Lei Geral de Proteção de Dados (LGPD)

LGPD

POCKET BOOK

IPACOM
Instituto Paranaense de Compliance

Coordenadores:
Letícia Sugai
Germano de Sordi

Autores:
Camilla M. Ribas da Silva
Júlia Chemin da Rocha
Laércio Almeida Junior
Luiz Carlos Rossi Filho
Germano de Sordi
Luciliane Ribeiro
Marizete Figueiredo
Murilo Pastori Roberti
Felipe Deckers Leme
Ana Paula Schimiloski

IPACOM
Instituto Paranaense de Compliance

Edição: Marizete Figueiredo

IPACOM
Instituto Paranaense de Compliance

SUMÁRIO

1. INTRODUÇÃO

Este Guia Prático da LGPD tem como missão levar conhecimento ao público em geral sobre a Lei Geral de Proteção de Dados. É aqui que, tanto o titular quanto o responsável pela coleta e tratamento dos dados pessoais, poderão ter uma perspectiva da lei e seu contexto histórico, direitos dos titulares, tipos de dados pessoais, personagens, como se adequar, como fazer mapeamento de dados, quais são as sanções em caso de descumprimento da lei e uma perspectiva dos desafios que deverão ser enfrentados a partir da vigência da lei.

Pois bem, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), dispõe sobre o tratamento de dados de pessoas naturais (a exemplo do RG, CPF, nome, endereço etc.) de forma digital ou física, realizado por pessoa jurídica de direito público ou privado e também por pessoa física (profissionais liberais), sempre que houver alguma operação de tratamento de dados realizada em território nacional ou de pessoa localizada no Brasil.

Mas a LGPD inclui no seu texto outras categorias de dados como é o caso de dados pessoais “sensíveis”, que são dados relacionados à característica da personalidade do indivíduo e suas escolhas pessoais.

A LGPD destina-se aos profissionais liberais e às empresas independente do porte, ou seja, tanto as grandes corporações quanto as pequenas, médias, microempresas, MEI e pessoas físicas que tratem dados pessoais, sejam de consumidores, clientes ou terceiros com quem mantenham relação comercial, todos terão que se adequar à legislação.

A fiscalização acerca do cumprimento desta nova legislação está a cargo da Autoridade Nacional de Proteção de Dados (ANPD), que pode receber inclusive denúncias sobre descumprimentos da lei, e está incumbida aplicar sanções prevista na LGPD, que vai desde multa pecuniária que pode ser de até 2% do faturamento bruto da empresa, até a obrigação de se retratar publicamente, conforme será melhor detalhado em tópico próprio.

Destaca-se que não existe uma fórmula pronta para a implementação da LGPD, afinal dependerá do nicho econômico da empresa, volume de dados coletados e armazenados, quais tipos de dados são tratados, as peculiaridades do negócio etc.

De todo modo, é salutar que as empresas estejam atentos quanto ao tema proteção e privacidade de dados, o que a LGPD dispõe a respeito e quais medidas precisam ser tomadas para que estar em conformidade com a lei.

Por fim, o presente guia não tem o intuito de exaurir o assunto, mas sim oferecer um panorama geral da lei e dos principais pontos e conceitos que ela traz para que o leitor possa conhecer e também nortear aqueles que queiram iniciar a adequação e introduzir na organização a cultura de proteção de dados.

2. CONTEXTO HISTÓRICO

A Lei Geral de Proteção de Dados no Brasil sofreu influência norte-americana e, principalmente, europeia. A bem da verdade a LGPD foi inspirada no GDPR (General Data Protection Regulation) – que trata da regulamentação de dados da União Europeia. Assim, para explicar o contexto histórico da LGPD é preciso entender o contexto histórico mundial, especialmente no viés europeu.

A Europa enxerga o direito à privacidade como um direito humano e desde 1950 fala-se de proteção de dados, ainda que de forma incipiente. A Declaração Europeia dos Direitos do Homem e a Declaração Universal dos Direitos Humanos foram as primeiras declarações internacionais que se preocuparam com o direito à privacidade, sendo assim utilizadas como pilares para a elaboração do GDPR.

Por volta de 1995 assuntos sobre proteção de dados já eram tratados como lei na Europa, visto que a Diretiva 95/46/CE tratava da proteção e tratamento de dados. O GDPR a revogou e trouxe novos pontos para atualizá-la. Mas qual foi a principal motivação para que o Brasil elaborasse, às pressas, uma regulamentação acerca dos dados pessoais?

Em 2017, houve uma sinalização de interesse do Brasil para ingressar à OCDE (Organização de Desenvolvimento Econômico). Para a entrada de novos países, há critérios rígidos que estes devem seguir e, entre eles, está o critério de lei de proteção de dados. Para isso, então, era necessário que o Brasil avançasse com a Lei de Proteção de Dados, motivo pelo qual sua aprovação foi tão rápida.

Além disso, o GDPR prevê que seus estados-membros só devem fazer negócios com países que possuam minimamente uma legislação acerca da proteção de dados, o que fez com que vários países começassem a se agilizar para promulgar leis acerca do tema. Desta forma, houve também pressão das empresas de tecnologia, que sentiam insegurança jurídica para troca de informações entre Brasil – EUA e Brasil – Europa, sem uma lei que tratasse minimamente de proteção de dados pessoais. Por tais razões, a criação da LGPD no Brasil ocorreu de forma relativamente rápida e teve como inspiração a GDPR europeia, que entrou em vigor na União Europeia em 25 de maio de 2018.

Aqui no Brasil, a primeira consulta pública acerca do tema de proteção de dados pessoais ocorreu em 2010, seguido de algumas leis relacionadas ao tema, como a Lei de Acesso à Informação (Lei nº 12.527/2011) e a Lei Carolina Dieckmann (Lei nº 12.737/2012) – que veio para tipificar crimes cometidos no ambiente virtual, promovendo alterações no Código Penal Brasileiro. Temos também o Marco Civil da Internet (Lei nº 12.965/2014), promulgado em 2014, cujo principal objetivo é a regulação da internet no Brasil, estabelecendo princípios, direitos e deveres no ambiente virtual.

A LGPD representa um marco na proteção e tratamento dos dados pessoais, trazendo diretrizes e conceitos. A publicação da lei ocorreu em agosto de 2018, mas sua entrada em vigor ocorreu apenas em 18 de setembro de 2020, em que pese as sanções administrativas só poderão ser aplicadas a partir de 01.08.2021 (Lei nº 14.010/2020).

3. PERSONAGENS E PAPÉIS NA LGPD

Além de toda a regulamentação sobre o tratamento de dados, a LGPD apresenta cinco personagens e seus papéis, cada qual com suas atribuições e responsabilidades e que, seguramente, passarão a fazer parte do dia-a-dia das empresas. São eles:

- Titular dos dados: é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, diga-se de passagem, é principal personagem da LGPD. Em outras palavras, somos nós, cidadãos que no dia-a-dia fornecem dados pessoais para as mais diversas finalidades: compras em empresas de forma presencial ou pela internet, para realizar consultas médicas, na admissão de um empregado pela empresa etc. Por isso a importância da LGPD pois a todo momento dados pessoais estão sendo fornecidos pelos titulares.
- Controlador: pode ser pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados e que se beneficia de alguma maneira pela utilização dos dados fornecidos pelos titulares. Cabe ao Controlador garantir que as normas previstas na LGPD sejam cumpridas, seja quando ele próprio trata dados pessoais, seja quando terceiriza em seu próprio nome. Ocorrendo danos aos titulares no tratamento de dados, o Controlador responde diretamente ou tem responsabilidade solidária quando o dano for causado pelo Operador que agiu sob suas ordens.
- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, podendo o próprio Controlador também atuar como Operador. Está sujeito a sanções sempre que causar dano ao titular de dados e responde de forma solidária junto com o Controlador quando não seguir as diretrizes impostas por este.

- Encarregado de Dados: também chamado de DPO (Data Protection Officer), é a pessoa física ou jurídica indicada pelo Controlador que, de acordo com a LGPD, atua como canal de comunicação entre o titular de dados, Controlador e Autoridade Nacional de Proteção de Dados (ANPD). Entretanto, outras funções e responsabilidades vêm sendo absorvidas pelo Encarregado, por força do próprio mercado, como por exemplo gerenciar o projeto de compliance de proteção de dados de acordo com a LGPD, fazer o monitoramento de processos que envolvam dados pessoais, desenvolver a cultura de privacidade nas organizações etc. Importante ressaltar que na LGPD não há previsão de sanção ou penalidade para o Encarregado no exercício da função, já que atua em nome do Controlador, cabendo tão somente a este e ao Operador eventual responsabilização.
- ANPD: Autoridade Nacional de Proteção de Dados é um órgão federal ligado à Presidência da República que tem como principal objetivo zelar pela proteção dos dados de pessoas físicas e definir as diretrizes relacionadas à Política Nacional de Proteção de Dados e Privacidade. É responsável ainda pela fiscalização quanto ao cumprimento da LGPD, podendo aplicar as sanções previstas na lei.

4. TIPOS DE DADOS PESSOAIS

A LGPD classificou em seu texto quatro tipos de dados. O primeiro e mais importante, o dado pessoal, é toda informação que identifica ou pode tornar identificável uma pessoa física. Como exemplos podemos citar nome, CPF, RG, sobrenome, endereço residencial, e-mail, características físicas, placa do automóvel, número do IP, dados acadêmicos, histórico de compras, entre outros.

Outra categoria de dados são os dados pessoais sensíveis, que são dados relacionados a característica da personalidade do indivíduo e suas escolhas pessoais, tais como: origem racial ou étnica, religião, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Temos o dado anonimizado que é o dado relativo ao titular que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Um exemplo de anonimização é apagar parte dos dados referente ao nome da pessoa e suas características pessoais, trocando-os por um número sem que seja possível realizar qualquer associação no futuro que permita identificar as pessoas por este número.

Por fim, temos o dado Pseudonimizado que é o dado que perde a possibilidade de ser associado a um indivíduo por si só e que precisa ser associado a mais alguma informação para se chegar a identificação de uma pessoa. Ex.: dado criptografado. Nesse caso, como o dado pseudonimizado não identifica uma pessoa e nem pode torná-la identificável, a LGPD não se aplica.

Uma curiosidade: a LGPD não atinge diretamente documentos confidenciais, segredos de negócios, fórmulas, algoritmos, direitos autorais ou propriedade industrial, que são protegidos por outras normas, mas somente eventuais dados pessoais que estejam dentro de tal tipo de conteúdo.

5. TRATAMENTO DE DADOS

Quando se fala em LGPD, inevitavelmente sempre se ouve a palavra Tratamento de dados, mas não se explica o que significa.

Tratamento de dados é tudo o que é feito com os dados pessoais, desde a coleta, utilização, transmissão, processamento, compartilhamento, arquivamento, até eliminação ou exclusão.

Os dados pessoais podem ser coletados de forma on-line (dados que fornecemos ao fazer uma comprar em um site) e de forma física (como o preenchimento de uma ficha cadastral para abertura de um crediário).

A LGPD enumera vinte operações de tratamento de dado pessoal, são elas: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

No entanto, é preciso ter em mente que para ocorrer o tratamento de dados pessoais necessário se faz utilizar uma das bases legais prevista na lei. Cabe lembrar que sempre que houver tratamento de dados, o agente de tratamento deve ter o registro da operação .

Por fim, ocorrerá o encerramento do tratamento de dados pessoais quando a finalidade foi alcançada ou os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada, com o fim do período de tratamento, quando o titular revogar o consentimento dado ou ainda por determinação da autoridade nacional quando houver violação da LGPD.

6. PRINCÍPIOS E HIPÓTESES DE TRATAMENTO

Além de trazer os conceitos acima, a LGPD determina a aplicação da boa-fé e baseia-se em princípios fundamentais que devem ser aplicados nas atividades de tratamento de dados, quais sejam:

- Finalidade: o tratamento de dados precisa ter propósitos legítimos, específicos e explícitos, com ciência do titular e sem possibilidade de tratamento posterior incompatível.
- Adequação: compatibilidade do tratamento com a finalidade informada, mantendo-se o mesmo contexto.
- Necessidade: o limite do tratamento deve ser o cumprimento de sua finalidade, de forma proporcional e não excessiva.
- Livre acesso: o titular tem a garantia de consulta facilitada e gratuita sobre seus dados, a forma e duração do tratamento.
- Qualidade dos dados: fica garantido a exatidão, clareza, relevância e atualização dos dados para cumprimento da finalidade.
- Transparência: garantia de informações claras, precisas e facilmente acessíveis sobre o tratamento e os agentes.
- Segurança: os dados devem estar protegidos de acessos não autorizados ou de situações acidentais ou ilícitas de vazamentos.
- Prevenção: devem ser adotadas medidas preventivas para evitar danos.

Essas bases legais são previstas na LGPD para que o agente possa fazer a coleta de dados pessoais e o tratamento, o que impede que as empresas utilizem os dados de forma ilimitada, ilegal ou para seu próprio benefício, gerando, assim, maior proteção ao titular dos dados.

Ao todo são dez bases legais, sendo que as empresas precisarão escolher a qual será mais adequada para justificar o tratamento do dado e, desta forma, estarem em conformidade com a LGPD, quais sejam:

- Consentimento do titular;
- Legítimo interesse;
- Cumprimento de obrigação legal ou regulatória;
- Tratamento pela administração pública;
- Realização de estudos e pesquisa;
- Execução ou preparação contratual;
- Exercício regular de direito;
- Proteção da vida e da incolumidade física;
- Tutela de saúde do titular;
- Proteção de crédito.

7. COMO SE ADEQUAR À LGPD

Inobstante os conceitos postos na LGPD, princípios, sanções e termos técnicos, o processo de adequação não é de alta complexidade. Como uma roupa sob medida, a implementação e adequação de um programa de privacidade e proteção de dados deve ser desenhado de acordo com o segmento da empresa, seu perfil e volume de dados tratados.

Iniciado o processo de adequação, em primeiro lugar, sem dúvida alguma, se faz necessário realizar um mapeamento de processos e de dados pessoais na empresa, como se dá o ciclo de vida dos dados (desde a coleta até o descarte), quais as bases legais utilizadas para o tratamento de dados e quais tipos de dados são tratados (há dados sensíveis?). Essa tarefa inicial é fundamental para permitir um diagnóstico inicial, viabilizar sua execução e dar efetividade a um programa de privacidade e proteção de dados.

Evidentemente que a depender do tamanho da empresa e o volume de dados tratados, uma alternativa seria a contratação de uma empresa especializada para realização do trabalho.

Outro passo importante é a criação de um Comitê de Privacidade e a nomeação de um Encarregado (também chamado de DPO- Data Protection Officer). O Encarregado será o principal responsável por gerenciar e monitorar o programa. É importante que o Encarregado tenha bom conhecimento na área de proteção de dados e da LGPD, o que não significa que deva ser necessariamente alguém da área de informática.

Como todo programa, existem documentos que vão evidenciar e registrar todo o processo de adequação que precisam ser elaborados pelo Controlador, em formato físico ou digital, como as políticas de privacidade e de cookies, política de segurança da informação, contratos com fornecedores, clientes, funcionários ou outros stakeholders contendo cláusulas de proteção de dados, termo de consentimento e o próprio relatório de impacto à proteção de dados.

Como não poderia deixar de ser, é necessário também que os colaboradores, diretoria e alta administração passem por treinamento a fim de criar uma cultura de proteção a dados. Investir em treinamento, cursos e workshops (em especial para aqueles que trabalharão diretamente no programa de proteção) é de fundamental importância.

Por fim, e não menos importante, é recomendado revisar e investir em ferramentas de proteção de dados para proteger e fortalecer a empresa contra eventuais ataques cibernéticos, pois os danos podem ser irreparáveis e ainda poderá haver responsabilização do Controlador por eventuais danos causados aos titulares de dados afetados.

7.1. Mapeamento de Dados

Dada a importância do mapeamento, será tratado neste item para melhor entendimento do leitor. E, neste particular, existem dois tipos de mapeamento, o de processos e o de dados.

O mapeamento de processos é uma técnica aplicada para ilustrar os fluxos de uma organização, procedendo da perspectiva macro do trabalho aos níveis hierárquicos dos subprocessos e das atividades executadas, identificando as informações necessárias para detalhar o modelo de negócios e serviços.

Já o mapeamento de dados é o processo de realizar um inventário dos dados que a organização coleta, processa e, em seguida, o que faz com estas informações, rastreando todo o seu ciclo de vida na empresa.

Para aplicar as tomadas de ações em conformidade com as exigências da LGPD, é importante ter uma compreensão clara dos fluxos de dados pessoais e/ou sensíveis sob o controle da organização. Isso envolve entender alguns fatores neste processo, como quais são os meios de entradas e saídas das informações, quais dados são coletados, para qual finalidade, qual é a base jurídica para o processamento destes dados, em qual local são armazenados, quem tem acesso, se há alterações, se são realizadas transferências, por qual período serão retidos e o que fazer com eles quando não forem mais necessários.

O mapeamento de dados é considerado como uma das etapas importantes para implantação do processo de conformidade com a LGPD. Para iniciar um bom mapeamento de dados é essencial realizar um primeiro diagnóstico a fim de conhecer as características da organização, identificando seu ramo de negócio, porte empresarial, suas bases legais e regulatórias, a quantidade de departamentos e funcionários, seguimento de clientes e públicos-alvo, bem como fornecedores ou outros vínculos terceirizados, as tecnologias inseridas e meios de comunicações internas e externas, seus fluxos macros e setoriais identificando cada instância onde os dados estão sendo processados, e sua maturidade na Cultura de segurança e proteção das informações.

Além da conformidade com a LGPD, o mapeamento de dados pode proporcionar a identificação das eficiências operacionais, bem como as fragilidades da organização como procedimentos excessivos e desnecessários, otimizando e agilizando as operações.

8. DIREITOS DOS TITULARES

A LGPD elenca inúmeros direitos dos titulares, os quais, de forma objetiva, indica-se abaixo:

- Acesso aos dados: Direito ao acesso a todos os dados pessoais de sua titularidade que estão sendo coletados e tratados pelo controlador. Cabe ao controlador fornecer o acesso fácil e gratuito a esses dados pessoais.
- Correção: Direito de correção a dados incompletos, inexatos ou desatualizados, mantendo a qualidade dos dados atualizados.
- Consentimento: Direito de restringir o tratamento de dados pessoais, por meio da recusa em dar o consentimento.
- Anonimização, bloqueio ou eliminação de dados desnecessários: Direito de solicitar e questionar os dados desnecessários, excessivos ou tratados em desconformidade com a LGPD ou cujo consentimento foi revogado pelo titular.
- Portabilidade: Direito de transferir todos os seus dados pessoais que tenham sido fornecidos a um controlador, inclusive de forma eletrônica e que possam ser acessados por outros sistemas, para outro fornecedor, mediante solicitação do titular.
- Compartilhamento: Informações das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.
- Revogação de consentimento: Direito de revogar o consentimento dado para tratamento dos dados pessoais a qualquer momento, mediante manifestação expressa, de forma gratuita e facilitada.
- Oposição: o titular dos dados tem o direito de se opor a quaisquer tratamento de dados e informações que não estejam em conformidade com a lei.
- Confirmação da existência: o titular dos dados tem direito de receber informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados pelo controlador para a tomada de decisão com base em tratamento automatizado de dados pessoais .
- Reclamação contra o controlador: Direito de abrir reclamação junto à autoridade nacional – ANPD.

- Revisão de decisões tomadas: solicitação de revisão de perfil com base em tratamento automatizado.
- Eliminação: Direito a informações claras sobre as consequências da negativa do consentimento. Eliminação dos dados pessoais tratados com o consentimento do titular.

Como se percebe, a lei conferiu ao titular dos dados, personagem principal da LGPD e dono dos dados, a autonomia necessária para dispor sobre seus dados.

9. PLANO DE CONFORMIDADE E ADEQUAÇÃO

A fim de demonstrar a conformidade da empresa com a LGPD, mantê-la constantemente alerta para ajustes e melhorias necessárias e orientá-la quanto à adequação de seus processos envolvendo dados, a confecção de um Plano de Conformidade e Adequação é o entregável ideal para essa etapa.

Esse plano pode ser construído de forma customizada ao negócio, mas sem deixar de observar as recomendações da ANPD e as melhores práticas de mercado, as quais se destacam as seguintes:

- Nomeação de um Encarregado (DPO) pela empresa que pode ser funcionário da organização ou também uma empresa terceirizada conforme já abordado neste guia;
- Constituição de um comitê de privacidade de dados, também já citado, não é uma medida obrigatória, mas em empresas de grande porte é comum a criação de um Comitê de Privacidade formado por profissionais com formações multidisciplinares;
- Mapeamento de dados e processos, já tratado em tópico anterior;
- Análise de controles, que pode ser dividido sob dois enfoques, o primeiro relacionado à tecnologia e o segundo relacionado aos processos;
- Indicadores de monitoramento, o que se justifica por se tratar de um Plano de Conformidade. Uma vez a organização

estando adequada à Lei, é preciso que o monitoramento do ciclo permaneça ocorrendo. Para isso, recomenda-se criar e monitorar os indicadores, sem deixar de realizar a comunicação com todos os envolvidos no processo.

Ademais, é sempre bom sugerir ou apontar as melhorias necessárias, investir e reforçar constantemente o compromisso da organização com a Lei Geral de Proteção de Dados.

10. SANÇÕES

A LGPD também prevê sanções administrativas em caso de descumprimento da lei, a serem aplicadas pela ANPD, que vão desde advertências até multas elevadas.

Contudo, tais sanções somente poderão ser aplicadas a partir de 1º de agosto de 2021 (lei 14.010/2020).

De qualquer sorte, inobstante a ANPD só possa aplicar sanções administrativas a partir da data indicada, com a vigência da LGPD qualquer titular de dados, órgãos de defesa e proteção do consumidor e também autoridades públicas que identificarem violações à lei, podem acionar o controlador judicialmente.

Pois bem, voltando as sanções administrativas, segundo a LGPD poderão ser aplicadas as seguintes penalidades pela autoridade nacional:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- Multa diária, observado o limite posto na lei;
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- Eliminação dos dados pessoais a que se refere a infração.

É importante destacar que a ANPD, ao aplicar as penalidades previstas na lei levará em consideração a gravidade e a natureza das infrações e dos direitos pessoais afetados, a boa-fé do infrator, a vantagem auferida ou pretendida e a condição econômica do infrator, a reincidência, o grau do dano, a cooperação do infrator, a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, a adoção de política de boas práticas e governança, se adotou medidas corretivas e, por fim, a sanção deverá ser proporcional à gravidade da falta cometida.

11. DESAFIOS DA LGPD

11.1 – Para Empresas

Em que esse as inovações trazidas com a LGPD, o que evidencia um avanço sobre o tema e deve ser comemorado, não há como deixar de reconhecer que muitos desafios ainda estão por vir, sobretudo para empresas.

Nesse sentido, há que se mencionar que vários pontos da lei necessitam de regulamentação e vão demandar que a ANPD se pronuncie a respeito, dentre os quais se destaca:

- Como se dará o processo de apuração de incidentes de segurança?
- Qual será o prazo para resposta a um incidente de segurança?
- A nomeação de Encarregado será obrigatório para MEI e empresas de pequeno porte?
- Será possível compensação de dados pessoais nos casos de vazamento, violações e “maus-tratos”?
- Será exigido um padrão ou certificação para validar uma adequação à LGPD feita pelas empresas?
- Como ficam as empresas que não têm recursos técnicos para estar em conformidade com a LGPD, principalmente as micro, pequenas e MEI?

Os desafios não são poucos e a ANPD terá muito trabalho pela frente.

11.2 Para Titulares de Dados

Assim como para as empresas, para os titulares de dados os desafios são grandes e é provável que o maior deles seja entender a lei e cobrar das empresas o devido cumprimento.

Mas não é só, algumas questões vêm à tona que merecem atenção:

- Como garantir que as empresas farão o tratamento de dados dos titulares de forma transparente e dentro das previsões legais?
- Como garantir que o titular de dados no Brasil tenha acesso ao Encarregado de dados de empresa digital com sede no exterior, mas que mantém negócios no Brasil?
- Será possível garantir que dados perdidos sejam recuperados ou haja compensação de perdas?

A Lei acabou de sair do forno, não há certeza de como será sua reverberação no mercado e como será encarada pelo judiciário quando uma controvérsia for instaurada, então por enquanto o que se tem são incertezas, dúvidas e especulações.

12. CONCLUSÃO

Sabemos que a jornada de adequação à LGPD não é rápida e nem simples. É preciso o envolvimento de diversos players, muito investimento em treinamento e mudança de hábitos. No entanto, qualquer transformação cultural deve superar desafios como esses.

Dentro do seu processo de implementação da Lei, atente-se para a composição de um time multidisciplinar. Não é por se tratar de uma lei que seu desafio se restringe a questões jurídicas - pelo contrário. E, claro: coloque o titular no centro de tudo.

Estamos falando de mais do que obedecer à legislação, mas criar uma cultura de respeito à individualidade e à privacidade de cada um. Práticas ostensivas e abordagens indesejadas não devem mais ser aceitas como algo comum.

Enquanto grandes responsáveis pelo estabelecimento de uma cultura, portanto, as organizações têm papel fundamental nesse trabalho, e para elas que esse material foi feito.

Esperamos que nosso trabalho dê suporte para suas principais dúvidas em relação à LGPD.

Promovendo a cultura do compliance

IPACOM
INSTITUTO PARANAENSE DE COMPLIANCE

QUEM SOMOS

Fundado em 2017 na cidade de Curitiba, Paraná, o Instituto Paranaense de Compliance – IPACOM –, sociedade civil de direito privado e sem fins lucrativos, foi criado com o objetivo de contribuir para a formação e o aperfeiçoamento das organizações e dos profissionais que atuem, direta ou indiretamente, com a área de compliance no estado do Paraná.

Através de cursos, eventos, congressos, palestras, debates, núcleos de estudo, seminários, workshops, parcerias e outras atividades, o IPACOM busca cooperar para a difusão da cultura do compliance, da integridade e da transparência nas atividades exercidas por estas organizações e pelos profissionais em seus negócios.

Também estão em nossos objetivos firmar convênios e manter relacionamento com entidades de direito público para propor e colaborar com pesquisas, identificar problemas e sugerir soluções para a realização de tarefas voltadas às questões de compliance.

Para saber mais informações basta entrar em contato com nossa equipe através dos nossos canais:

http://ipacom.org

https://br.linkedin.com/company/ipacom