COMISSÃO DE ESTUDOS EM COMPLIANCE

COMPLIANCE, LGPD E A ADVOCACIA

ABRIL/2021

SUMÁRIO

1. Prefácio

2. Apresentação

3. Introdução

4. Conceitos da LGPD

5. Fundamentos da LGPD

6. Princípios

7. Bases Legais

8. Boas Práticas de Governança em Privacidade e Proteção de Dados

9. Medidas para estar em Compliance com a LGPD

10. Penalidades

11. Conclusão

12. Referências Bibliográficas

1

PREFÁCIO

Quantos dados pessoais passam por nossas mesas de trabalho todos os dias? O que eles dizem sobre cada uma das pessoas que atendemos? De certa forma, o tema da proteção de dados, que ganha força com a **Lei Geral de Proteção de Dados (LGPD)**, não é novidade para os advogados. Intrínseca à nossa atividade temos a prerrogativa do sigilo e a confidencialidade, decorrentes da relação de confiança entre nós e nossos clientes. Estamos acostumados a compreender nossos locais de trabalho como seguros para as informações de nossos clientes. À nossa prerrogativa, somam-se agora deveres concretos para a proteção específica dos dados pessoais.

Evidentemente, a confidencialidade na relação com nossos clientes abrange todos os dados aos quais temos acesso e não apenas aos pessoais. Enquanto a proteção de dados pessoais estende suas garantias a qualquer titular de dados e não apenas aos nossos clientes. Mas é importante chamar a atenção para esta intersecção existente para enraizar o tema entre nós. A nossa preocupação com a garantia dos direitos e liberdades fundamentais não é nova. A LGPD traz apenas uma nova dimensão a ela.

A Comissão de Estudos em Compliance da OAB Subseção Campinas elaborou essa Cartilha que servirá de guia inicial para se familiarizar com os conceitos e os princípios trazidos pela lei. Além disso, ela traz uma perspectiva chave: as boas práticas de Governança em Privacidade. Elas aparecem ao final da lei, como faculdade a todos que tratam dados pessoais, quase ofuscadas entre as normas de responsabilidade e segurança e as sanções administrativas. Curiosamente, sem elas será difícil estar em conformidade com as demais normas.

A perspectiva mais importante desta Cartilha e para a qual gostaria de chamar particularmente sua atenção é a de que a conformidade com a LGPD não está em uma entrega específica – uma revisão de contrato, uma política interna, um aviso de privacidade, por exemplo – nem em um conjunto delas.

Para os profissionais de *Compliance*, como os colegas que generosamente elaboraram essa Cartilha, é claro compreender a estruturação de Governança como necessária para o cumprimento de qualquer legislação: anticorrupção, fiscal, trabalhista, ambiental, para nomear as mais conhecidas. A importante perspectiva compartilhada por eles é a de que o mesmo ocorre para a legislação de proteção de dados e nesse caso, a própria lei nos aponta o caminho.

A proteção de dados precisa estar enraizada em nossas rotinas, em nossas atividades cotidianas. Precisa ser um valor reafirmado dentro de nossas organizações. Por isso, iniciei com a lembrança de que apesar de nova a lei, ela nos traz um valor que já carregamos conosco. Seja para adequar nossos próprios escritórios, como todos temos a obrigação de fazer; seja para auxiliar nossos clientes, como muitos de nós temos feito, essa Cartilha empresta os olhos do *Compliance* para que possamos ver a proteção de dados pessoais como um caminho a ser trilhado. E está apenas começando.

Nuria López

Sócia da área de Tecnologia, Privacidade e Proteção de Dados da Daniel Advogados. Doutora em Teoria e Filosofia do Direito pela PUC-SP.

Em todo o globo, o fluxo e troca de informações aumentaram exponencialmente nas últimas décadas. Vazamento de dados e segurança da informação se tornaram uma recorrente notícia em nosso cotidiano e por esta razão, hoje vivemos a preocupação com as consequências jurídicas destes incidentes.

Inspirada na Lei Europeia, General Data Protection Regulation (GDPR), a Lei nº 13.709/18, denominada **Lei Geral de Proteção de Dados Pessoais**, inovou trazendo a tutela dos direitos e suas diretrizes à proteção e privacidade dos dados pessoais.

E para garantir que os entes em atividades econômicas que tratam dados pessoais, sejam eles empresas ou até mesmo escritórios de advocacia, estejam em Compliance com esta Lei, há a necessidade de seu estudo e adoção de um programa de governança.

E desta forma, a **Comissão em Estudos de Compliance da OAB Subseção Campinas**, pretende abordar este tema trazendo aspectos relevantes da lei e sua adequação, abrangendo inclusive requisitos a serem observados para a comunidade jurídica.

O material tem o condão de trazer elementos essenciais, mas também traz reflexões e inquietações, pois trata-se de uma legislação nova e sujeita ainda a interpretações e definições por parte da Autoridade Nacional de Proteção de Dados.

Espero que tirem proveito deste material, que foi feito com muito carinho por membros da comissão para a advocacia campineira, e nos colocamos à disposição para permanecermos no debate sobre o tema através de nosso e-mail compliance@oabcampinas.org.br

Daniela Reni Dorian Martinez

Presidente da Comissão de Estudos em Compliance da OAB Campinas

3
INTRODUÇÃO

O tema desta cartilha é a Lei nº 13.709/2018, conhecida como a **Lei Geral de Proteção de Dados Pessoais**, ou simplesmente LGPD.

Publicada em 14 de agosto de 2018, a lei teria inicialmente uma *vacatio legis* de 18 meses, porém já no mesmo ano foi prorrogada para vigorar em 24 meses.

Entre idas e vindas de medidas provisórias e projetos de leis, todos visando um novo adiamento para o ano de 2021, a LGPD entrou de fato em vigor em 18 de setembro de 2020.

Ressalte-se que os artigos 52, 53 e 54 que tratam das sanções administrativas aplicáveis pela ainda já atuante Autoridade Nacional de Proteção de Dados Pessoais – ANPD, excepcionalmente entrarão em vigor a partir 1º de agosto de 2021.

O que, em verdade, não traz muito alívio, vez que todos os demais artigos da lei já estão vigentes e passíveis de serem cobrados, inclusive através de tutela jurisdicional.

Por isso é tão urgente conhecer essa legislação e implementar um programa de adequação e manutenção da conformidade com a LGPD.

Diga-se de passagem, não é algo tão simples, tendo em vista que a lei rompe com antigas práticas de tratamento de dados pessoais. A título de exemplo, a LGPD determina que deve haver uma justificativa legal para o uso do dado pessoal e essa justificativa deve se enquadrar dentro do rol de dez bases legais trazidas pela lei.

Ainda, trata-se de uma norma muito principiológica, de modo que não apenas devem ser observadas as justificativas legais para o tratamento, como também esse uso do dado precisa estar em conformidade com os princípios e fundamentos da LGPD.

A norma também traz um empoderamento ao titular dos dados, ao trazer como um de seus fundamentos a autodeterminação informativa, esclarecendo que caberá ao titular do dado pessoal determinar quais dados ele permite que sejam expostos e quais pretende manter de maneira privada.

E nos casos em que há imperiosa necessidade de compartilhamento dos dados, seja por uma obrigação legal ou contratual, a LGPD reforça a necessidade da **transparência** em todo o processo de tratamento dos dados, desde a sua coleta até o seu descarte.

Para que tudo isso também ocorra de forma adequada à lei, será necessário tomar medidas técnicas e administrativas que ofereçam a **segurança** desses dados, a fim de se evitar, por exemplo, vazamento, perda, destruição acidental e até mesmo, inexatidão dos dados.

Então, como se pode observar já na introdução, há um grande caminho a ser percorrido por todas as organizações que tratam dados pessoais, e em especial, aos profissionais da advocacia, pois estes além de precisarem se adequar a legislação, prestarão auxílio aos seus clientes nessa nova jornada proposta pela LGPD.

4
CONCEITOS DA LGPD

A LGPD traz novos termos e conceitos que precisam ser conhecidos. Aqui são apresentados os principais, quais sejam:

1 **Titular de dado pessoal:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

2 **Dado pessoal:** toda informação relacionada a pessoa natural que possa identificá-la ou torná-la identificável;

3 **Dado pessoal sensível:** todo 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;

4 **Banco de dados:** é o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

5 **Tratamento de dados:** 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;

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

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

8 **Os agentes de tratamento:** o controlador e o operador;

9 **Encarregado de Proteção de Dados /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 (ANPD);

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

11 **Relatório de impacto à proteção de dados pessoais- RIPD:** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

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

Esses conceitos são apresentados no **artigo 5º da Lei Geral de Proteção de Dados Pessoais** e precisam ser bem conhecidos para correta interpretação em um projeto de adequação à LGPD. Da mesma maneira é necessário conhecer muito bem os fundamentos da LGPD contidos no artigo segundo da Lei.

5
FUNDAMENTOS DA LGPD

A Lei Geral de Proteção de Dados Pessoais, em seu artigo 2º, trouxe importantes fundamentos para o devido tratamento dos dados, sendo eles:

(i) o respeito à privacidade; (ii) a autodeterminação informativa; (iii) a liberdade de expressão, de informação, de comunicação e de opinião; (iv) a inviolabilidade da intimidade, da honra e da imagem; (v) o desenvolvimento econômico e tecnológico e a inovação; (vi) a livre iniciativa, a livre concorrência e a defesa do consumidor; e (vii) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Estes fundamentos vêm refletidos nos princípios que regem o tratamento de dados pessoais (artigo 6º) e foram inspirados na regulação europeia de direito de proteção de dados.

Para Fábio Konder Comparato, o termo fundamento "*designa o que serve de base ao ser, ao conhecer, ou ao decidir. Fundamento é, pois, a causa ou razão de algo*". Isto é, ao realizar o tratamento de dados, é necessária a observância dos fundamentos supramencionados, servindo estes como sustentação da Lei nº 13.709/18.

Podemos extrair dos referidos fundamentos que esta lei é construída sob a premissa do respeito à privacidade e à liberdade, sendo o titular dos dados soberano sobre suas próprias informações, sejam elas encontradas em formato físico ou digital.

Vale destacar, por fim, que o advento da Lei Geral de Proteção de Dados Pessoais não é um empecilho ao desenvolvimento econômico e tecnológico brasileiro, mas sim visa estabelecer meios para que os cidadãos possam ter seus dados protegidos.

Sem dúvida é um tópico de extrema relevância aos escritórios de advocacia que precisam adequar-se o quanto antes à legislação, e que poderá ainda originar novas oportunidades de atuação aos profissionais do direito, tanto como representantes legais de seus clientes na defesa de seus direitos, como também na prestação de consultoria nos programas de adequação à LGPD, e até mesmo, como encarregado de proteção de dados.

6
PRINCÍPIOS

Os princípios são de suma importância na LGPD, pois devem ser observados em todo o processo de tratamento dos dados pessoais, servindo como norte na aplicação da lei. Em seu art. 6º, a Lei de Proteção de Dados Pessoais trouxe dez princípios, além da boa-fé. São eles:

a) A boa-fé

Um dos mais importantes preceitos a serem observados e orientador dos demais princípios, consiste em um comportamento correto e adequado nas relações com terceiros, observando a coerência, a informação e a cooperação. Flávio Tartuce ainda aponta que ela está relacionada com os deveres anexos ou laterais de conduta, que são, dentre outros: dever de respeito, de lealdade, de probidade e de agir conforme a confiança depositada.

b) Finalidade

Deve ser exposto ao titular o motivo pelo qual serão utilizados os seus dados pessoais, não podendo haver alteração posterior. A observância aos limites legais, se torna imprescindível, bem como a clareza das cláusulas, para que o titular possa decidir de forma consciente se quer ou não compartilhar os seus dados, visando assim mitigar o uso secundário do dado sem sua anuência.

c) Adequação

Os dados pessoais tratados estarão em consonância com a finalidade. Ou seja, a justificativa para o tratamento dos dados deve ter conexão com a informação que se pede.

d) Necessidade

Os dados utilizados devem ser os estritamente necessários para atingir a finalidade.

e) Livre Acesso

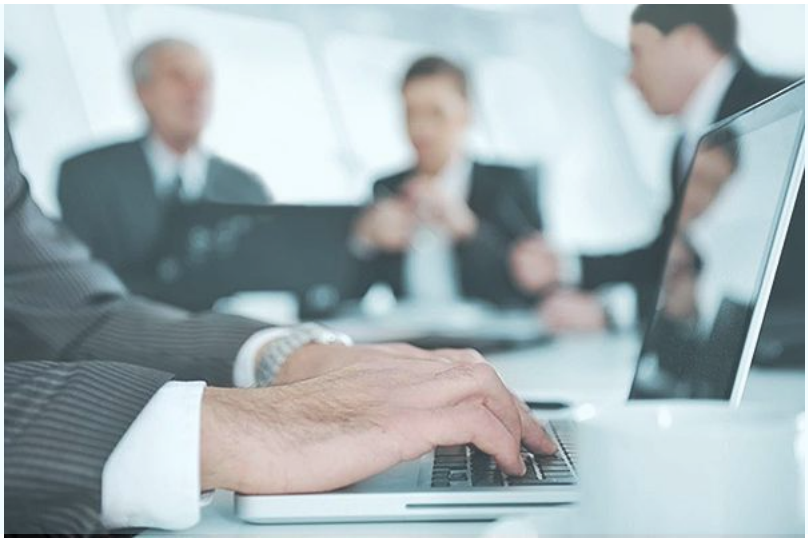
O titular que fornece os dados deve ter acesso a todos eles, de forma simples e gratuita, devendo ser detalhado o que a organização faz com os dados, como o tratamento é realizado e a sua duração.

f) Qualidade dos Dados

Garantia de que as informações coletadas sejam verdadeiras e atuais. Atenção especial à exatidão, clareza e relevância dos dados, compatíveis com a necessidade e a finalidade de seu tratamento.

g) Transparência

É necessário que os titulares de dados tenham amplo e fácil acesso às informações sobre o tratamento de seus dados. Essas informações devem ser claras e precisas a respeito daquilo que será feito com os dados.



h) Segurança

Os dados devem ser protegidos por meio de medidas técnicas e administrativas capazes de evitar incidentes de segurança que levem a violações de dados pessoais acidentais ou ilícitas, tais como acessos não autorizados e situações de destruição, perda, alteração, comunicação ou difusão de dados.

i) Prevenção

O tratamento dos dados deve ser feito de forma a prevenir a ocorrência de incidentes, adotando-se boas práticas de governança e os conceitos de privacidade desde a concepção.

j) Não discriminação

Impossibilidade de tratar dados pessoais que culminem em estigmatização, classificação ou segregação, seja de forma automatizada ou não no tratamento de dados pessoais. Assim, é proibida a utilização de dados sensíveis, tais como etnia, raça, orientação sexual, convicção político-partidária etc., para fins discriminatórios ilícitos ou abusivos, entre outros.

k) Responsabilização e prestação de contas

Os dados devem ser protegidos de forma adequada e, quando solicitado, deve ser demonstrada a efetividade das medidas de proteção utilizadas.

Como se pode observar, os princípios são determinantes para a aderência à LGPD, especialmente considerando que é uma legislação que demanda muitas regulamentações específicas, ainda a serem formuladas, de modo que os princípios é que trarão o direcionamento do programa de adequação.

7
BASES LEGAIS

Segundo a LGPD o tratamento de dados pessoais somente poderá ser realizado nas hipóteses trazidas pelo artigo 7º da lei, as chamadas bases legais, ou seja:

I - mediante o fornecimento de **consentimento** pelo titular;

II - para o **cumprimento de obrigação legal** ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de **políticas públicas** previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de **estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para **a execução de contrato** ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o **exercício regular de direitos em processo judicial, administrativo ou arbitral**, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a **proteção da vida** ou da incolumidade física do titular ou de terceiro;

VIII - para a **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; *(Redação dada pela Lei nº 13.853, de 2019) Vigência*

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

X - para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente.

Além das bases legais previstas no artigo 7º, a LGPD trouxe um rol diferenciado para os casos de dados pessoais sensíveis. Em seu artigo 11 a lei dispõe que o tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal **consentir**, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

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

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

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da *Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;*

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

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

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

Importante destacar que não há qualquer hierarquia entre as bases legais, não sendo o consentimento mais importante que o legítimo interesse, por exemplo. No entanto, a indicação da base legal deve ser a mais adequada para o tratamento do dado.

Ainda, basta a indicação de uma única base legal para conformidade, de modo que, se o tratamento do dado pessoal for necessário para execução do contrato, ou para cumprimento de uma obrigação legal, por exemplo, não se fará necessário coletar o consentimento do titular dos dados.

De toda forma, para indicação da base legal será importante a realização do mapeamento do fluxo dos dados, para tomar conhecimento de sua origem e finalidade, pois trará melhores condições para identificação da adequada base legal.

8

BOAS PRÁTICAS DE GOVERNANÇA EM PRIVACIDADE E PROTEÇÃO DE DADOS

Como já mencionado, a **Lei Geral de Proteção de Dados Pessoais** traz à tona a importância de adoção de boas práticas de governança em privacidade e proteção de dados pessoais.

O **artigo 46** da lei prevê que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas para proteção dos dados pessoais de:

i) acessos não autorizados;

ii) situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Bem como, a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados (**artigo 52**, §1º, VII), em consonância com o disposto no inciso II do § 2º do **art. 48** da Lei.

O parágrafo 2º do **artigo 46** da LGPD afirma que essas medidas deverão ser observadas desde a fase de concepção do produto, ou do serviço, até a sua execução, também chamado de *privacy by design*.

Mas afinal, quais seriam essas boas práticas de governança em privacidade e proteção de dados pessoais?

A LGPD traz um referencial importante, muito embora não apresente um manual exato do que a organização deve fazer para demonstrar que atende aos requisitos da lei.

O **artigo 50** da lei estabelece que os controladores e operadores poderão formular regras de boas práticas e de governança que estabeleçam:

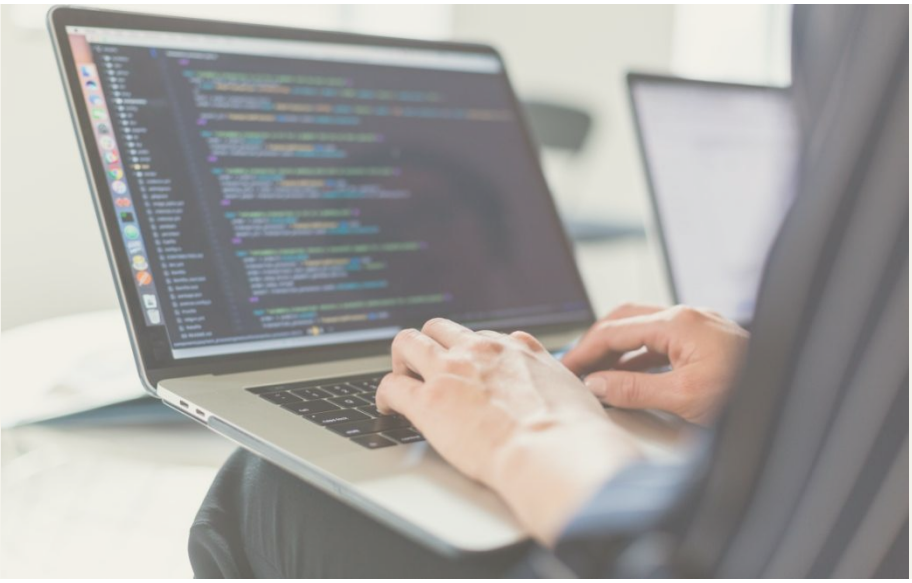
a) as condições de **organização**, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares,

b) as normas de **segurança** e os padrões técnicos,

c) as **obrigações** específicas para os diversos envolvidos no tratamento,

d) as ações **educativas**,

e) os mecanismos internos de supervisão e de **mitigação de riscos** e outros aspectos relacionados ao tratamento de dados pessoais.



Também se extrai da lei que ao se estabelecer regras de boas práticas, o controlador e o operador devem levar em consideração, em relação ao tratamento dos dados: a natureza, o escopo e a finalidade, além dos riscos e benefícios decorrentes do tratamento dos dados.

E ainda, o controlador precisará implementar um **programa de governança em privacidade** que, no mínimo:

a) demonstre o **comprometimento do controlador** em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja **aplicável a todo o conjunto de dados pessoais** que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à **sensibilidade dos dados tratados**;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática **de impactos e riscos à privacidade**;

e) tenha o objetivo de estabelecer **relação de confiança com o titular**, por meio de atuação transparente e que assegure mecanismos para sua participação;

f) esteja integrado a sua estrutura geral de governança, estabeleça e aplique **mecanismos de supervisão internos e externos**;

g) conte com **planos de resposta a incidentes** e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir do **monitoramento contínuo** e avaliações periódicas;

Assim como num programa de compliance, a implementação de políticas e controles auxiliam na implementação e manutenção da adequação à LGPD.

Para complementar, segundo Tarcísio Teixeira:

> *Como exemplo de boas práticas os agentes poderão adotar política de privacidade interna, instituir canais de denúncia para a proteção de dados, promover ações educativas e treinamentos, criar manuais para rotina de vazamento de dados, planos de vazamento de dados, de forma a engajar todos os setores de uma empresa para a política de proteção de dados pessoais.*

Também esclarece a Dra. Patrícia Peck que:

> *A instituição de medidas e regras de boas práticas e de governança é essencial para que todos os requisitos necessários à proteção de dados pessoais sejam efetivados.*
> *Conforme os artigos 40,41,42 e 43, as medidas de boas práticas envolvem um sistema amplo e complexo de relações e previsões como instituição de mecanismo de educação e prevenção em face da segurança da informação, atuação de organismo de certificação e treinamento de equipes junto à atuação das autoridades supervisoras.*

Como se pode extrair será imprescindível a adoção de **boas práticas de governança em privacidade e proteção de dados** para implementação e manutenção de um programa de adequação à Lei Geral de Proteção de Dados Pessoais.

9
MEDIDAS PARA ESTAR EM COMPLIANCE COM A LGPD

As empresas e entidades que se comprometerem a implementar um programa de compliance em privacidade de proteção de dados pessoais, além de evitar as árduas penalidades que podem ser impostas pela Autoridade Nacional de Proteção de Dados (ANPD), também irão adquirir uma camada de proteção reputacional, assim como uma grande vantagem competitiva ao adotarem medidas corporativas de integridade e segurança dos dados pessoais.

Assim como pilares de um **programa de compliance**, apresenta-se abaixo 10 medidas que auxiliarão as organizações e os escritórios de advocacia na implementação de um programa de adequação, quais sejam:

Suporte da alta cúpula: engajamento dos profissionais em posição de direção e gerência da organização, para que todas as medidas em favor da privacidade de dados pessoais possuam apoio dos responsáveis pelas decisões organizacionais e pela definição do orçamento.

Avaliação de riscos: análise minuciosa dos processos internos, em conjunto com outros departamentos, que impliquem na coleta e uso de dados pessoais de funcionários, clientes e terceiros a fim de entender o ciclo de vida da informação pessoal e possíveis riscos de incidentes de privacidade.

Políticas corporativas: elaboração de códigos internos como políticas de privacidade, plano de ação e resposta em caso de incidentes com dados pessoais, políticas internas sobre privacidade e proteção de dados para orientar os colaboradores, bem como políticas externas para demonstrar aos clientes, parceiros e terceiros o comprometimento da empresa quanto ao tema.

Controles internos: criação de mecanismos de tecnologia e segurança da informação para garantir que as políticas corporativas de privacidade sejam aplicadas e que os processos da empresa estejam em conformidade com a lei, como, por exemplo, utilização de criptografia, senhas, tokens, controles de acesso e adaptação das estruturas físicas do ambiente de trabalho.

Cultura e Treinamento: instruir e treinar periodicamente os colaboradores sobre as normas internas de proteção de dados pessoais, nos termos da política de privacidade e conscientizá-los quanto à importância do cumprimento da LGPD.

Canais de denúncia: criação de um canal de comunicação sigiloso para que os colaboradores e terceiros possam delatar eventuais violações aos direitos de privacidade ao departamento responsável pela proteção de dados.

Encarregado: nomeação de um profissional que atuará como o gestor do programa a fim de garantir o sucesso das medidas de proteção, e como canal de comunicação entre a empresa, os colaboradores, os titulares dos dados pessoais e a ANPD.

Investigações internas: criação de procedimentos de apuração de eventuais violações à LGPD e determinação das respectivas sanções aos responsáveis pelo dano.

Due Dilligence: checagem prévia do nível de conformidade em normas de privacidade e proteção de dados, pesquisando informações sobre terceiros e parceiros de negócios, avaliando seus antecedentes, em especial, com relação a incidentes de segurança e vazamento de dados pessoais.

Monitoramento: avaliar periodicamente se as medidas adotadas são efetivas para assegurar a proteção de dados pessoais, e ajustá-las conforme a necessidade e as inovações nas regulamentações de proteção de dados pessoais.

10
PENALIDADES

A LGPD prevê penalidades administrativas a serem aplicadas pela ANPD (Autoridade Nacional de Proteção de Dados) no seu art. 52, quais sejam:

Penalidades pecuniárias (art. 52, incisos II e III, LGPD):

multa simples ou diária no valor de até 2% do faturamento da empresa, limitada ao teto de 50 milhões de reais;
O valor fixado deve observar a gravidade da infração e a extensão do dano ou prejuízo causado.

Penalidades administrativas (art. 52, incisos I, IV, V, VI, X, XI e XII, LGPD):

- **Advertência** e prazo para adoção de medidas corretivas;
- **Publicização**: após confirmada a infração em procedimento administrativo;
- **Bloqueio dos dados pessoais** a que se refere a infração até a regularização destes;
- **Eliminação** dos dados pessoais a que se refere a infração;
- **Suspensão parcial do funcionamento do banco de dados,** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- **suspensão do exercício da atividade de tratamento dos dados pessoais** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- **Proibição total ou parcial** do exercício de atividades relacionadas a tratamentos de dados.

As penalidades serão aplicadas mediante procedimento administrativo regular e deverão ser observados os princípios do contraditório e ampla defesa, garantidos constitucionalmente. Para a **aplicação das penalidades**, a ANPD considerará os seguintes **parâmetros e critérios:** (art. 52, §1°, incisos I ao XI, LGPD)

- A proporcionalidade entre a gravidade da falta e a intensidade da sanção;
- A gravidade e a natureza das infrações e dos direitos pessoais afetados;
- A reincidência e o grau do dano;
- A vantagem auferida ou pretendida pelo infrator e sua condição econômica;
- A boa-fé, cooperação e pronta adoção das medidas corretivas pelo infrator;
- Adoção de adoção de política de boas práticas e governança;
- A adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados;

Penalidades Administrativas: em que pese a LGPD prever a aplicação das penalidades administrativas pela ANPD somente a partir de 01 de agosto de 2021, outras medidas podem ser acionadas para o cumprimento da lei (art. 52, §2°, LGPD), visto que as penalidades aplicadas pela ANPD não impedem consequências civis, penais, ou mesmo as administrativas por outros órgãos, como por exemplo, as sanções impostas pelo Procon com fundamento no Código de Defesa do Consumidor.

Assim, há de se ressaltar as **medidas judiciais**, tanto por iniciativa do Ministério Público (Ação Civil Pública), quanto diretamente por aqueles que tenham seus dados pessoais violados (Ações Indenizatórias). Portanto, todos que exercem a atividade de tratamento de dados devem estar em conformidade com a LGPD de imediato.

Prejuízos aos negócios: ressalte-se que as penalidades podem ir muito além das que estão já previstas em lei, tendo em vista que uma quebra de sigilo de dados pessoais pode culminar em execução de **multas contratuais, perdas de contratos**, além de prejudicar a **reputação** da organização, afetando em especial a **confiança** do cliente.

Abalos a **credibilidade** podem afastar não só consumidores, como também fornecedores, investidores, empregados e parceiros comerciais, o que causaria sem sombra de dúvida prejuízos inestimáveis à **imagem** da organização e, consequentemente, prejuízos financeiros.

Especialmente considerando a relação entre cliente e advogado, é certo que fatores como reputação, confiança, imagem e credibilidade são fundamentais para o sucesso de um escritório de advocacia.

11 CONCLUSÃO

Diversas outras frentes e comissões das seções e subseções da **Ordem dos Advogados do Brasil** tratam e estudam este tema tão relevante e suas implicações até com maior profundidade.

No entanto, a **Comissão de Estudos em Compliance da OAB Subseção Campinas**, dentre outras iniciativas de prestar sua contribuição para temas relevantes em Compliance, pretendeu trazer as primeiras impressões, e quiçá questionamentos sobre esta tão impactante Lei, em especial para que os advogados e escritórios de advocacia possam dar seus primeiros passos para a adequação e compliance à lei.

Muito está por vir em relação a resoluções e normativas da Autoridade Nacional de Proteção de Dados, pela jurisprudência dos mais diversos tribunais e pela repercussão da própria sociedade. Este é somente o começo de uma nova era.

CÔRREA, Adriana Espíndola. Lei de Proteção de dados e a identificação nacional: há antinomias? Disponível em: <https://www.conjur.com.br/2019-fev-18/direito-civil-atual-lei-protecao-dados-identificacao-nacional-antinomias.> Acesso em: 17/09/2020.

COMPARATO, Fábio Konder. Rumo à Justiça. Pág. 43. 2013. Editora Saraiva: São Paulo. 2. ed.

Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. Brasília, DF, 14 ago. 2018.
Disponível em:
<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

PECK, Patricia P. - Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação.2018 PESTANA, Marcio. Conjur, 2020. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). Disponível em: https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf,

TEIXEIRA, Tarcisio; ARMELIN, Ruth M.G.F. Lei Geral de Proteção de Dados Pessoais: Comentada artigo por artigo – Salvador: Editora JusPodium, 2019.

TOMASEVICIUS, Eduardo. CONJUR, 2019. O princípio da boa-fé na Lei Geral de Proteção de Dados –publicado em: 9/03/2020.
Disponível em:
<https://www.conjur.com.br/2020-mar-09/direito-civil-atual-principio-boa-fe-lgpd#:~:text=Conforme%20disposto%20nos%20arts.,tenham%20acesso%20a%20essas%20informa%C3%A7%C3%B5es>,

EQUIPE DE ELABORAÇÃO DA CARTILHA

Esta Cartilha foi elaborada e produzida por integrantes da **Comissão de Estudos em Compliance:**

Camila de Proença Negretti

Carolina Elias da Silva

Daniela Reni Dorian Martinez - *Coordenadora*

Diana Cristina Rosa Santana - *Coordenadora*

Isabela Guarino Tancredo

Jacinta Dias Barros

Thiago Henrique Bueno Vaz

Vanessa Juliana Domingues Scaquetti

Comissão de Estudos em Compliance - Composição

Presidente
Daniela Reni Dorian Martinez

Secretária
Ana Teresa Carvalho do Castro Mesquita

Membros Efetivos
Alex Bonini
André Pagliaro Rossi
Aline da Silva Teles
Bruna Alves Galante Longhi
Camila de Proença Negretti
Carolina Elias da Silva
Cristiane Silvestrini
Cristiane Vergani
Daniel Ceccon Guimarães
Diana Cristina Rosa Santana
Elen Moretti
Gabriela Marangoni
Gabriella Assis E. de Lima Oliveira
Geise Tamires Fogo
Gustavo Costa Biagioli
Henrique Aparecido Casarotto
Isabela Guarino Tancredo
Jéssica Yumi da Silva Sato
Júlia Dutra Silva Magalhães
Letícia Martins Socio Ferreira
Lucas Rosa da Cunha
Lydiane Berrnava Alves
Marcelo Ribeiro
Matias Dallacqua Illg
Patricia de Oliveira Borges
Rafael Priviero D'Abruzzo
Sarah Regina de Oliveira Campos
Silmara Bernava Alves Moreira
Thiago Henrique Bueno Vaz
Vanessa J. Domingues Scaquetti

Membros Efetivos Regionais
Janetcler Florencio Lopes
Rayane Nunes Santos

Membros Colaboradores
Diego Luiz Silva Joaquim
Karina Bonetti Badawi
Letícia Raquel Gatto
Marcelo Pereira Fujita
Marjorie M. Franco de Medeiros
Talita Andreotti Costola

3ª SUBSEÇÃO DA ORDEM DOS ADVOGADOS DO BRASIL

GESTÃO 2019/2021

Diretoria

Daniel Blikstein
Presidente

Luciana Freitas
Vice-Presidente

Paulo Braga
Secretário Geral

Cláudio Vieira
Secretário Geral-Adjunto

Ivan Castrese
Diretor Tesoureiro

Campinas
3ª SUBSEÇÃO

www.oabcampinas.org.br

@oabcampinas
@oabspcampinas

@oabcampinas

https://www.youtube.com/c/OABCampinasSubseção