CHRISTIAN TEIXEIRA
ADVOGADOS

Cartilha LGPD

JULHO/2021

SUMÁRIO

“Todos temos três vidas.
A vida pública,
a vida privada e
a vida secreta”

Gabriel García Marquez

A LGPD

A Lei nº 13.709/2018 – Lei Geral de Proteção de Dados – LGPD, foi aprovada em agosto de 2018 e entrou em vigência a partir de 14 de agosto de 2020. O assunto é de suma importância, pois visa à segurança jurídica, padronizando normas e práticas, promovendo a proteção de dados pessoais de todos os cidadãos, em âmbito nacional.

A elaboração da LGPD foi pautada no General Data Protection Regulation (GDPR), Regulamento de Proteção de Dados da União Europeia. Em 2016, foi apresentado ao Parlamento Europeu o Regulamento Geral de Proteção de Dados que está em vigor na Europa desde 2018.

INTRODUÇÃO

A LGPD regula a atividade sobre o uso de dados pessoais, de colaboradores e de terceiros, por todos os tipos de organizações que operam em território brasileiro, estabelecendo rigorosas sanções, em caso de descumprimento de suas determinações.

No Brasil, a proteção de dados possui natureza jurídica de direito e garantia fundamental, com base no inciso XII-A do art. 5º e o inciso XXX do art. 22 da Constituição Federal, acrescentados pela Emenda Constitucional nº 17, que altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Sua aplicação se estende a qualquer pessoa, natural ou jurídica, de direito público ou privado, que realize o tratamento de dados pessoais, online e/ou offline.

Assim, a importância da referida Lei se reflete em maior segurança jurídica e proteção aos direitos dos titulares de dados. Os dados deverão ser utilizados apenas para as finalidades específicas para as quais foram coletados e devidamente informadas aos titulares (Princípio da Finalidade).

Somente devem ser colhidos os dados mínimos necessários para que se possa atingir a finalidade (Princípio da Minimização da Coleta). Após alcançada a finalidade pela qual eles foram coletados, deve ser feita a imediata exclusão dos dados (Princípio da Retenção Mínima).

PONTOS IMPORTANTES

• ABRANGÊNCIA:

Quaisquer dados pessoais obtidos em qualquer tipo de suporte (papel, eletrônico, em ambiente virtual, som, imagem, etc.).

• FISCALIZAÇÃO CENTRALIZADA:

Ficará a critério da Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

• RESPONSABILIDADE CIVIL:

O responsável que, em razão do exercício de atividade de tratamento de dados, causar dano patrimonial, moral, individual ou coletivo, será obrigado a repará-lo.

• FINALIDADE E NECESSIDADE:

Os quesitos de tratamento devem ser previamente informados aos titulares.

• REGRA PARA TODOS:

Criação de um panorama de segurança jurídica para todo o país e em nosso contexto, para todas as empresas.

• CONTRATOS DE ADESÃO:

Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou serviço, o titular deverá ser claramente informado.

• TRANSPARÊNCIA:

Ocorrendo vazamento de dados, a ANPD e os indivíduos afetados, devem ser comunicados.

CONCEITOS DA LGPD

• **AGENTES DE TRATAMENTO**: o controlador e o operador;

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

• **AUTORIDADE NACIONAL (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei;

• **BANCO DE DADOS:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

• **BLOQUEIO:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

• **CONSENTIMENTO:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

• **DADO PESSOAL:** informação relacionada à pessoa natural identificada ou identificável. Essa informação representa todo e qualquer dado que possa tornar uma pessoa identificável, seja ela diretamente relacionada ao seu titular (como um nome ou número de documento) ou mesmo indiretamente relacionada, mas com potencial de identificá-lo (a) (como endereço, idade, informações sobre hábitos de compra etc);

• **CONTROLADOR:** pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais;

• **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;

• **ELIMINAÇÃO:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

• **ENCARREGADO (DPO):** 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;

• **OPERADOR:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

• **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;

• **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.

• **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 e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

• **TITULAR:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

• **TRANSFERÊNCIA INTERNACIONAL DE DADOS:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

• **USO COMPARTILHADO DE DADOS:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por entidades e órgãos públicos no cumprimento de suas competências legais, ou entre entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

• **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.

PRINCÍPIOS DA LGPD

As condutas conceituadas como “tratamento da informação” deverá observar os seguintes princípios:

• **ADEQUAÇÃO** - compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

• **FINALIDADE** - realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

• **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;

• **NÃO DISCRIMINAÇÃO** - impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos;

• **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;

• **PREVENÇÃO:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

• **QUALIDADE DOS DADOS:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

• **RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas;

• **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 das informações sob custódia.

• **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.

PRIVACIDADE DOS DADOS PESSOAIS

Na atualidade, a informação tornou-se um dos bens mais valiosos.

A frase “dados são o novo petróleo”, em tradução livre para a original “data is the new oil”, foi criada por Clive Humby, um matemático londrino especializado em ciência de dados.

Diariamente, usamos, absorvemos, produzimos e transmitimos informações o tempo todo. ALGPD assegura a toda pessoa natural a titularidade de seus dados pessoais e garantia dos direitos fundamentais de liberdade, intimidade e privacidade. Desta forma, podemos afirmar que um dos grandes desafios contemporâneos é assegurar a proteção e a privacidade para estes dados. Esta garantia

se aplica independente do meio ou forma de tratamento dos dados coletados ou recebidos, incorrendo que todo aquele que faz uso do dado deve observar as regras legais. Desta forma, para que haja o cumprimento das obrigações e procedimentos previstos na lei, o conceito de privacidade dos dados pessoais deverá nortear qualquer tratamento de dados realizado pelos controladores.

CRITÉRIOS PARA O USO DE DADOS

Os dados pessoais somente poderão ser tratados em duas hipóteses:

1º - Consentimento

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

DICA: O Consentimento é granular, não admite interpretação extensiva.

2º Base Legal – Art. 7º da LGPD

• Para o cumprimento de obrigação legal ou regulatória pelo responsável pelo tratamento;

• Para a realização de estudos por órgão de pesquisa, sem a individualização a pessoa;

• Para o exercício regular de direitos em processos judicial, administrativo ou arbitral;

• Para execução de contrato ou procedimentos preliminares relacionados a um contrato;

• Pela administração pública, para o uso compartilhado de dados necessários à execução de políticas públicas;

• Para a tutela da saúde, com procedimento realizado por profissionais da área ou por entidades sanitárias;

• Para a proteção do crédito, nos termos do Código de Defesa do Consumidor.

Exceto quanto as hipóteses legais, a regra é: **o titular sempre deverá consentir para o uso de seus dados.**

DICA: O tratamento de dados tem início, meio e fim.

PROGRAMA DE IMPLEMENTAÇÃO

• Conseguir o **envolvimento dos gestores** desde o início do plano de adequação para que a proteção de dados pessoais esteja incorporada aos princípios da Empresa e assim o tema ganhe engajamento e a força necessária;

• **Estabelecer as ações e um gestor líder para o plano**, identificando os principais projetos e áreas da empresa afetadas pela LGPD e eventuais legislações setoriais;

• **Criar um programa de governança em proteção de dados** com a elaboração de medidas e controles para o acompanhamento da implantação de padrões que estejam em conformidade com a LGPD e legislações setoriais aplicáveis;

• Elaborar e **rever documentos jurídicos com a realização de eventuais adendos aos contratos existentes** para adequação aos padrões de proteção de dados, principalmente para aqueles que envolvam o tratamento e compartilhamento de dados pessoais;

• **Garantir o exercício dos direitos dos titulares**, mediamente a confirmação da implementação de medidas técnicas e organizacionais;

• **Realizar treinamentos internos** para apresentação das novas políticas de proteção de dados pessoais e disseminação da cultura sobre o tema.

A IMPLEMENTAÇÃO DA LGPD está pautada em 3 principais pilares:

IMPLANTAÇÃO | RELACIONAMENTO | MONITORAMENTO

DICA: O elo mais importante é a conscientização.

AÇÕES BÁSICAS DE IMPLANTAÇÃO

Buscando a implementação da LGPD, sugerimos algumas ações básicas como:

1º - NOMEAÇÃO DO DPO

Você sabe quem é o Data Protection Officer (DPO)? A partir de agora, após a Lei Geral de Proteção de Dados (LGPD) entrar em vigor, muitas empresas vão precisar desse profissional.

Ele é Encarregado de Proteção de Dados (Data Protection Officer – DPO).

A ideia é que após a LGPD as empresas tenham alguém para cuidar da proteção de dados pessoais dos titulares (clientes, funcionários, fornecedores, indivíduos de fora da organização ou ambos). Por isso, a norma exige que as empresas que efetivem o tratamento de dados de terceiros tenham um DPO.

Quem pode ser o DPO

A LGPD define os dois tipos de empresas que têm responsabilidades, deveres jurídicos e penalizações específicas:

• Controlador – Empresa que toma as decisões referentes ao tratamento de dados pessoais

• Operador – Empresa que realiza o tratamento dos dados em nome do controlador.

O DPO pode ser um membro da empresa controladora ou operadora. As organizações relacionadas podem usar o mesmo indivíduo para supervisionar a proteção de dados coletivamente, desde que todas as atividades sejam gerenciadas com eficácia.

Neste cenário, o DPO deve ser facilmente acessível por qualquer pessoa de qualquer uma das organizações relacionadas, sempre que for preciso. É necessário

que as informações do DPO sejam divulgadas publicamente e fornecidas à Autoridade Nacional de Proteção de Dados (ANPD).

Para entender quem pode ser o DPO, primeiro é aconselhável que este cargo deve ser designado a alguém com experiência em leis e práticas de proteção de dados. Além disso, o DPO deve ter entendimento completo da infraestrutura de TI, tecnologia e estrutura técnica e organizacional da empresa.

O DPO pode ser um funcionário da empresa? Sim. Desde que as tarefas do funcionário sejam compatíveis com os deveres do DPO e não levem a um conflito de interesses. Então, a empresa pode nomear um funcionário existente como seu DPO, em vez de criar um novo cargo.
É possível terceirizar o DPO? As empresas podem terceirizar o DPO, com base em um contrato de serviço com um indivíduo ou uma organização, o que chamamos de DPOaaS (DPO as a Service). É importante estar ciente de que um DPO externo deve ter o mesmo cargo, tarefas e deveres que um nomeado internamente.

O DPO é responsável pela conformidade? O DPO não é especificamente responsável pela conformidade da proteção de dados. Como controlador ou processador, é responsabilidade da empresa cumprir o que diz a LGPD. Entretanto, o DPO desempenha um papel crucial em ajudar as empresas a cumprirem as obrigações de proteção de dados.

Chegamos então à conclusão que as empresas precisam ter um DPO, pois esta figura irá ajudá-la a ter uma boa reputação quanto à proteção e privacidade de dados e também a operar em conformidade com a LGPD.

E que o DPO precisa ter excelentes habilidades de gestão e muito conhecimento sobre segurança da informação para garantir a conformidade interna e ainda alertar as autoridades sobre o não-conformidade, se tal evento ocorrer.

2º - MAPEAMENTO DE DADOS

Este levantamento poderá ser feito a partir da análise dos seguintes pontos:

• Tipos de dados comuns e sensíveis que fazem parte dos processos da empresa;

• Local em que ficam armazenados;

• Forma de tratamento;

• Por onde trafegam;

• Relação de profissionais que têm acesso aos dados e qual o tipo de acesso que cada um deles tem;

• Mecanismos de controle disponíveis para a aplicação da política interna de proteção;

• Profissional qualificado para análise e atualização da política interna de proteção de dados, caso necessário;

• Pontos frágeis e estratégias para minimizá-los;

• Se os dados foram avaliados e classificados de forma apropriada seguindo os conceitos atuais da LGPD.

3º - REVISÃO DE CONSENTIMENTO

Agora que a empresa já sabe sua matriz de dados, é fundamental fazer a revisão do consentimento desses dados. Ou seja, ou a autorização é de base legal, de consentimento ou o dado não pode ser tratado pela empresa.

BASE LEGADO: Continuar usando, eliminar ou pedir consentimento?

DICA: É fundamental e oportuno diminuir o volume de dados como medida de diminuição de risco.

4º - DEFINIÇÃO DE FLUXO DE DADOS

Com base nestas informações, será possível identificar os sistemas e a equipe que lida diretamente com os dados pessoais e conhecer os pontos de risco da atual segurança de dados, ajudando a consolidar uma política interna eficaz em relação às normas da LGPD.

Assim, após o mapeamento dos dados, é fundamental estabelecer um novo fluxo de dados, obviamente o mais enxuto possível.

Criado este panorama, a empresa deve ainda estabelecer um Comitê de Segurança da Informação para analisar os procedimentos internos. Dentro deste Comitê haverá o encarregado exclusivo para a proteção dos dados e responsável pelo cumprimento da nova lei, o Data Protection Officer (DPO).

Considerando ainda que a Autoridade Nacional de Proteção de Dados (ANPD) pode solicitar a comprovação do cumprimento da lei, recomenda-se que seja elaborado um Manual de Boas Práticas e de Governança em privacidade.

E como dito, o primeiro passo para implementação da referida lei é fazer o mapeamento de dados, que consiste em identificar e categorizar toda e qualquer relação de coleta, armazenamento e tratamento dos dados sensíveis de seu órgão público ou entidade.

5º - ADEQUAÇÃO CONTRATUAL

A empresa deve se adequar contratualmente à LGPD, para tanto deve elaborar e rever documentos jurídicos com a realização de eventuais adendos aos contratos existentes para adequação aos padrões de proteção de dados, principalmente para aqueles que envolvam o tratamento e compartilhamento de dados pessoais.

Exemplos de Contratos e Termos que devem ser revistos:

- Termos de Uso de Site;
- Política de Privacidade;
- Contrato de Trabalho;
- Contrato de Confidencialidade;
- Termo de Consentimento;
- Código de Conduta;
- Cláusulas contratuais em contratos com fornecedores;

6º - MITIGAÇÃO DE RISCOS

Considerando que o incidente é inevitável, a Empresa deve fazer tudo o que estiver ao seu alcance para evitá-lo e estar preparada para mitigar o incidente na ocasião da ocorrência, para isso **deve ter um Protocolo de Emergência pronto**.

São referências importantes para a gestão de segurança da informação a base para a certificação ISO 27001 e 27002. O que compõe a segurança da informação:

DADOS | CONFIDENCIALIDADE | INTEGRALIDADE | DISPONIBILIDADE

Matriz de risco:

- Quais são os principais ativos da empresa;
- Quem são os adversários principais;
- Quais são as fontes de ameaça;
- Qual o impacto se o pior acontecer;
- Como esse impacto será quantificado;
- Frequência desse risco;

Dica: Existe um seguro específico para riscos cibernéticos.

RELACIONAMENTO

Uma vez implantada a LGPD, a empresa deve criar canais de fácil acesso e mecanismos para garantir o direito dos titulares, prestando as informações pertinentes e adotando as providências necessárias segundo o regramento da LGPD.

E não só deve se relacionar com os Titulares mas também com a Autoridade Nacional de Proteção de Dados, estando apta a prestar as informações necessárias.

DICA: Facilite a saída dos seus leads. A saída deve ser tão fácil como a entrada.

MONITORAMENTO

Tão importante quanto a implantação e o relacionamento é o monitoramento. Boa parte dos vazamentos de dados sequer é notada pela parte prejudicada. A empresa deve adotar uma prática proativa em razão da LGPD, efetuando regularmente:

- Treinamento rotineiro da equipe;
- Auditorias de Consentimento;
- Periódicas testagens dos mecanismos de segurança;
- Testagem do Protocolo de Emergência;
- Monitoramento da internet;
- Estudo de casos.

DICA: Discursos diários de Segurança – DDS – é uma prática muito eficaz.

INCIDENTES

- **Invasão ao Twitter: suspeito de 22 anos é preso na Espanha**

> 21/07/2021 às 13:06

Netflix, LinkedIn, Last.FM e outros – 1,4 bilhão de senhas vazadas

No fim de 2017, foi encontrado um arquivo que reúne mais de 1,4 bilhão de nomes de usuários e senhas de diversos sites, como Netflix, LinkedIn, MySpace, Las.FM, Minecraft e YouPorn.

O arquivo era organizado por ordem alfabética e frequentemente atualizado pelos hackers. Ele poderia ser facilmente encontrado por meio de plataformas para download de torrents e na dark web (uma parte da deep web onde são compartilhadas informações ilegais).

Apesar de a Netflix ter negado o vazamento, especialistas que tiveram acesso ao arquivo que compilava as senhas afirmaram que muitas delas estavam corretas.

Hacker preso por megavazamento de dados tem 24 anos e vive em Uberlândia; ele também é suspeito de invadir o Senado, o Exército e o TSE

> 19/03/2021 às 09h21

Após hacker exigir US$ 1 milhão para devolver dados, cartório cria sistema próprio em Caxias do Sul. Somente nesta semana, outras três empresas da cidade tiveram plataformas virtuais bloqueadas. 03/07/2019 – 18h00min

O **ransomware**, como é conhecido este tipo de crime, é um cyberataque feito por hackers que **bloqueiam dispositivos e cobram resgate** para devolver o acesso.

De acordo com o Internet Threat Security Report (ISTR 2016), em 2015 **mais de 1,5 milhões de malwares foram criados por dia**, com mais de 430,5 milhões de ocorrências registradas pela Symantec – referência em segurança na internet – cerca de 35% a mais do que no ano anterior.

• Ataque Hacker ao Facebook gera o bloqueio de 90 milhões de contas!

Invasão ao Ashley Madison (2015)

Imagina a vergonha de ver toda a internet descobrindo que você estava traindo seu cônjuge? Pois é. Em 2015, um grupo autodenominado The Impact Team, ou O Time de Impacto, invadiu os servidores do site de traição Ashley Madison e alertou em público que, se os responsáveis pelo serviço não o desligassem imediatamente, eles iam divulgar informações privadas de seus usuários.

A diretoria da plataforma não deu muita atenção para a ameaça. Bom, hacker promete, hacker faz. Um arquivo que pesava 25 gigabytes foi publicado na web e lá dentro estava nomes, endereços e outros dados de quase 40 milhões de usuários do Ashley Madison. Esse ataque merece entrar na nossa lista pelos impactos que ele causou. Além de ter feito muita gente se divorciar por aí, **o vazamento culminou em três suicídios.**

DICA: O incidente é inevitável. Esteja preparado para ele.

PENALIDADES

A partir de agora, além dos prejuízos causados pelo vazamento de dados, multas serão aplicadas aos descuidados.

O tratamento de dados deverá ser feito com a máxima prudência, visto que a Lei Geral de Proteção de Dados, em seu artigo 52, prevê sanções em caso de infrações, conforme segue:

A - Advertência, indicando o prazo para adoção de medidas corretivas;

B - Multa simples, de até 2% (dois por cento) do faturamento do grupo no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

C - Multa diária, observado o limite total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

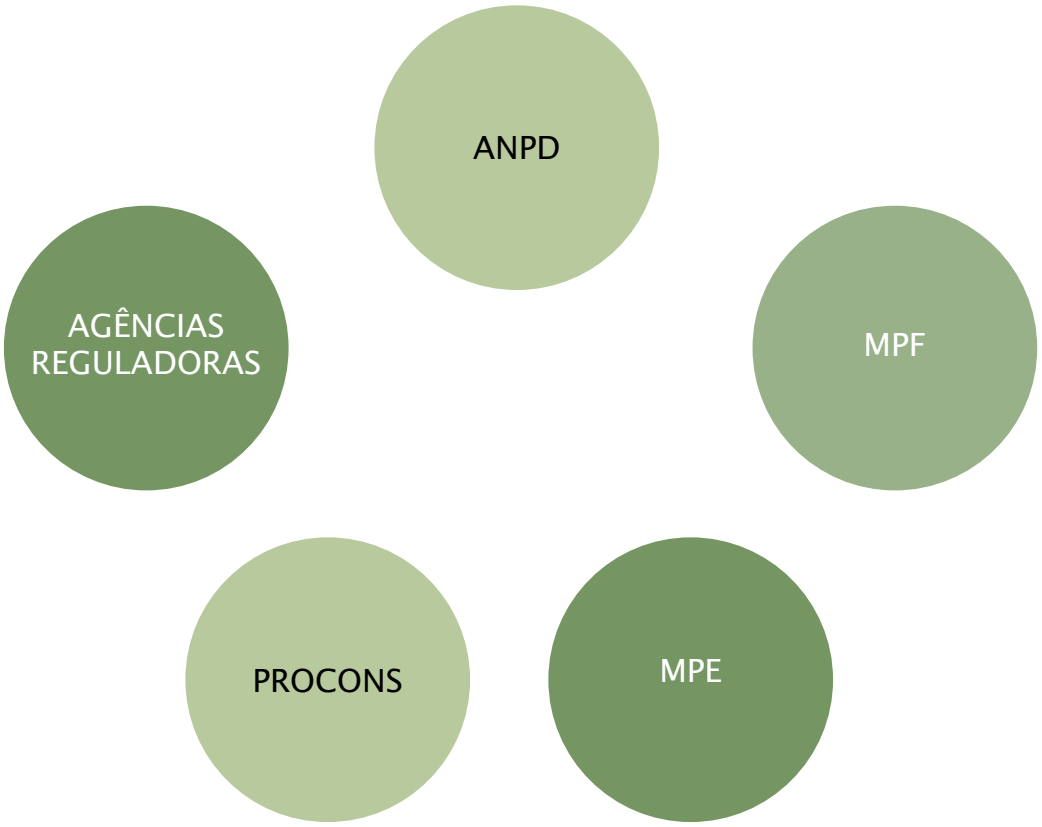
D - Publicização da infração após devidamente apurada e confirmada a sua ocorrência;

E - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

F - Eliminação dos dados pessoais a que se refere a infração.

A fiscalização e aplicação das penalidades elencadas acima, serão feitas pela Autoridade Nacional de Proteção de Dados (ANPD). A Lei nº 14.010, de 10 de junho de 2020, definiu que as sanções previstas na LGPD serão aplicadas **a partir de agosto de 2021**.

MÚLTIPLA FISCALIZAÇÃO E POSSIBILIDADE DE MÚLTIPLAS MULTAS



RESPONSABILIDADE E RESSARCIMENTO DE DANOS

O tratamento de dados pessoais está centralizado em dois agentes, sendo o controlador e o operador, definidos neste material.

De acordo com a legislação, os operadores devem realizar o tratamento de dados conforme as instruções fornecidas pelo controlador, que possui obrigações mais intensivas. **Regra geral, a responsabilidade entre tais agentes não é solidária.**

As responsabilidades são distintas, podendo ser maiores, no caso do controlador e menores para o operador. **O art. 42 da LGPD estabelece que o controlador ou o operador que causar dano patrimonial, moral, individual ou coletivo, no exercício da atividade, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.**

CONSIDERAÇÕES FINAIS

Em relação aos dados pessoais armazenados nos bancos de dados da empresa, é imprescindível identificar o consentimento do titular para qualquer tratamento de dados ou a base legal que autorize o seu tratamento.

Não identificado o suporte de autorização, os dados devem ser eliminados.

FUNDAMENTOS LEGAIS BRASIL:

- Constituição Federal de 1988. BRASIL;
- Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. BRASIL;
- Lei nº 10.406 de 2002, Código Civil. BRASIL;
- Código de Defesa do Consumidor, Lei 8.078/90, BRASIL;
- Decreto 7.962/2013, BRASIL;

CHRISTIAN TEIXEIRA
ADVOGADOS

Cartilha LGPD

chteixeira.adv.br
@christianteixeiraadvogados
@chteixeira2019

2002 2021 15 ANOS

JULHO/2021