei Geral de Proteção de Dados não veio proibir essas práticas como praticado pela empresa Target, pelo contrário, veio para regular e trazer meios claros de como utilizar ferramentas estratégicas utilizando dados pessoais. A LGPD traz com ela alguns princípios e bases legais que terão que ser aplicadas nos tratamentos de dados realizadas pelas empresas a partir da entrada em vigor da lei.



2. BASES LEGAIS QUE SERÃO OBSERVADAS PARA TRATAR DADOS PESSOAIS

Com o intuito de estabelecer as regras, de forma a não prejudicar ou erradicar nenhum tipo de Modelo de Negócio interferindo negativamente nos negócios privados ou de setores públicos, foram desenvolvidas as Bases Legais da LGPD.

As bases legais trazidas pela LGPD autorizam legalmente o tratamento de dados pessoais por empresas e órgão públicos. Para cada dado tratado se utiliza uma base legal. Para isso, são descritas 10 situações em que tratar dados pessoais é possível, justificável e legítimo, para que a sua finalidade se enquadre e o seu tratamento esteja de acordo com essas Bases Legais da LGPD.

2.1. CONSENTIMENTO

Consentimento caracteriza a permissão do titular de dados para que ocorra um determinado tratamento de finalidade previamente informada. Assim, essa Base Legal indica a autorização expressa do titular, para que você possa utilizar seus Dados Pessoais. O consentimento tem que ser livre – o titular não poderá ser condicionado a entrega de seus dados a nenhuma outra situação; exemplo: só será possível conceder descontos caso o titular apresente CPF para realização de um cadastro. O consentimento tem que ser específico – O titular terá a clareza para que os seus dados serão utilizados. O consentimento também terá que ser inequívoco - essa característica aponta que o titular não deve ficar confuso ou ser manipulado, tem que ter consciência exata para que o seu consentimento será usado. E por fim, o consentimento precisa ser expresso. A lei fala que o consentimento tem que ser escrito. Mas ao definir como “escrito”, isso não quer dizer que tenha que ser a mão. Apenas que o formato ideal é por meio de um texto, dentro do meio que for viável para empresa.

2.2. OBRIGAÇÃO LEGAL

Conforme o próprio nome diz, é uma obrigação imposta por lei ou instrumentos fundamentados por lei. Nesses casos, não é necessário o uso do consentimento, sendo que a obrigatoriedade vem da própria lei sendo necessário o tratamento de dados pessoais. Um exemplo de tratamento de dados porque a lei assim o obriga é o caso de arquivar dados pessoais para garantir a defesa em uma futura ação trabalhista, que nesse caso os dados dos colaboradores terão que ficar no banco de dados da empresa no período de cinco anos de acordo com a legislação trabalhista. Um outro exemplo se trata de guardar livros de registro e contratos de trabalho onde a lei especifica traz tempo indeterminado para que a empresa possua esses dados internamente, sendo assim a lei em ambos os casos terão que ser aplicadas.

2.3. POLÍTICAS PÚBLICAS

Como o próprio nome sugere, a lei permite o tratamento de Dados Pessoais com a finalidade do desenvolvimento de Políticas Públicas. Esta base legal é destinada aos órgãos da Administração Pública direta ou indireta, de modo que restringe o seu uso apenas a eles.

2.4. PESQUISAS

Esta base legítima o tratamento de dados com a finalidade específica de pesquisas científicas, tecnológicas, históricas etc., desde que feitas por órgão de pesquisa.

2.5. EXECUÇÃO DE CONTRATO

Essa base legal legítima o tratamento de dados para o cumprimento de uma obrigação prevista em um contrato, ou seja, uma obrigação contratual, de que faça parte o titular ou ao pedido do titular. Então, se faz necessário o tratamento de dados para que o contrato seja executado. Um exemplo claro dessa base legal é o tratamento de dados dos colaboradores pelas empresas a qual fazem parte do quadro de funcionários.

2.6. EXERCÍCIO REGULAR DE DIREITO EM PROCESSO

Essa base traz o direito de uma empresa ter dados pessoais por questão do direito de acesso à justiça. Não faria sentido pedir o consentimento para uma pessoa a qual se tem pretensão de processa-la. Essa base também é utilizada para justificar utilização de dados para possíveis defesas, resguardando um direito constitucional da ampla defesa e do contraditório. Logicamente esses dados terão que ser arquivados, observando sempre o período prescricional que a legislação nos traz. A empresa não poderá ficar eternamente com dados pessoais, salvo determinação legal.

2.7. PROTEÇÃO DA VIDA

Neste caso, você não precisa utilizar do consentimento, quando se trata de um risco e situação que envolve a Proteção da Vida de uma pessoa. Esta Base Legal legítima o tratamento de dados toda vez que a vida do titular ou de um terceiro estiver em iminente risco.

2.8. TUTELA DA SAÚDE

Essa base legal é exclusiva para utilização por profissionais da saúde. Para o uso dessa Base Legal existe uma restrição, uma vez que aponta casos de prestação de serviços essenciais à saúde, por profissionais da área da saúde ou agentes sanitários.

2.9. PROTEÇÃO DE CRÉDITO

Instituições financeiras podem tratar dados com objetivo de evitar inadimplências. Visa proteger as instituições financeiras de prejuízos. Os bancos e grandes instituições financeiras demandarem esse suporte, para restringir ao crédito os que são considerados no mercado financeiro como inadimplentes ou maus pagadores; beneficiando aqueles que estão com as finanças em dia.

2.10. LEGÍTIMO INTERESSE

Essa base tem que ser utilizada com muita cautela. Para que ela possa ser aplicada será necessário fazer o teste do LIA. O tratamento de dados justificado por essa Base Legal pode ser realizado quando for atender aos interesses do controlador ou de um terceiro, quando esse interesse não ultrapassar os direitos e liberdades fundamentais do titular de dados.

2.11. BASES LEGAIS PARA DADOS SENSÍVEIS

O tratamento de dados sensíveis requerer um cuidado dobrado. A base do consentimento já visto acima é aqui a base principal a ser aplicada em caso de tratamento de dados sensíveis. Relembrando que dados sensíveis são aqueles que podem gerar discriminação ao titular de dados, podendo trazer possíveis danos. Uma obrigação imposta pela lei é que em caso de tratamento de dados sensíveis se faz necessário elaboração de relatório de impacto, onde as demais categorias de dados não se faz necessário.

2.10. BASES LEGAIS PARA DADOS DE CRIANÇAS

A Lei Geral de Proteção de dados também traz tratamento de dados pessoais quando esses dados se tratar de criança. O estatuto da criança e do adolescente traz a definição de criança e adolescente: ART 2º do ECA - Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade.

Quanto ao tratamento de dados de crianças e adolescentes, a LGPD trouxe, em sua redação, que este deve ser realizado no melhor interesse e proteção integral deles. Vejamos: ART.14 - O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

O cuidado se dá devido ao não entendimento desses titulares em relação a distribuição de seus dados. A lei traz, no §1º do Art. 14 da LGPD, o tratamento de dados de criança, pode ser realizado mediante o consentimento específico de um dos pais ou responsável. Desta forma, a base legal exclusiva e prédeterminada a ser utilizada nestes casos é o Consentimento, salvo exceções destacadas pela LGPD.

Como observado, as empresas que prestem serviços ou oferecem produtos a essas categorias de titulares, principalmente a crianças onde a lei é mais clara, terão que ter muita atenção.

3. QUEM SÃO OS ATORES DA LEI

Quem são as pessoas envolvidas na LGPD! A Lei Geral de Proteção de dados traz algumas figuras a qual é de suma importância para o nosso conhecimento, até mesmo para ficar claro as funções de cada um desses personagens.

3.1. CONTROLADOR E OPERADOR

O controlador poderá ser pessoa jurídica ou pessoa física a quem competem as decisões referentes ao tratamento de dados pessoais. Esse agente possui o controle das decisões relacionadas a dados pessoais. Cabe a ele decidir quais dados serão tratados, como e porque será coletado, a vida útil de cada dado, a quem será compartilhado, como será arquivado ou descartado entre outros. Pode dizer que será o controlador que irá determinar o tratamento de dados de forma geral.

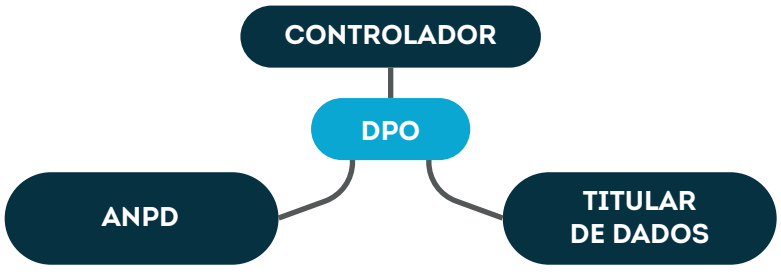
O operador poderá ser pessoa jurídica ou pessoa física, que realizará o tratamento de dados pessoais em nome do controlador. Esse agente irá tratar dados apenas se o controlador mandar. As obrigações que a LGPD traz dentro das disposições da Lei são maiores para o controlador, porque, afinal de contas, ele é quem determina o tratamento de dados.

3.2. AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Uma outra figura de extrema importância trazida pela LGPD, é a figura da ANPD (Agência Nacional de proteção de Dados). Ela será responsável pela implementação, fiscalização e monitoramento. Esse órgão de autonomia nacional será responsável em editar normas e publicar orientações, uma vez que a lei apresenta algumas lacunas e informações incompletas na sua estrutura. Caberá a ANPD aplicação das sanções e multas estipulado pela lei em caso de não cumprimento a LGPD.

3.3. DATA PROTECTION OFFICER - DPO/ENCARREGADO DE DADOS

Esse sujeito conhecido na Europa como DPO, é o mesmo que encarregado de dados. A lei traz como responsável entre a empresa, titular de dados e ANPD. O DPO nada mais é do que uma pessoa física ou jurídica, indicada pelo controlador para atuar como canal entre controlador - titular de dados - ANPD.



Dentre as responsabilidades do DPO estão:

- Elaborar relatório de impacto;
- Elaboração de política de privacidade;
- Comunicação de incidente de segurança ao titular e ANPD;
- Responder solicitações dos titulares e da ANPD;
- Verificação da conformidade da empresa com as regras da LGPD;
- Dar continuidade e monitorar o complice em proteção de dados internamente;
- Elaboração de treinamentos e conscientização; Criar e gerir comitê interno da empresa;
- Atualizar procedimentos e processos internos etc.

O DPO será responsável por toda ligação interna e externa da empresa relacionado a nova Lei Geral de Proteção de Dados, tendo como foco implementar políticas de compliance em proteção de Dados. Qualquer questionamento, dúvidas e problemas relacionados a privacidade e proteção de dados terá que ser reportado a esse profissional. Lembrando que de acordo com a lei, todas as empresas e órgãos públicos são obrigados a ter um DPO.

4. OS PILARES PARA CRIAÇÃO DE UMA CULTURA EM PROTEÇÃO DE DADOS

Nesse capítulo iremos tratar dos princípios que a Lei Geral de Proteção de dados nos traz. Os princípios informam a aplicação da própria lei. As regras impostas pela LGPD devem ser aplicadas sempre em conjunto com os princípios. Não tem como falar de cultura em proteção de dados sem falar dos princípios. Afinal os princípios são o alicerce da lei.

4.1. PRINCÍPIO DA FINALIDADE

Esse é considerado um dos principais princípios, sendo que não tem como falar de tratamento de dados, sem trazer a finalidade o porquê e para que a empresa está tratando determinado dado. O controlador (empresa), sempre terá que ter um motivo claro do porque o tratamento é feito e informar o titular do referido tratamento. Esse princípio é um dos motivos pelos quais surgiram uma série de problemas referentes a privacidade e proteção de dados. Muitas empresas estavam recolhendo dados para uma finalidade e utilizando-os de diversas maneiras.

4.2. PRINCÍPIO DA NECESSIDADE

Esse princípio traz a ideia que o controlador que trata dados deve colher apenas o que de fato sejam necessários para o tratamento. Aqui há uma ideia de minimização, ou seja, quanto menos dados forem coletados, melhor. Não há necessidade de pedir dados dispensáveis aquela finalidade.

4.3. PRINCÍPIO DA ADEQUAÇÃO

Nesse princípio traz obrigatoriedade que o tratamento de dados estejam compatível com a finalidade que justifique o tratamento. O meio de coleta do dado pessoal precisa ser adequado para atingir a finalidade determinada. Então, o prudente é sempre procurar pelo meio mais adequado e pelo melhor momento para fazer esse processo.

4.4. PRINCÍPIO DO LIVRE ACESSO

Refere-se a garantia de acesso que o titular terá que ter em relação aos seus dados a quais liberou para empresa tratar. Esse acesso traz ao titular consulta facilitada e gratuita sobre a duração do tratamento, quais dados estão sendo tratados, a quem serão compartilhados entre outras informações de direito do titular.

4.5. PRINCÍPIO DA QUALIDADE

Esse princípio rege que é preciso sempre garantir ao titular exatidão e precisão no tratamento de dados, ou seja, em sua qualidade. É de suma importância que os dados que a empresa tiver acesso, terá que está sempre atualizado, evitando assim, prejuízos ao titular. Os dados precisam ser coerentes e verídicos com a realidade.

4.6. PRINCÍPIO DA TRANSPARÊNCIA

Nesse princípio traz obrigatoriedade que o tratamento de dados estejam compatível com a finalidade que justifique o tratamento. O meio de coleta do dado pessoal precisa ser adequado para atingir a finalidade determinada. Então, o prudente é sempre procurar pelo meio mais adequado e pelo melhor momento para fazer esse processo.

4.7. PRINCÍPIO DA SEGURANÇA

Esse princípio dispõe sobre a necessidade de buscar meios seguros de proteger os dados que são tratados, ou seja, evitar de toda forma um incidente que gere dano ao titular dos Dados Pessoais.

4.8. PRINCÍPIO DA PREVENÇÃO

A empresa tem que buscar medidas técnicas e administrativas para prevenir ocorrências de danos.

4.9. PRINCÍPIO DA NÃO-DISCRIMINAÇÃO

Este princípio impossibilita que o tratamento de dados ocorra de modo a cometer qualquer tipo de ato ilícito ou discriminatório em face dos titulares dos dados. Isso significa que todas as vezes que produtos e serviços forem desenvolvidos com base em banco de dados, terão que observar os meios para se evitar discriminação de seus titulares.

4.10. PRINCÍPIO DA PRESTAÇÃO DE CONTAS

E por fim, trazemos a importância de documentar e demostrar para a empresa, titular de dado, ANPD e para o mercado que a empresa possui todos os meios e estratégias necessárias para minimizar quaisquer possíveis riscos relacionados a proteção de dados pessoais. É importante que a empresa tenha arquivado tudo o que foi feito em relação a proteção de dados.

Vimos então todos os princípios que norteiam a LGPD. Além de todos esses princípios, sempre é importante atentar ao Princípio da Boa-fé, que é um princípio que rege as relações interpessoais, por isso ela nunca pode ser deixada de lado.

5. DOS DIREITOS DOS TITULARES

Nesse capítulo iremos conhecer quais os direitos dos titulares trazidos pela Lei Geral de Proteção de dados em seu ART. 18. Para a empresa assegurar todos os direitos e necessário compreendê-los .

5.1. CONFIRMAÇÃO

O direito de confirmação é a empresa sendo contactada pelo titular para confirmar se há tratamento de dados referente a seus dados dentro da empresa, ou seja, confirmar ou não se detém informações, proveniente da coleta de dados daquela pessoa. A empresa poderá fazer de forma simplificada e imediata ou de forma completa sendo o prazo de entrega da confirmação de 15 dias (art.19).

5.2. ACESSO

O titular pode, a qualquer momento, pedir o Acesso aos dados pessoais que determinada empresa possui em seu Banco de Dados. No direito ao acesso pelo titular, a pessoa já sabe da existência do tratamento dos dados e quer ter acesso e saber o que de fato está sendo feito com seus dados.

5.3. RETIFICAÇÃO

O direito da retificação é dado ao titular pela lei, em caso de ser constatado que a empresa detém algum dado incorreto. Assim terá o direito de solicitar para a empresa a correção. Nesse caso diferente do direito de confirmação, a lei não traz um prazo de resposta por parte da empresa, mas caso não responda imediatamente, terá que justificar ao titular

5.4. CANCELAMENTO

O direito ao cancelamento se dá quando a base legal aplicada pela empresa foi o consentimento. Quando o titular através de autorização por consentimento dado a empresa para tratar seus dados, a qualquer momento esse titular terá o direito de solicitar a exclusão dessas informações pessoais no banco de dados da empresa. Esse caso segue a mesma ideia do direito de retificação, a lei não traz um prazo determinado.

5.5. OPOSIÇÃO

No caso do direito a oposição não se aplica quando o consentimento for a base legal aplicada para tratar dados. É recomendado que a empresa busque tornar públicos seus atos de proteção de dados, as políticas que é utilizada para tratamento de dados na empresa, para que o titular entenda quais os direitos que ele poderá exercer.

5.6. PORTABILIDADE

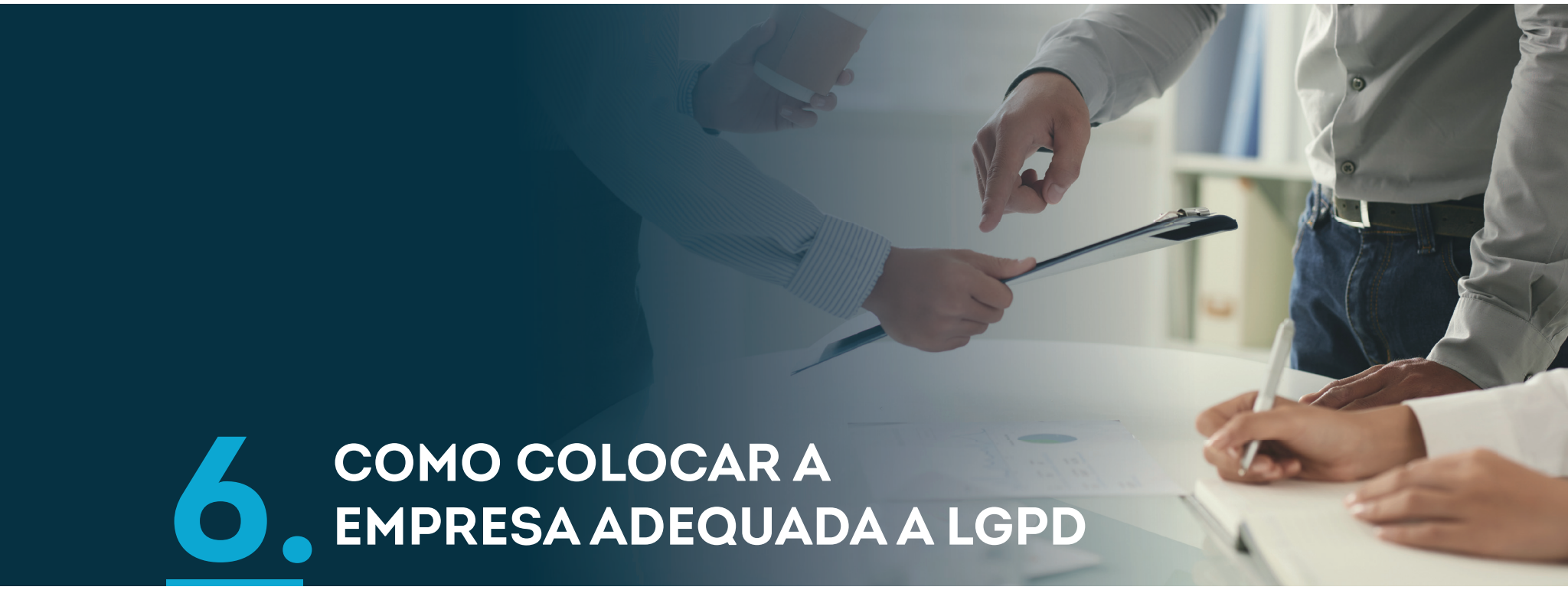
O direito de portabilidade dá ao titular, autorização para solicitar a transferência ou compartilhamento de seus dados de uma emprW de plano de saúde ou de companhia de telefone, ele pode solicitar ao antigo controlador para enviar os seus dados diretamente para o novo controlador. A lei não traz a forma que irá ocorrer essa portabilidade, caberá a ANPD regular essa transferência

5.7. COMPARTILHAMENTO DE DADOS

Outro direito dado ao titular é poder buscar por informações que indiquem com quais entidades os seus dados foram compartilhados. O titular tem que saber com quem seus dados foram compartilhados e a empresa tem que resguardar esse direito para ele. O prazo para essa resposta também não está expressamente determinado, voltando para a ideia de que se não for imediato, deve ser justificado e é importante fazer o mais rápido possível.

5.8. REVISÃO DAS DECISÕES AUTOMATIZADAS

Nosso último direito se trata de o titular solicitar revisão de uma decisão dada de forma automática, ou seja, dado por algum sistema de análise. Isso ocorrre devido a possibilidade de erros que a tecnologia de inteligência artificial possui. Essa parte ainda é polêmica, e será necessário que ANPD regulamente esse direito.



6. COMO COLOCAR A EMPRESA ADEQUADA A LGPD

A ideia nesse capítulo é expor como uma empresa está adequada a Lei Geral de Proteção de Dados. O programa de Governança em Proteção de Dados é um projeto que tem como objetivo implantar uma nova cultura em tratar informações pessoais de clientes, colaboradores e parceiros. O programa de implementação dentro traz algumas fases que será analisada por cada empresa. O plano de governança não é uma receita de bolo, ou seja, não está pronta, cada empresa terá que ser analisada devido sua individualidade de mercado.

6.1. COMITÊ DE PROTEÇÃO DE DADOS

O primeiro passo começa montando um comitê em proteção de dados. Mas afinal o que é isso? O comitê nada mais é do que a escolha de um representante de cada departamento da empresa. Esse colaborador trará sua expertise para propor soluções ligadas na proteção de dados. O colaborador selecionado está dia-a-dia lidando com as deficiências e por esse motivo sua visão é ampliada para diagnosticar possíveis procedimentos a serem adequados conforme estabelecido em lei.

6.2. CONSCIENTIZAÇÃO

A primeira fase do programa de adequação é a conscientização. Essa fase não pode ser ignorada pela empresa. É nela que será exposta como a lei funciona, a sua importância, os impactos entre outros. Por se tratar de uma novidade legislativa, as pessoas associam como um processo negativo, tendo então um conceito equivocado da LGPD. E será nesse momento que muitos preconceitos serão esclarecidos. Uma das informações que tem que ficar clara para todos que estão fazendo parte desse programa de adequação é que a lei veio para equilibrar os direitos dos titulares e das empresas, trazendo inteligência de mercado e oportunidades as organizações que enxergarem a LGPD como um “PLUS” a ser acrescentado ao portifólio da empresa.

6.3. MAPEAMENTO

A fase do mapeamento será o momento de rastrear os dados pessoais que estão no banco de dados da empresa. Esse banco de dados podem ser digitais ou físicos. Será feito um mapeamento do fluxo de dados dentro da empresa. É impossível identificar problemas sem antes saber quais são esses problemas. Esse mapeamento quando se trata de grandes empresas se faz necessário a utilização de softwares devido o grande número de dados pessoais, trazendo maior otimização nesse processo.

6.4. GAPY ANALYSIS

Essa fase será identificada os riscos existentes dentro da empresa em se tratando de proteção de dados. O termo “GAPY ANALYSIS” significa técnicas para identificar o cenário atual do projeto e o que se pretende alcançar ao final desse projeto. Nesse momento irá ser detectado toda situação em que a empresa está em desacordo com a LGPD. Através do mapeamento feito na segunda fase é possível identificar o caminho percorrido pelo dado, afim de identificar onde estão as exposições e contingências desses tratamentos pela empresa.

6.5. PLANEJAMENTO

Na fase de planejamento é o momento que será apresentada o plano de ação dos “gapys” encontrados. É aqui que determinará de fato o que será alterado ou adequado conforme estipulado pela LGPD. O plano de ação deverá ser apresentado conjuntamente com um cronograma de execução, constando as datas de cada execução. Deve-se iniciar o plano de ação nas principais contingências da empresa, aquelas que trazem maiores riscos, como por exemplo do exercício dos direitos dos titulares.

6.6. IMPLEMENTAÇÃO

A primeira fase do programa de adequação é a conscientização. Essa fase não pode ser ignorada pela empresa. É nela que será exposta como a lei funciona, a sua importância, os impactos entre outros. Por se tratar de uma novidade legislativa, as pessoas associam como um processo negativo, tendo então um conceito equivocado da LGPD. E será nesse momento que muitos preconceitos serão esclarecidos. Uma das informações que tem que ficar clara para todos que estão fazendo parte desse programa de adequação é que a lei veio para equilibrar os direitos dos titulares e das empresas, trazendo inteligência de mercado e oportunidades as organizações que enxergarem a LGPD como um “PLUS” a ser acrescentado ao portifólio da empresa.

6.7. MONITORAMENTO

Chegamos a última fase de um programa de adequação. Quando se chega nesse momento, significa que todo programa de adequação já foi realizado. Mas, não acabou! O programa de conformidade em proteção de dados é eterno, nunca acaba. Nessa fase, o objetivo é monitorar se a empresa continua verificando e validando todas as ações executadas pela empresa relacionada a proteção de dados pessoais.

Como mencionado em capítulos anteriores, o DPO será o responsável de manter a implementação do programa de conformidade atualizada e efetiva.

7. SANÇÕES APLICADAS AS EMPRESAS QUE NÃO SE ADEQUAREM A LGPD

A Lei Geral de Proteção de dados, traz em seus artigos: 52 ao 54, as sanções que poderão ser aplicadas em caso de descumprimento.

A ANPD é a Autoridade responsável para aplicação das sanções administrativas e não posso deixar de mencionar que o órgão já está constituído. A lei expõe 9 tipos de penalidades que poderão ser aplicadas, não sendo somente o pagamento de multas, como a maioria acredita.

VEJAMOS:

ADVERTÊNCIA

A empresa será advertida e estipulado um prazo para adotar as medidas corretivas determinadas pela ANPD.

MULTA SIMPLES

Até 2% do faturamento da empresa ou grupo econômico do seu último exercício, limitada o total de 50 milhões de reais.

MULTA DIÁRIA

ANPD poderá estipular multa diária até que se corrija o dano. Poderá ser mulativa com outras penalidades.

SUSPENSÃO PARCIAL

A empresa poderá ter parcialmente seu banco de dados suspenso por período de 6 meses podendo ser prorrogável.

PUBLICIZAÇÃO

Após confirmado a ocorrência de dano pela empresa, se tornará público o incidente.

BLOQUEIO

A empresa poderá ter os dados pessoais a que se referem a infração bloqueados.

ELIMINAÇÃO

A empresa poderá ter os dados pessoais que referem se a infração eliminados.

PROIBIÇÃO PARCIAL OU TOTAL

A empresa poderá ficar proibida detratar dados pessoais.

As sanções aplicadas pela Agência Nacional de Proteção de Dados (ANPD), respeita o procedimento administrativo, respeitando a ampla defesa e o contraditório. Será observado as peculiaridades do caso concreto, tendo como parâmetros: Art.52, $ 1º:

> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

A LGPD já é uma realidade no Brasil, cabendo as empresas se ajustarem aos novos parâmetros. Além de se ajustarem aos aspectos técnicos através do programa de implementação, os diretores, gestores e colaboradores deverão se atentarem aos direitos relativos as informações pessoais no diaa-dia da atividade da empresa.

Vale ressaltar que outros órgãos detém a competência para fiscalizar, como Procon, Ministério Público Estadual e Federal e as possíveis demandas judiciais relacionadas ao tema.

8. DESAFIOS DO COMERCIAL, RH, COBRANÇA, COMPRAS, MARKETING, MÍDIAS SOCIAIS E TI

No setor automobilístico, especialmente, nas concessionárias de veículos, é importante destacar quatro áreas relevantes, as quais tratam um volume expressivo de dados pessoais: Comercial, Cobrança, Recursos Humanos e Compras.

8.1. ÁREA COMERCIAL

Para a Área Comercial, destaca-se, principalmente, o atendimento na ponta, ou seja, a venda direta para o consumidor. Nesse caso, recomenda-se cuidado com detalhes que, às vezes, podem passar despercebidos como, por exemplo, a coleta de informações e documentos do comprador (pessoa física), com os quais o vendedor tem acesso e contato, e que podem envolver Imposto de Renda, CPF, RG, Comprovante de Endereço, Número de Celular, WhatsApp, entre outras informações exigidas.

Vale lembrar que a placa do veículo também é um dado pessoal. É comum que vendedores recebam cartões dos clientes, onde constam nome, sobrenome e número de telefone pessoal, assim como fiquem de posse dos dados constantes na ficha cadastral. Logo, essa é uma fonte de entrada de dados pessoais que precisa ser muito bem tratada, para estar em conformidade com a nova legislação, tanto no sentido de atender aos princípios apontados, quanto, principalmente, para prevenir e evitar vazamentos de informações. O comercial também lida com bases de dados pessoais, oriundas de outras fontes, para geração de leads, sejam de parceiros ou mesmo de fontes públicas, como a Internet. É importante dizer que a Lei permite o uso dessas informações, mas é preciso que sejam de fontes legítimas, e para as quais o titular tenha consentido o compartilhamento dos seus dados pessoais, com terceiros, em alguma política de privacidade. Um bom exemplo é se o titular dos dados tiver participado de um evento, como um Feirão de Automóveis, visitado um estande, para o qual forneceu seus dados. Se tiver preenchido alguma ficha, que já o avisava e coletava seu consentimento para compartilhamento de seus dados, vinculados às finalidades informadas, então, não haverá problema.

8.2. ÁREA DE COBRANÇAS

Para a Área de Cobrança, destaca-se que, além de Dados Pessoais, por vezes, utilizam-se Dados Pessoais Sensíveis (como ocorre com a autenticação, e verificação biométrica, ou a análise de reconhecimento facial) e, muito embora possam ser tratados como exceção de consentimento, conforme as bases legais, previstas na LGPD, com a finalidade de proteção do crédito de prevenção à fraude, será necessário atender ao princípio da transparência, ou seja, informar, ao titular, para que os dados, que estão sendo coletados, serão usados. Além disso, saber abordar o consumidor/titular pode fazer muita diferença. Atenção! Dados bancários, que permitam identificar, direta ou indiretamente, o titular/pessoa natural/pessoa física, também são considerados dados pessoais. No entanto, se forem dados de uma conta de Pessoa Jurídica/Empresa, não serão considerados dados pessoais, exceto se a documentação tiver alguma informação sobre a pessoa responsável pela empresa (que a identifique). Um ponto importante é o cuidado com a qualidade de dados, pois, durante a cobrança, pode acontecer de se entrar em contato com a pessoa por canais que podem não estar atualizados, e a LGPD traz esta exigência. Já houve aplicação de multa, na Europa, devido ao envio de mensagem para o celular da pessoa errada, fazendo cobrança, por informação desatualizada. Desse modo, é possível realizar o enriquecimento da base de dados para atualizar as informações, para fins de cobrança, inclusive, a partir de dados de origem pública, justamente, para atender ao princípio da qualidade e evitar este risco.

Por fim, também alertamos sobre o Compartilhamento de dados, na terceirização, que será, extremamente, necessário estabelecer regras e responsabilidades, tendo em vista que o contratado, neste caso, será considerado, sempre que promover o tratamento de dados, em nome do Controlador, o que é comum nos contratos com agências de mídias digitais, marketing, despachantes, entre outros.

8.3. ÁREA DE RECURSOS HUMANOS

A área de Recursos Humanos merece atenção especial, pois, apesar de não lidar com dados de clientes, promove o tratamento de dados pessoais dos colaboradores. Existem vários desafios para o RH, a começar pelo processo seletivo, tendo em vista que se trata de uma relação onde ainda não há vínculo empregatício e nem, sequer, um contrato. Portanto, recomenda-se estabelecer regras específicas, controles e formas de informar, ao titular/candidato, antes da coleta dos dados pessoais, a política do processo seletivo, e que diga, ao menos, quais dados pessoais são necessários, para quais finalidades, por quanto tempo esses dados serão tratados e se haverá compartilhamento com terceiros. Ou seja, para adequar a base do "Trabalhe Conosco" à LGPD é importante que o candidato seja informado, e aceite, as condições, previamente, estabelecidas, em algum momento, no fluxo de cadastro. Isso porque o recebimento de curriculum pode ocorrer por várias formas, mas, deve haver um momento em que haja a centralização e o controle. Deve-se, também, lembrar que, pela nova Lei, onde houver uma base de dados pessoais, deve ser aplicado o descarte seguro. Logo, se for impresso, depois do seu uso, para realizar alguma entrevista ou dinâmica, é recomendável que seja feita sua eliminação, picotando os papéis. O que percebemos é que será necessária uma mudança de procedimentos, e de cultura, no ambiente de trabalho.

Pode ocorrer, ainda, o compartilhamento de dados dos colaboradores para concessão de benefícios, como saúde, alimentação, transporte, previdência, entre outros, incluindo informações do cônjuge e dependentes. Vale ressaltar que, quando isso ocorrer por exigência legal, para cumprimento do contrato de trabalho ou legítimo interesse, não haverá necessidade de consentimento.

O ideal é elaborar a Política de Conduta, bem como a Política de Benefícios, para que fiquem claros quais dados são coletados, se há compartilhamento, com quem, se há internacionalização dos dados, e que haverá tratamento, também, para registro de acervo histórico e memória da empresa, com guarda permanente. Este último item é, extremamente, relevante, pois haverá dados pessoais, como registros de imagens, vídeos, fotos, e mesmo documentos que ficarão guardados, no legado, e não poderão ser apagados.

ATENÇÃO

Quando o titular/cliente usa a mídia social, como meio de autenticação para serviços (para não preencher cadastro), o primeiro contato da empresa pode ser feito, também, pela rede social. Vale ressaltar que o cliente terá que ser informado sobre as finalidades futuras, inclusive para novos contatos do mesmo Controlador.

Para outras finalidades, será preciso analisar se essas estão descritas na própria mídia social e acompanhar o que está ali contido. Portanto, os dados não poderão ser utilizados para qualquer finalidade que não a expressa quando o dado se tornou público, pela mídia social.

Nos termos do art. 8º, parágrafo 6º em caso de nova finalidade o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

8.4. ÁREA DE MARKETING

O departamento de marketing e mídias sociais, são as áreas mais impactadas pela Lei Geral de Proteção de Dados. Se faz necessário a análise de todos os sites, e-commerce da empresa e também de seus parceiros. A LGPD traz como um dos documentos a serem obrigatórios em sítios eletrônicos a política de privacidade. E nesse documento que a empresa vai deixar em uma escrita clara para seus usuários como é utilizado os dados pessoais, para qual finalidade, com quais empresas serão compartilhados seus dados, se há coleta de cookies, opção de cardápio de cookies para que o usuário do site possa escolher quais dados poderão ser colhidos, se há transferência internacional de dados, por quanto tempo ficará armazenados esses dados entre outros. A lei traz a obrigação de constar nos sites o canal que será disponibilizado para solicitação dos titulares conforme exposto acima.

O setor de marketing deverá iniciar o envio de e-mails as suas lides para autorização do titular através do consentimento ou não, buscando através dos registros comprovar esse consentimento. Em caso de não ter consentido, deverá ser excluído esses dados das lides, sendo proibido envio de e-mail marketing.

Todos os canais digitais passarão por adequação, principalmente aqueles meios ao qual é utilizado para contato com cliente, como exemplos: chatbot, whatsapp, campo de agendamento de serviços, preenchimento de cotação, fale conosco, entre outros. O recomendado é que cada um desses acessos conste informações (pequenos textos) sobre a proteção dos dados. Aqui não é algo engessado. Sabemos que essas áreas são bem dinâmicas e criativas, podendo trazer ideias inovadoras e claro atrativas ao consumidor.

8.5. ÁREA DE T.I.

O departamento de TI se fará muito presente a todo tempo, inclusive após a finalização de toda adequação a LGPD. Sabemos que o processo de governança em proteção de dados é eterno, nunca será finalizado. O pessoal da TI, segurança da informação, sempre andará junto com o DPO.

Em primeira análise que terá que ser feita é sobre as licenças para utilização de pacote office dentro da empresa, lembrando que a utilização sem as devidas licenças não é somente pela adequação a LGPD, mas também caracteriza crime de pirataria. Um outro ponto se trata a questão de acessos a colaboradores. Em um possível vazamento de dados pessoais, se for verificado que se deu mais acesso do que deveria, a empresa irá ter multas e penalidades agravadas. É de suma importância rastrear todos os acessos e verificar o que é realmente necessário e os excessos serem excluídos, evitando inclusive futuras demandas judiciais.

8.6. ÁREA DE COMPRAS

Em relação à área de Compras, talvez esta seja a que lide com dados pessoais em menor quantidade e finalidade. O principal ponto de atenção é para dados relacionados aos parceiros e fornecedores, pessoa física envolvida nas transações contratadas, como funcionários dos contratados ou responsáveis ou representantes dos prestadores de serviços, que constam nos contratos. Mas, podem ocorrer situações que envolvam compartilhamento de dados pessoais com esses terceirizados, em função da atividade contratada como, por exemplo, contratação de serviços de armazenamento ou análise de dados (como serviço de “cloud”). Portanto, na contratação de operadores, os contratos deverão ser atualizados, com cláusulas específicas, considerando atribuição de responsabilidades e obrigações relacionadas à proteção de dados pessoais. aos treinamentos, deve ser percebida como uma forma de mitigar riscos e capacitar os funcionários sobre como devem proceder, em todos os estágios da coleta das informações.

CONCLUSÃO

A cartilha de proteção de dados pessoais tem como finalidade conscientizar diretores, colaboradores, e todos aqueles que farão parte do programa de adequação do Grupo Umuarama, da existência da Lei Geral de proteção de dados, que está vigente no país desde 18 de agosto de 2020.

A elaboração de um instrumento que traz informações claras sobre proteção de dados dentro da empresa é uma exigência da LGPD. O conteúdo aqui exposto é um resumo do texto da lei, apresentada de forma suscinta e clara, sendo esse o objetivo fundamental da elaboração da cartilha.

É sabido que grandes empresas serão as primeiras na mira da fiscalização; e por esse motivo, o Grupo Umuarama preocupado com seus colaboradores, clientes e boa reputação de mercado, não medirá esforços para trazer segurança e proteção as informações pessoais a todos que fazem parte dessa cadeia.

Grupo Umuarama desde 1970 busca atender as exigências de mercado, tendo como diferencial perante a concorrência, zelar pela satisfação de seus clientes e colaboradores. Com essa cultura já implantada, não seria diferente com a na nova Lei Geral de Proteção de Dados. É de grande relevância que todos se envolva nesse projeto, para que ao final da implantação do programa de governança, ele seja eficaz e efetivo conforme estabelecido pela LGPD.

TERMO DE CIÊNCIA E CONCORDÂNCIA

Declaro que recebi a Política Interna de Uso de Dados de Clientes do Grupo Umuarama, descrita nesta Cartilha.

Por fim, declara que concorda e aceita o teor deste Termo e das normas a que faz referência, bem como que teve acesso a cópias dos documentos aqui mencionados.

GRUPO
UMUARAMA