OABRJ LEOPOLDINA

A LEI GERAL DE PROTEÇÃO DE DADOS

NOS ESCRITÓRIOS DE ADVOCACIA

FERNANDA SANAN (ORG.) | ISABELLA CARDOSO | JULIANE NAEGELE | LARISSA CARNEIRO

GUIA ORIENTATIVO

A LEI GERAL DE PROTEÇÃO DE DADOS

NOS ESCRITÓRIOS DE ADVOCACIA

A Lei Geral de Proteção de Dados nos escritórios de Advocacia

Coordenadora
Fernanda Aparecida Pina Sanan

Revisão Textual
Autoras

Diagramação
Giceli Valadares da Silva

Capa
Giceli Valadares da Silva

1ª Edição: Novembro de 2023

Dados Internacionais de Catalogação na Publicação (CIP-Brasil)

G633s

Sanan, Fernanda Aparecida Pina (Org.).

A Lei Geral de Proteção de Dados nos escritórios de Advocacia / Fernanda Aparecida Pina Sanan; – Cacoal: Priint Impressões Inteligentes, 2023.

ISBN: 978-85-5963-168-5

1. Proteção de Dados 2. Escritório de Advocacia 3. Lei Geral I. Título.

CDU 658

Impresso no Brasil por:

priint impressõesinteligentes

(69) 9.9251.0505 (WhatsApp)
priintcacoal@gmail.com • @priinteditora
www.fb.com/PriintEditora • www.priint.com.br

COORDENADORA

Fernanda Aparecida Pina Sanan
Presidente da Comissão de Proteção de Dados e Privacidade da 58ª subseção – OAB/RJ – Leopoldina

A LEI GERAL DE PROTEÇÃO DE DADOS

NOS ESCRITÓRIOS DE ADVOCACIA

- **Fernanda Aparecida Pina Sanan** – Presidente da Comissão de Proteção de Dados e Privacidade da 58ª subseção – OAB/RJ – Leopoldina
- **Isabella Coelho da Mata Cardoso –** Membro da Comissão de Proteção de Dados e Privacidade da 58ª subseção – OAB/RJ – Leopoldina
- **Juliane Rocha Naegele –** Membro da Comissão de Proteção de Dados e Privacidade da 58ª subseção – OAB/RJ – Leopoldina
- **Larissa Alves Carneiro –** Vice-presidente da Comissão de Proteção de Dados e Privacidade da 58ª subseção – OAB/RJ – Leopoldina

Apresentação da Obra

Dr. Walter Aranha Capanema

Com imenso orgulho, apresento a obra intitulada "A Lei Geral de Proteção de Dados nos Escritórios de Advocacia". Esta notável criação é coordenada pela ilustre Dra. Fernanda Aparecida Pina Sanan e enriquecida com as valiosas contribuições das Dras. Isabella Coelho da Mata Cardoso, Juliane Rocha Naegele e Larissa Alves Carneiro.

A Lei 13.709/2018, reconhecida como "Lei Geral de Proteção de Dados" (LGPD), reformulou as relações jurídicas em todas as esferas, afetando tanto entidades estatais quanto privadas, destacando a necessidade de se preservar e respeitar os dados pessoais.

Nas páginas deste livro, distribuídas ao longo de 15 tópicos meticulosamente elaborados, apresenta-se uma visão ampla da LGPD. A obra fornece informações de inestimável valor à comunidade jurídica, desvendando, de maneira didática, os intrincados conceitos legais, além de abordar os direitos dos titulares de dados pessoais e outras iniciativas de relevância inquestionável.

Um enfoque especial é conferido à adaptação dos escritórios de advocacia à LGPD, com orientações preciosas sobre a digitalização e o armazenamento seguro de documentos, a segurança de dados e a inclusão de cláusulas de proteção de dados em contratos, entre outros aspectos cruciais.

É uma verdadeira inspiração saber que, em um mundo repleto de desafios, quatro profissionais notáveis uniram seus conhecimentos para orientar e criar uma obra de utilidade inestimável para a comunidade jurídica.

Sobre a 58ª Subseção da OAB/RJ – Leopoldina

Presidente – Dr. Alexandre Aguilar

Com imenso prazer, na qualidade de Presidente da 58ª Subseção da Leopoldina-RJ, e com grande entusiasmo que apresento o "Guia Orientativo para Adequação à LGPD em Escritórios de Advocacia". Essa iniciativa pioneira e inovadora é resultado do incansável trabalho da Comissão de Proteção de Dados desta instituição, ressaltando o papel crucial da comissão não apenas para a nossa subseção, mas também para toda a advocacia.

A proteção de dados emergiu como um tema de extrema importância em um mundo cada vez mais digitalizado. Torna-se imperativo que os advogados estejam devidamente preparados para enfrentar as complexidades da LGPD. Nossa comissão, formada por especialistas dedicados, desempenha um papel essencial na capacitação de nossos colegas nessa área crítica.

Este guia representa uma valiosa ferramenta destinada para auxiliar nossos advogados na compreensão e na implementação das práticas de conformidade com a LGPD em seus escritórios. Ele oferece orientações práticas e dicas essenciais, garantindo que nossa classe esteja plenamente alinhada com os requisitos da legislação de proteção de dados. Em meio ao cenário jurídico em constante evolução, a Comissão de Proteção de Dados continua a ser um farol de conhecimento e apoio para nossa subseção. Estamos confiantes de que este guia se tornará uma ferramenta inestimável para fortalecer nossos escritórios de advocacia, preservar a confiança de nossos clientes e assegurar a proteção dos dados confiados a nós.

Juntos, avançamos na jornada da conformidade com a LGPD, e este guia é um passo significativo para garantir que nossos advogados estejam na vanguarda da proteção de dados. Agradecemos o comprometimento de nossa comissão e convidamos os advogados e advogadas a aproveitarem ao máximo este recurso valioso.

Sobre as Autoras

FERNANDA APARECIDA PINA SANAN – Presidente da Comissão de Proteção de Dados e Privacidade da 58ª subseção – OAB/RJ – Leopoldina. Advogada e consultora em Lei Geral de Proteção de Dados Pessoais. Especialista em Direito do Trabalho, Compliance e LGPD pela Universidade de Coimbra – Portugal. Especialização em Lei Geral de Proteção de Dados pela PUC/RS. Especialização em Lei Geral de Proteção de Dados pela *Nextlaw Academy* – Fundamentals e Trilha LGPD. Advogada e sócia no escritório Sanan Advogados, atuando em complexas questões do mundo digital, principalmente em projetos de adequação à LGPD, como consultora e DPO – *Data Protection Officer*. Diretora Jurídica na Empresa Doctor Privacy. *E-mail*: sananfernanda@gmail.com

JULIANE NAEGELE – Membro da Comissão de Proteção de Dados e Privacidade da 58ª subseção – OAB/RJ – Leopoldina. Advogada e consultora em Lei Geral de Proteção de Dados Pessoais. Pós Graduada em Direito Empresarial pela PUC/RJ. Especialização em Lei Geral de Proteção de Dados pela *Nextlaw Academy* – Fundamentals e Trilha LGPD. MBA Business and Law pela FGV/RJ. Pós Graduanda em Direito Digital, Compliance Trabalhista e Proteção de Dados pela Escola Mineira de Direito. *E-mail*: junaegele@yahoo.com.br

ISABELA CARDOSO – Membro da Comissão de Proteção de Dados e Privacidade da 58ª subseção – OAB/RJ – Leopoldina. Advogada, Consultora em Lei Geral de Proteção de Dados Pessoais, Mentora e Professora em Cursos *online* referente a proteção de dados. Especialização em LGPD – Legale Educacional – Pós Graduanda em Direito Digital, Compliance Trabalhista e Proteção de Dados pela Escola Mineira de Direito. Especialização em Lei Geral de Proteção de Dados pela *Nextlaw Academy* – Fundamentals e Trilha LGPD. Advogada no escritório Isabela C M Cardoso Sociedade Individual de Advocacia, atuando no direito Digital, Imobiliário e Condominial, principalmente em projetos de adequação à LGPD, como consultora e DPO – *Data Protection Officer*. Diretora Jurídica na Empresa CondoPrivacy. *E-mail*: isabelacardosoadv@gmail.com

LARISSA CARNEIRO – Vice-presidente da Comissão de Proteção de Dados e Privacidade da 58ª subseção – OAB/RJ – Leopoldina. Advogada e socióloga. Mestre em Ciências Sociais pela UERJ, pós-graduada em Direito Público e Privado pela EMERJ, pós-graduada em Direito do Trabalho e Previdenciário pela UCAM e pós-graduada em Direito Digital pela Faculdade Ésper. Secretária-Adjunta da ABA Estadual RJ, Vice-presidente da Comissão de Direito Digital da ABA-RJ, Vice-presidente da Comissão de Proteção de Dados da OAB Leopoldina e Coordenadora do Caarj 4.0 Digital. *E-mail*: carneirolarissa.adv@gmail.com

Introdução

LGPD na Advocacia – protegendo dados, garantindo direitos

Bem-vindo ao Guia Orientativo da LGPD para Advocacia, idealizado pela 1ª Comissão de Proteção de Dados e Privacidade da 58ª OAB – Leopoldina. A obra é o resultado de muito estudo, dedicação, vivência teórica e prática de profissionais que atuam com Proteção de Dados nos mais distintos segmentos.

Em um mundo cada vez mais digitalizado, a proteção dos dados pessoais tornou-se uma prioridade global. No Brasil, a Lei Geral de Proteção de Dados (LGPD), em vigor desde setembro de 2020, trouxe mudanças significativas na forma como as organizações lidam com informações pessoais.

Para profissionais da advocacia, a LGPD é uma realidade que não pode ser ignorada. Ela não apenas define obrigações legais claras relacionadas à coleta, armazenamento e uso de dados pessoais, mas também representa uma oportunidade de fortalecer a confiança e a transparência nas relações com clientes e colaboradores.

O Guia Orientativo foi elaborado com o objetivo de auxiliar advogados, escritórios de advocacia e profissionais do setor jurídico a compreenderem e cumprirem as disposições da LGPD de forma eficaz. Abordaremos os princípios fundamentais da LGPD, as implicações para a advocacia, as melhores práticas para a coleta e tratamento de dados pessoais, e como implementar medidas de segurança robustas.

Entendemos que os requisitos normativos e de segurança da informação da LGPD podem parecer complexos, mas estamos aqui para descomplicá-la. O Guia oferece insights valiosos, exemplos reais e dicas acionáveis para garantir que a sua prática jurídica esteja em conformidade com a lei.

Lembramos que a LGPD não é apenas sobre cumprir obrigações legais, mas também sobre proteger os direitos individuais e a privacidade das pessoas. Acreditamos que, com o conhecimento e as ferramentas certas, ela pode ser uma aliada na construção de relações de confiança e no fortalecimento da sua atuação na advocacia.

Nossa gratidão aos que nos ajudaram a concretizar esta obra. Ao Presidente da 58ª Subseção da OAB/RJ, Dr. Alexandre Aguilar, nossa admiração e respeito, conte com nossos esforços no caminho da conformidade. Ao ilustre Dr. Walter Aranha Capanema, nosso agradecimento e admiração, obrigada por nos brindar com suas generosas palavras.

Aos caros colegas de profissão, aproveitem o Guia Orientativo como uma ferramenta educacional e prática para navegar pelo universo da LGPD na advocacia. Esperamos que ela seja um recurso valioso e esclarecedor para o seu trabalho diário.

Sumário

Lei Geral de Proteção de Dados Pessoais

Muito tem se falado sobre a Lei Geral de Proteção de Dados, mas você sabe o que significa? Sabe o que ela visa proteger?

A Lei foi internalizada no nosso ordenamento sob o nº 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD), é um importante marco legal para a proteção de dados no Brasil. Ela é resultado de um movimento espontâneo da sociedade e de autoridades brasileiras, na tentativa de unificar toda abordagem sobre dados pessoais, online e offline, substituindo certas regulações e suplementando outras.

Empresas e usuários vêm buscando respostas para as questões de segurança virtual, que ganham relevância em função da escalada do cibercrime. Assim, a LGPD surge do esforço conjunto de diversas instâncias no sentido de combater fraudes e crimes virtuais que, com o tempo, cresceram no Brasil.

É a primeira legislação do Brasil que trata especificamente do uso de dados pessoais. Nossa Lei tem uma grande influência da legislação Europeia, a *General Data Protection Regulation* (GDPR), que é considerada uma das maiores referências no mundo.

O GDPR tem eficácia no território da União Europeia, mas seu amadurecimento legislativo, principalmente nas questões de proteção de dados e inteligência artificial – IA – impacta e influencia muitos países, como o Brasil. Diante desse cenário, outros países sentiram a necessidade de ter uma lei semelhante para manter os direitos dos seus dados exportados, e foi exatamente daí que surgiu a demanda de uma versão brasileira.

Não há dúvidas de que a Lei Geral de Proteção de Dados é um marco na história do Brasil. Diferente do que alguns enxergam, a diretriz não vem simplesmente para punir vazamentos de informações (que, inevitavelmente, podem ocorrer com qualquer empresa), mas sim para promover, a nível federal, uma conscientização mais apurada, em respeito ao direito fundamental à privacidade, que já era previsto na Constituição de 1988 e que se consolidou com a EC 115/22, acrescentando ao artigo 5º da Constituição Federal, o inciso LXXIX, assegurando o direito à proteção dos dados pessoais.

Na elaboração do Guia Orientativo, objetivamos apresentar a lei e sua aplicação na prestação dos serviços advocatícios como auxílio aos operadores de direito na implementação das diretrizes legais em seus escritórios em obediência aos preceitos legais e respeito às informações que clientes/titulares de dados fornecem para efetivação de seus direitos nos âmbitos consultivo, administrativo e judicial.

1. ALCANCE DA LEI

A Lei Geral de Proteção de Dados no Brasil foi sancionada com o objetivo de garantir a soberania de dados ao seu titular e regular as atividades de tratamento e coleta de dados, bem como criar a estrutura de fiscalização e responsabilidade da cadeia produtiva em torno do tema.

1.1. A quem se aplica a LGPD?

A Lei Geral de Proteção de Dados se destina a toda pessoa física ou jurídica, de direito público ou privado que manipula dados pessoais da pessoa natural, seja em meio físico ou digital, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade.

1.2. Aplicação territorial.

Iremos aplicar a LGPD a qualquer operação de tratamento realizada por pessoa física ou pessoa jurídica, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- a operação de tratamento seja realizada no território nacional;
- a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços a indivíduos localizados no território nacional;
- os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

1.3. Exceções de aplicação da lei.

De acordo com o art. 4º, a lei não se aplica para os fins:

I	realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II	realizado para fins exclusivamente: **a)** jornalístico e artísticos; ou **b)** acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
III	realizado para fins exclusivos de: **a)** segurança pública; **b)** defesa nacional; **c)** segurança do Estado; ou **d)** atividades de investigação e repressão de infrações penais; ou
IV	provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

2. ENTENDENDO OS CONCEITOS DA LEI

2.1. O que são dados pessoais?

É toda informação que pode identificar ou tornar identificável uma pessoa natural, tais como: nome, CPF, RG, dados de navegação, número de telefone, número de IP e etc.

Você já deve ter ouvido falar que os dados são o novo petróleo, e é isso mesmo, pois muitas empresas tinham a prática de compartilhar de forma irregular o seu banco de dados, monetizando informações dos titulares de dados.

Com a promulgação da LGPD essa prática é expressamente proibida, o que dá maior segurança aos titulares dos dados.

2.2. O que são dados pessoais sensíveis?

Dado pessoal sensível é dado 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.

Os dados pessoais sensíveis estão sujeitos a regras mais rigorosas ante a possibilidade de serem utilizados para fins discriminatórios.

Quando nos referimos a dados pessoais de crianças, adolescentes e idosos, devemos ter uma proteção mais rigorosa, portanto, é imprescindível obter o consentimento inequívoco de um dos pais ou responsáveis e se ater a solicitar apenas o conteúdo estritamente necessário para a atividade econômica ou governamental em questão.

A Lei Geral de Proteção de Dados em seu artigo 11, dispõe hipóteses em que os dados sensíveis podem ser tratados com ou sem consentimento. Em regra, para que haja o tratamento de dados sensíveis, é necessário o consentimento livre, inequívoco e informado do titular ou responsável legal.

Já as hipóteses que excepcionam a exigência do consentimento ocorrem quando for indispensável em situações ligadas: a uma obrigação legal; a políticas públicas; a estudos via órgão de pesquisa; a um direito, em contrato ou processo; à preservação da vida e da integridade física de uma pessoa; à tutela de procedimentos feitos por profissionais das áreas da saúde ou sanitária; à prevenção de fraudes contra o titular.

2.3. O que são dados anonimizados?

Dado anonimizado é dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Na verdade, tem atecnia falar em dado pessoal "anonimizado" pois se ele é anônimo ele deixou de tornar identificado ou identificável a pessoa natural, mas a Lei assim o conceituou.

2.4. O que são dados pseudonimizados?

Dado pessoal que, por meio de tratamento, perde a possibilidade de ser associado direta ou indiretamente a um indivíduo, a menos que o controlador use uma informação adicional que era mantida separadamente em ambiente seguro. Exemplo: dados criptografados.

2.5. O que é banco de dados?

Banco de dados é um conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Temos que desmistificar que ao guardar aquela velha agenda não se trata de banco de dados. Não é necessário você contratar suporte na nuvem para que seja considerado banco de dados.

Em nosso dia a dia cada vez mais virtual, é muito normal termos pen drives e HD externos com todas as nossas iniciais, documentos de cliente, fotografias, e com isso criando o nosso banco de dados.

2.6. Titular de dados

O titular dos dados pessoais é VOCÊ, isso mesmo, você que está lendo essa cartilha. É a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. É o indivíduo que informa seus dados pessoais a uma **organização/pessoa natural**, a fim de fazer parte da base de dados desta.

Não é raro irmos ao mercado, farmácia e pedirem o nosso CPF, e muitas vezes somos coagidos a fornecer nossos dados, pois se não fornecermos podemos perder o desconto daquele estabelecimento. O que devemos questionar é se a empresa está solicitando para meros dados estatísticos ou para desvirtuar da sua atividade fim.

A LGPD possui um capítulo que trata exclusivamente dos direitos do titular e cabe à empresa/ pessoa respeitar essas exigências. Ou seja, se isso não for atendido, podem ocorrer sanções por parte da ANPD, bem como propositura de ações cíveis pelo titular de dados, em caso de descumprimento dos direitos.

São direitos dos titulares de dados:

- ✓ confirmação da existência de tratamento;
- ✓ acesso aos dados;
- ✓ correção de dados incompletos, inexatos ou desatualizados;
- ✓ anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- ✓ portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

- ✓ eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
- ✓ informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- ✓ informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e
- ✓ revogação do consentimento.

2.7. Controlador

É o responsável pelos processos de controle de coleta, tratamento e compartilhamento de dados pessoais que estão sob sua custódia. Na LGPD, ele é descrito como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Ou seja, é o profissional ou empresa que coordena como os dados pessoais serão coletados e tratados. Ele é o dono das regras do jogo, desta forma, tem poder de decisão sobre como os dados serão tratados.

O controlador, seja pessoa física ou jurídica, exerce um papel de grande responsabilidade. O controlador precisa criar processos que estejam de acordo com as bases legais da norma e compete a ele criar o Relatório de Impacto à Proteção de Dados Pessoais, que pode ser solicitado pela ANPD a qualquer momento. Cabe ao controlador explicar, através das políticas de privacidade, por que cada informação será coletada e para que ela será utilizada, bem como os direitos do cidadão como "dono" daquele ativo.

2.8. Operador

É o profissional da organização que realiza o tratamento de dados pessoais em nome do controlador. Na LGPD, ele é descrito como "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador". Ou seja, o operador é diretamente subordinado ao controlador e deve garantir que o processamento de informações esteja de acordo com as regras definidas por ele.

Embora responda às regras do controlador, o operador também pode responder solidariamente a eventuais incidentes de segurança que coloquem em risco a privacidade do titular, especialmente se o incidente foi causado pelo descumprimento das instruções do controlador.

2.9. Encarregado de dados ou DPO (*data protection officer*)

O Encarregado de Proteção de Dados é a 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). Esse profissional é um especialista em proteção de dados e monitora empresas para garantir que elas estejam de acordo com as regras e boas práticas do setor.

A lei não exige formação específica para ser DPO, mas apesar da formação não ser obrigatória, o ideal é que esse profissional tenha habilidades técnicas para o tratamento de dados e conhecimentos jurídicos.

São atividades do DPO previstas na legislação:

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

II receber comunicações da autoridade nacional e adotar providências;

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

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

2.10. Autoridade Nacional de Proteção de Dados (ANPD)

A ANPD é uma autarquia de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública, com autonomia técnico-decisória, com patrimônio próprio, responsável pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil. A ela cabe estabelecer normas e diretrizes para a sua implementação, buscando zelar pela garantia do direito de todos os brasileiros terem seus dados pessoais devidamente protegidos, bem como aplicar sanções quando houver violação desses direitos.

Nesse âmbito de atuação, destacam-se as seguintes as funções:

- ✓ elaborar as diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- ✓ promover a disseminação de conhecimentos sobre as normas e as políticas públicas relacionadas à proteção de dados pessoais e às medidas de segurança;
- ✓ promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
- ✓ estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais;
- ✓ fiscalizar e aplicar sanções em caso de tratamento de dados realizados em descumprimento à legislação.

2.11. Mapeamento de dados

O mapeamento de dados pessoais consiste na identificação e categorização de todos os dados pessoais dentro da empresa, é a análise do caminho que o dado pessoal percorre desde o momento em que é coletado pela empresa/pessoa até o seu descarte.

É quase como um raio X de tudo que envolve os dados coletados. Somente assim a empresa consegue ter um conhecimento completo da sua situação atual e, também, o nível de maturidade no que se refere à proteção de dados.

Não é um trabalho fácil de fazer, pois, em sua grande maioria estes dados se encontram de maneira 'confusa', já que estão em vários departamentos: comercial, marketing, recursos humanos e financeiro, entre outros. É um trabalho minucioso e que requer muita atenção, pois através da análise do mapeamento será possível aplicar a minimização dos dados, objetivando mapear os dados estritamente necessários à finalidade pretendida.

O mapeamento de dados deve ser elaborado em conjunto pelos múltiplos setores da empresa com auxílio técnico e jurídico para análises das possíveis vulnerabilidades encontradas.

2.12. Compartilhamento de dados

O compartilhamento de dados pode ser entendido como as situações em que os dados pessoais são **comunicados, difundidos, transferidos internacionalmente ou interconectados**.

Também entra nessa lista o tratamento compartilhado de bancos de dados pessoais feito por órgãos e entidades públicas que

estejam cumprindo competências legais, ou entre órgãos públicos e entidades privadas. Nesses casos, todas as partes envolvidas devem possuir autorizações específicas para executar uma ou mais modalidades de tratamento.

Entretanto, esse consentimento pode ser dispensado se houver uma base legal que o regulamente.

O compartilhamento de dados pode ocorrer em diferentes situações e modelos de negócio, em um simples processamento da folha de pagamento ou na cobrança de um devedor. Em alguns casos esse uso compartilhado é previsto e amparado pela LGPD. Já em outros, pode ser considerado crime contra a integridade dos indivíduos.

As empresas devem, portanto, reconhecer em quais situações podem fazê-lo e como se ajustar para não cometer erros.

2.13. Transferência internacional de dados

É a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro. Porém, a transferência descrita na lei não pode ser realizada de forma indiscriminada. Pelo contrário, o controlador deve utilizar algum dos mecanismos previstos na LGPD que autorizam que seja realizada a transferência dos dados pessoais a outro país.

A LGPD deixa clara a obrigatoriedade de observância dos mecanismos elencados no seu artigo 33, ao prever expressamente que a transferência internacional de dados pessoais "somente é permitida" nos casos contemplados pela lei.

3. O IMPACTO DA LGPD NOS ESCRITÓRIOS DE ADVOCACIA

3.1. O advogado/escritório de advocacia, precisa cumprir as determinações da LGPD?

A privacidade e proteção de dados pessoais passaram a ter mais valor e a irresponsabilidade no cuidado com eles pode gerar danos. Diante disso, os escritórios precisam abandonar os velhos hábitos e adotar novas medidas de proteção nas suas atividades.

A Lei Geral de Proteção de Dados (LGPD) determina diversas obrigações que organizações e empresas devem ter em relação ao manuseio e tratamento de dados pessoais de clientes em ambiente de trabalho, inclusive os escritórios de advocacia também devem estar atentos e adequados a essa nova lei!

Destaca-se que o inciso X do art. 5º da Lei n.º 13.709/2018, toda operação, física ou digital, realizada com dados pessoais para fins econômicos inclusive por pessoa natural, é considerada como tratamento de dados pessoais e se submetem à adequação.

A todo momento a prática jurídica envolve o uso de dados pessoais, seja no contato com clientes, prospecção, na produção de petições judiciais ou administrativas, bem como pareceres jurídicos e elaboração de contratos, entre outras atividades da profissão.

A advocacia é uma profissão que sempre viveu sob rígido controle da ética profissional da confidencialidade e proteção à privacidade. Isso já é característico da profissão, logo, a proteção de dados pessoais sempre foi necessária dentro dos escritórios, mesmo que não fosse de forma expressa, e embora ainda não existissem penalidades severas para falhas de tratamento.

Como veremos a seguir, a lei trouxe diversos desafios para os escritórios de advocacia e advogados autônomos. Porém, é necessário promover a adequação e melhorar a relação entre empresa e cliente.

3.2. Quais os impactos gerais da lei nos escritórios de advocacia?

Desde a vigência da mencionada lei, se tornou necessária a construção de uma política de governança em privacidade e o desenvolvimento de diretrizes para o armazenamento e tratamento de dados pessoais.

Os escritórios de advocacia não ficaram imunes à obrigatoriedade de adequação, inclusos de acordo com o art. 3º da referida lei, que não deixa dúvidas da extensão dos seus efeitos.

As múltiplas tarefas na rotina dos escritórios de advocacia, se tornam um maior desafio no processo de adequação. Por exemplo, para cumprir a rotina de análise de processos, petições, consultas, audiências, reuniões, contratos, dentre outras, faz com que no dia a dia muitos escritórios adotem procedimentos e ferramentas frágeis para assegurar a privacidade das informações.

Vale destacar que o Código de Ética e Disciplina da OAB, em seu artigo 25, trata da defesa ao sigilo profissional como forma de garantir o livre exercício da profissão, o que não se confunde com a proteção de dados em virtude da relação de negócio estabelecida entre as partes. Por isso, se esse advogado disponibilizar essa informação em software, por exemplo, é importante ter atenção com relação ao sigilo perante terceiros e a segurança do sistema, tendo em vista a relação negocial entre as partes.

Vejamos alguns casos na prática:

Uma conduta comum em escritórios é quando um cliente liga para o escritório querendo marcar uma reunião, e já na ligação a recepcionista colhe os primeiros dados como nome, e-mail, telefone, motivo do assunto. *No seu escritório, onde esses dados ficam armazenados e quem tem acesso a eles?*

Outro exemplo, é na primeira reunião o advogado já tem diversas informações pessoais, muitas vezes sigilosas sobre o cliente. Bem como também passa a armazenar documentos (escaneados ou originais) como comprovante de residência, contas bancárias, certidões (nascimento, casamento, óbito e outras), contracheque, fotos, provas sobre o caso. *Esses documentos vão para um sistema ou onde ficam armazenados? Quem no escritório consegue ter acesso a essas informações?*

As empresas e escritórios que não se adequarem à LGPD estão sujeitos às seguintes penalidades que serão aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD): **advertência, multas, publicização da infração, bloqueio dos dados pessoais, eliminação do banco de dados.**

Entre as penalidades que podem receber está a multa, que pode chegar a 2% do faturamento anual, entre outras penalidades previstas em lei. Como também, o advogado pode ter o seu banco de dados bloqueado ou sofrer alguma punição em relação à associação com outros advogados.

O escritório que não cumprir com a lei pode ter empecilhos com seus clientes e parceiros. Isso porque as pessoas estão cada vez mais cuidadosas com as empresas que desejam contratar, sobretudo se ela tiver de manejar seus dados pessoais. Sendo assim, os escritórios e advogados que não estiverem adequados podem perder parcerias jurídicas e comerciais.

Além disso, como já dissemos, uma multa pode ser aplicada ao escritório que não se adequar à lei, o que pode causar um dano financeiro a sua empresa. Bem como o dano à imagem do escritório diante do mercado, **que pode dificultar na conquista e fidelização de clientes, gerando graves prejuízos ao escritório.**

Diante do exposto, como primeiros passos para organizar o escritório estão: identificar quais dados você realmente necessita, fazer uma política de consentimento, revisar os seus contratos de honorários e deixar o cliente seguro sobre os dados que são coletados.

3.3. Como a LGPD afeta o escritório?

Os advogados lidam todos os dias com diversos dados confidenciais de clientes e parceiros e que, muitas vezes, podem ser acessíveis desde o computador da recepção até o acesso remoto de todos os estagiários e advogados.

Durante um processo judicial, por exemplo, documentos sempre são juntados contendo dados extremamente íntimos dos clientes. Por isso, os advogados devem se preocupar, por exemplo, com as seguintes questões:

- Como os dados dos clientes estão sendo solicitados?
- Qual o processo de armazenamento e exclusão desses dados?
- É pedida autorização para coletar essas informações dos clientes?
- Como é feita a exclusão dos dados: se o contrato não é firmado, as informações são removidas da sua base de dados?
- Leva-se em consideração as possíveis vulnerabilidades do sistema de armazenamento dessas informações a fim de estabelecer uma política de segurança efetiva e em conformidade com a LGPD?

A gestão de um escritório de advocacia, exige que o mapeamento de processos de recebimento e controle de dados, seja feito e reavaliado constantemente, para minimizar os riscos é importante tratar os dados desde quando são coletados até quando são excluídos.

Para isso é necessário saber qual a natureza dos dados mantidos, de que modo foram extraídos e com qual objetivo, quem pode acessá-los e manipulá-los, e qual será o período de retenção dessas informações.

Além disso, o processo de concessão de direitos sobre os dados deve ser feito tanto para quem já é cliente do escritório quanto para os novos clientes, por isso, é fundamental a revisão das atividades atuais de coleta de dados.

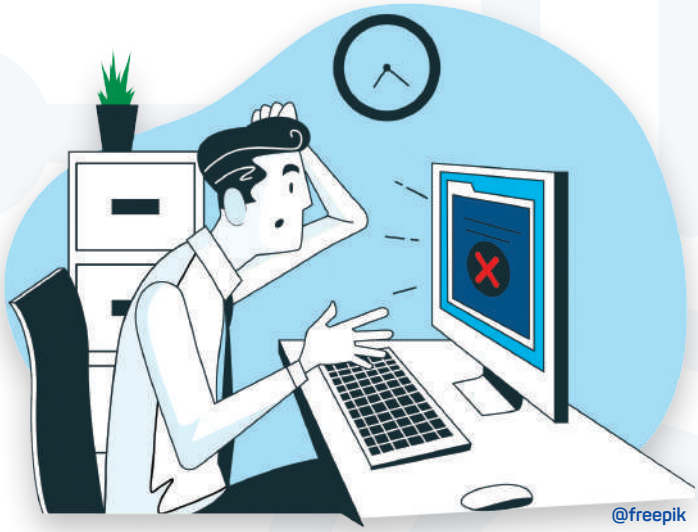
Também é importante que os advogados estejam atentos ao fato de que o cliente conta com o direito de obter informações acerca da coleta e o processamento de dados, assim como pode solicitar consultas, retificação, portabilidade e restrição, sendo assim, os escritórios devem estar preparados para isso, conforme previsto no rol de direitos dos titulares de dados, expostos nos artigos 18 e 20 da LGPD.

O gestor do escritório de advocacia deve analisar a maneira com que a coleta de dados é realizada, assim como as possíveis vulnerabilidades do sistema e buscar mitigá-las, a fim de estabelecer uma política de segurança efetiva e em conformidade com a LGPD.

Analisando os riscos na prática, imagine que o seu cliente teve um dado importantíssimo e íntimo exposto por uma falha na segurança do seu escritório, Devido a isso é emitido um alerta para a ANPD e iniciasse uma investigação e fiscalização e, ao fim, é constatado que o erro foi mesmo do escritório de advocacia.

Em decorrência disso, o escritório recebe uma multa, mas não basta pagá-la, é necessário corrigir o erro, caso não o façam, a ANPD pode bloquear os seus dados por um dia, até você corrigir o problema. *Imagine seu escritório e seus funcionários nessa situação: passar um dia inteiro sem conseguir acesso a nada do sistema interno e aos dados, ou seja, impossibilitados de trabalhar.*

Nada é tão ruim, que não possa piorar, se mesmo assim seu escritório não busca proteger seus dados e se adequar à nova Lei e a Autoridade resolve imputar



ao caso a exclusão do seu banco de dados: *Como seu escritório se manteria se todos os documentos, arquivos, fichas dos clientes desaparecessem de uma hora para outra?*

Além das consequências mencionadas, destaca-se o dano à imagem, ao nome do escritório que passará a ser totalmente denegrido com a publicidade diante de uma situação dessas, afinal de contas, se os advogados não conhecem e seguem a Lei nem para proteção interna do escritório, que dirá aplicar ela em prol dos clientes em suas causas.

Sendo assim, a LGPD afeta no dia a dia dos escritórios de advocacia na relação dele com seus colaboradores, com seus clientes, na revisão de contratos de honorários, com os cuidados com a utilização de aplicativos de troca de mensagens e comunicação em áudio e vídeo, e-mails corporativos e SMS, bem como os cuidados que devem ser observados nas reuniões virtuais, por isso, entre outras coisas, é importante criar políticas internas e manuais para a utilização desses mecanismos, além da utilização de plataformas seguras.

Além de afetar no tocante a relação do escritório e o poder público, sobretudo o Judiciário, o cadastro de documentos sigilosos em processo públicos, tudo passa a ser feito com mais cuidado e sigilo que o habitual.

Afeta também no substabelecimento de poderes para advogados correspondentes, no cuidado em saber onde estão armazenados os dados de clientes, colaboradores e fornecedores, e saber como é feito o descarte de documentos e dados pessoais internos e externos. Outro cuidado indispensável é com a relação do escritório de Advocacia e o site corporativo (termos de privacidade, uso de cookies), indicação de encarregado, cadastro de newsletter e formulários, por exemplo.

Todos esses instrumentos precisam ser tratados de acordo com as regras de sigilo e proteção previstas na LGPD.

3.4. Benefícios do cumprimento da lei nos escritórios de advocacia

Diante dos impactos da LGPD na advocacia já apresentados, é preciso criar uma cultura de proteção de dados interna nos escritórios, estabelecendo boas práticas e governança para conscientizar os colaboradores, funcionários, advogados e clientes que lidam todos os dias com dados pessoais.

Ao criar a cultura de proteção de dados, a tendência é que todos dentro do escritório, e mesmo os que trabalham remotamente, saibam utilizar os dados coletados de forma segura, tomando as decisões corretas a partir de dados extraídos de forma legal e, ainda, demonstrando transparência no relacionamento com os clientes.

O cumprimento da Lei dentro dos escritórios também será fundamental para os casos de compartilhamento de dados, são situações em que os dados pessoais são comunicados, difundidos, transferidos, interconectados ou internacionalmente.

Os terceiros, muitas vezes, representam riscos do ponto de vista da proteção de dados, por isso, os escritórios de Advocacia devem compreender claramente quais organizações que compartilham dados se vão realizar o tratamento deles ou não, e se estão dispostos a cooperar em questões relacionadas à proteção de dados. Os escritórios que se mostrarem adequados a essa nova Lei já se destacam dentro do mercado, o que gera grande benefício e visibilidade.

Outro ponto benéfico que a adequação à LGPD traz para os escritórios de advocacia são no tocante a Transferência internacional de dados, disciplinado pelos artigos 33 e 36 da Lei, a transferência internacional de dados apenas é permitida nos casos previstos em lei, como no caso de escritórios de advocacia que tenham escritórios correspondentes no exterior.

Contudo, isso vai variar de acordo com o nível de proteção de dados pessoais

que o país ou organismo internacional que o escritório brasileiro quiser fazer essa parceria, como correspondentes, ou outras que também envolvam transferência internacional de dados.

Para avaliar isso será analisado: as normas gerais e setoriais da legislação em vigor do local; a natureza dos dados; a observância dos princípios e direitos dos titulares; a adoção de medidas de segurança previstas em regulamento; a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais. Como também: o conteúdo de cláusulas-padrão contratuais; as normas corporativas globais; os selos, certificados e códigos de conduta aplicáveis.

Além disso, o compartilhamento internacional de dados também pode ocorrer em casos de o escritório ter clientes, pessoas físicas que sejam de outro país, ou até clientes pessoas jurídicas com filiais em outro país. Ou ainda se utilizar sistemas ou plataformas que tenham provedores internacionais, em todos esses casos deverá ser observada as regras dispostas na LGPD e as regulamentações da ANPD a respeito do tema.

4. COMPREENDENDO A LEI

4.1. Exceções ao cumprimento da LGPD nos escritórios de advocacia

Quando falamos da necessidade e importância de adequação à LGPD, inicialmente compreendemos que não importa a natureza jurídica de uma empresa, o seu tamanho, a volumetria dos dados, o número de colaboradores, ou até mesmo que não possua finalidades lucrativas, todas deveriam se adequar a nova lei.

Porém, no art. 4o., estão listadas as hipóteses de não aplicação da lei que são referentes apenas a alguns tipos específicos de tratamento e que não admitem ampliação interpretativa.

As hipóteses de isenção são quando o tratamento é realizado exclusivamente por pessoa natural para objetivos particulares/não econômicos; para fins jornalístico e artísticos, acadêmicos, de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais, devendo ser aprovada legislação especial para tais situações; ou provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Um exemplo disso é quando uma pessoa física, mesmo sendo pessoa natural, tratar de dados pessoais em sua atividade profissional cotidiana (por exemplo, os dados de seus clientes, fornecedores), deverá cumprir integralmente a LGPD no tocante ao tratamento desses dados. O que será uma exceção, pois, como regra geral, as pessoas físicas não estão sob a incidência da lei quanto aos dados forem tratados por ela para fins exclusivamente particulares e não econômicos.

Vale ressaltar que a Resolução nº 2 da ANPD cria características próprias para agentes de pequeno porte da adequação e cumprimento das novas regras da LGPD, porém, não os isenta.

Essa norma flexibiliza a LGPD para os agentes de tratamento de pequeno porte, tornando as regras mais simples de serem cumpridas se comparadas àquelas

previstas na lei geral, como para as microempresas e empresas de pequeno porte (sociedade empresária, simples, limitada unipessoal ou o empresário, inclusive o Microempreendedor Individual – MEI); as startups (organizações empresariais e societárias, nascentes ou em operação recente, que a atuação se caracterize pela inovação); as pessoas jurídicas de direito privado, inclusive sem fins lucrativos; e as pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais (profissionais liberais, condomínios, entre outros).

Contudo, conforme exposto, os escritórios de advocacia não estão inclusos no rol das exceções à aplicação da LGPD, muito pelo contrário, requer que sejam adequados imediatamente.

4.2. O que é tratamento de dados?

Tratamento de dados é 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, conforme previsto no artigo 5, inciso X, da LGPD.

Saber o que é tratamento de dados inclui também conhecer os seus princípios, que de acordo com o estabelecido na LGPD são divididos nos seguintes grupos:

- ✓ **Finalidade, adequação e necessidade:** visa limitar o uso e obtenção de dados.
- ✓ **Livre acesso, qualidade dos dados e transparência:** busca garantir que os donos das informações tenham acesso ao que foi feito com os seus dados.
- ✓ **Segurança, prevenção e não discriminação:** visa assegurar a proteção das informações.
- ✓ **Responsabilização e prestação de contas:** trata-se do dever de comprovar que adotou todas as medidas necessárias que assegurem a manipulação dessas informações em todos os momentos.

Como visto, o tratamento de dados pessoais é indispensável para todos que lidam com dados pessoais, veja a seguir quem são os agentes de Tratamento de Dados.

4.3. Quem são os agentes de tratamento de dados?

De acordo com a Lei Geral de Proteção de Dados, o tratamento de dados é realizado por dois agentes de tratamento: o controlador e o operador.

O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem decisões referentes aos dados pessoais. Ele é o responsável por tomar as decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento.

O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, incluindo agentes públicos bem como pessoas jurídicas diversas daquela representada pelo controlador.

Ou seja, quando um controlador atribui a outra pessoa o tratamento de dados, a ser realizado conforme a finalidade por ele delimitada, haverá um operador de dados, que trata os dados seguindo as orientações do controlador.

Ao tratar dados pessoais, a pessoa pode ser considerada um controlador ou operador. Esta definição tem impacto na responsabilidade e nas obrigações que você tem naquele determinado tratamento de dados.

Destaca-se também, um órgão importante, responsável pela fiscalização e pela regulação da LGPD, já mencionado aqui, é a ANPD (Autoridade Nacional de Proteção de Dados), vinculada à Presidência da República.

Na prática, o controlador possui mais obrigações pela LGPD, por exemplo, é ele que deve comunicar à ANPD, nos casos de incidentes de segurança, e elaborar o Relatório de Impacto à Proteção de Dados, nas hipóteses previstas na LGPD. Como também é seu dever o atendimento às solicitações dos titulares de dados.

Além disso, nos casos em que haja um dano decorrente de atividades de tratamentos de dados, o controlador pode ser responsabilizado perante terceiros pelas ações e omissões do seu operador.

A LGPD prevê também a figura do Encarregado pelo Tratamento de Dados Pessoais, esse é o principal responsável por garantir que uma organização esteja em conformidade com a LGPD, devendo atuar como um ponto de contato entre o controlador de dados, os titulares e a ANPD.

Na prática, entre as funções do Encarregado está: aceitar reclamações e comunicações dos titulares, receber comunicações da autoridade nacional e orientar funcionários e contratados sobre as práticas a serem tomadas em relação à proteção de dados pessoais.

4.4. Quem são os agentes de tratamento no escritório de advocacia?

Em todos os setores, inclusive nos escritórios de advocacia, é importante definir quem é o controlador ou operador. Para definir essas posições a ANPD publicou um Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, que traz orientações e exemplos sobre o tema.

Para isso, é preciso analisar se há outros agentes de tratamento envolvidos no procedimento em análise. O controlador será o advogado responsável pelo escritório, caso seja uma Sociedade Unipessoal de Advogado, caso seja uma Sociedade com mais de um advogado, o controlador será a própria pessoa jurídica. Ressalta-se que cabe ao controlador (advogado ou PJ), definir como os dados serão tratados, garantindo que o

escritório esteja em conformidade com as normas de privacidade de dados, protegendo, desta forma, as informações pessoais dos clientes (titulares de dados).

Por vezes, para desempenhar a prestação de serviços, pode ser necessário que o escritório de advocacia precise contratar empresa terceirizada para executar determinadas tarefas. Se na prestação do serviço, a empresa terceirizada tratar dados pessoais (pessoa física) dos clientes, será considerada operadora.

As empresas contratadas para executar funções específicas que envolvem dados pessoais em nome do controlador devem estar adequadas, uma vez que ao tratar dados, também são responsáveis pela conformidade no seu tratamento. A prestação de serviço pode incluir serviços de armazenamento em nuvem, serviços de processamento de folha de pagamento, empresas de gerenciamento de documentos, escritório de contabilidade, correspondente audiencista, entre outros.

Importante ressaltar que o controlador e a empresa operadora devem formalizar um contrato que defina claramente as obrigações e responsabilidades de ambas as partes em relação ao processamento de dados pessoais.

É fundamental que os escritórios de advocacia e as empresas operadoras entendam claramente suas responsabilidades em relação aos dados pessoais e estabeleçam procedimentos e acordos adequados para cumprir as regulamentações de proteção de dados, como a LGPD.

Em alguns casos, principalmente em pequenos escritórios, será comum que controlador e operador sejam a mesma pessoa, inclusive o próprio advogado.

Enquanto nos escritórios de advocacia, ainda que dispensado, caso o advogado indique um Encarregado, esta conduta será considerada uma boa prática, que pode contribuir para que eventuais sanções administrativas aplicadas pela ANPD sejam diminuídas.

A lei faculta que a sociedade de advogados possa escolher entre nomear uma pessoa física ou um grupo de pessoas para exercer o papel de Encarregado de Dados,

uma opção também nomear um comitê composto por um dos sócios e outras lideranças operacionais do escritório. O papel dele (ou deles) será discutir assuntos e tomar decisões acerca dos temas de privacidade e proteção de dados pessoais, representar o escritório na esfera judicial e administrativa, perante os órgãos fiscalizadores e aprovar eventuais mudanças operacionais que possam configurar fator de risco e penalidades.

Além disso, é importante que os escritórios de Advocacia compreendam claramente as organizações com as quais compartilham dados pessoais, e irão consequentemente realizar tratamento de dados pessoais em nome dos escritórios, e, portanto, serão operadores, além de compreender que os escritórios desenvolvem suas funções como controladores nesse contexto.

Como também devem ter atenção em como gerenciar o relacionamento com terceiros para assegurar que os dados pessoais estejam protegidos em todo o sistema ao qual são submetidos. É preciso que todos os parceiros dos escritórios adotem medidas apropriadas de proteção e segurança de dados e que estejam dispostos a cooperar em questões relacionadas à proteção de dados.

4.5. Quando o tratamento de dados é permitido no escritório de advocacia?

Conforme visto, o tratamento de dados dentro dos escritórios de advocacia é permitido em todas as atividades, desde o primeiro atendimento ao cliente até o arquivamento do processo, afinal de contas, os escritórios são grandes depósitos de dados pessoais, inclusive sensíveis.

Com o passar do tempo os próprios clientes passam a exigir a maior atenção com a privacidade de seus dados. Logo, o que antes era considerado apenas boa prática e diferencial competitivo para os escritórios de advocacia que já se preocupavam com isso, hoje passa a ser obrigação legal e requisito para se manter no mercado.

O processo de adequação é complexo e envolve uma ampla revisão das políticas de segurança e adoção de novos procedimentos internos dos escritórios, e exter-

@freepik

nos, no seu trato com clientes e parceiros, todas as atividades desempenhadas deverão passar por algum tipo de conformidade ou adaptação.

Por isso, é de extrema importância os escritórios trabalharem internamente sua cultura organizacional de proteção de dados, além de adotarem medidas que visem mitigar os riscos. Não basta que os escritórios passem por processos de adequação, mas sim que todos envolvidos sigam adotando medidas visando proteger os dados pessoais.

Diante disso, é fácil compreender que o tratamento de dados pessoais está presente em muitas atividades do cotidiano dos escritórios de advocacia, como por exemplo na relação com seus clientes, com seus colaboradores, como em novas contratações, ou até mesmo, na prospecção de novos clientes, através da adequação de sites e redes sociais de escritórios de acordo com a LGPD.

5. PRINCÍPIOS DA LGPD

A intenção com este tópico é que o advogado consiga perceber como os princípios são importantes, como realmente são a base de tudo. Entendendo-os, você começa a perceber situações do dia a dia que antes não eram notadas, como a quantidade de dados que são solicitados e não há verdadeira necessidade de coleta. Conscientização é a palavra-chave!

No Art. 6º, a LGPD determina 10 princípios que devem nortear o tratamento de dados pessoais. Estes princípios é que vão ajudar a garantir que a empresa esteja em conformidade e adequada à lei, são eles:

1	**finalidade:** propósitos legítimos, específicos, explícitos e informados ao titular;
2	**adequação:** compatibilidade do tratamento com as finalidades informadas ao titular;
3	**necessidade:** limitação do tratamento ao mínimo necessário, utilizando-se apenas de dados pessoais essenciais a suas finalidades;
4	**livre acesso:** consulta facilitada e gratuita, pelos titulares, sobre a forma, a duração do tratamento e a integralidade de seus dados pessoais;
5	**qualidade dos dados:** exatidão, clareza, relevância e direito à atualização dos dados;
6	**transparência:** informações claras, precisas e facilmente acessíveis aos titulares, observados os segredos comercial e industrial;
7	**segurança:** utilização de medidas técnicas e administrativas para proteger os dados pessoais;
8	**prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
9	**não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
10	**responsabilização e prestação de contas:** demonstração, pelos agentes de tratamento, da adoção de medidas eficazes e capazes de comprovar o cumprimento da lei.

6. QUAIS SÃO OS DIREITOS DOS TITULARES DE DADOS?

Antes de falar sobre os direitos dos titulares de dados, preciso explicar quem é essa figura tão importante na LGPD.

O Titular de Dados consoante prescreve a Lei nº 13709/18 em seu art.5º, inciso V, é "pessoa natural a quem se refere os dados pessoais que são objeto de tratamento". O dado pessoal, por sua vez, é definido como "informação relacionada a pessoa natural identificada ou identificável" (art 5º, I, LGPD). Ou seja, qualquer um de nós somos titulares de dados, inclusive o seu cliente.

Os titulares de dados pessoais (o cliente) poderão, a qualquer tempo, exercer os direitos perante o controlador de dados (advogado ou escritório de advocacia), de acordo com artigo 18 da lei, os direitos dos titulares de dados são:

6.1. Direito de confirmação da existência de tratamento

De acordo com a LGPD, o titular de dados tem o direito de obter do controlador (o advogado ou escritório de advocacia) a confirmação da existência de tratamento de seus dados pessoais. Esse direito é importante para que o titular de dados possa exercer seus outros direitos, como o direito de acesso, correção e exclusão de seus dados pessoais.

Para exercer esse direito, o titular de dados deve entrar em contato com o controlador de dados e solicitar a confirmação da existência de tratamento de seus dados pessoais. O controlador tem um prazo de até 15 dias para fornecer uma resposta ao titular de dados, que deve ser clara, precisa e objetiva.

É importante destacar que o direito de confirmação não garante ao titular de dados o acesso imediato aos dados pessoais em questão, mas apenas a confirmação de que eles estão sendo tratados pelo controlador. Para obter acesso aos dados pessoais, o titular deverá exercer o direito de acesso, que é outro direito previsto pela LGPD que falaremos a seguir.

6.2. Direito de acesso

Esse direito permite que o titular dos dados (ou seja, a pessoa a quem os dados se

referem) solicite informações sobre quais dados estão sendo coletados, processados e armazenados sobre ele ou ela.

De acordo com a LGPD, o titular dos dados pode solicitar acesso aos seus dados de forma gratuita e em formato claro e acessível, além de poder solicitar a correção de informações incorretas ou incompletas. O responsável pelo tratamento dos dados deve fornecer as informações solicitadas dentro de um prazo razoável e garantir a segurança e a privacidade dos dados durante o processo.

O direito de acesso é uma importante ferramenta para garantir a transparência e a responsabilidade no tratamento de dados pessoais e permite que os titulares dos dados tenham maior controle sobre suas informações pessoais.

6.3. Direito de correção de dados incompletos, inexatos ou desatualizados

De acordo com a LGPD, toda pessoa tem o direito de exigir que os controladores de dados corrijam suas informações pessoais, caso estas estejam incompletas, inexatas ou desatualizadas. Esse direito pode ser exercido de forma gratuita e a qualquer momento.

Vale ressaltar que o direito de correção não se limita apenas a dados pessoais. Ele também se aplica a qualquer informação que possa ser utilizada para identificar uma pessoa física, incluindo dados sensíveis, como informações médicas e religiosas.

O não cumprimento do direito de correção pode acarretar sanções administrativas, como multas e até mesmo a suspensão das atividades do controlador de dados.

6.4. Direito de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD

A anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD são medidas importantes para garantir a proteção dos dados pessoais dos usuários.

A anonimização consiste em tornar os dados pessoais irreversivelmente impossíveis de identificar, garantindo que não haja possibilidade de identificação dos indivíduos a que se referem. O bloqueio, por sua vez, consiste em suspender o acesso aos dados pessoais, mas mantendo-os armazenados. Já a eliminação é a remoção definitiva dos dados pessoais do sistema o qual devemos observar que nem todos os dados poderão ser eliminados tendo em vista que, se houver embasamento legal para guarda deverá ser comprovado ao titular de dados tal motivo.

Assim, as empresas devem garantir que os dados pessoais dos usuários sejam anonimizados, bloqueados ou eliminados quando necessário, de forma a evitar o tratamento indevido dessas informações e proteger a privacidade dos seus clientes, conforme previsto na LGPD.

6.5. Direito de portabilidade

Os titulares de dados têm o direito de transferir seus dados pessoais de uma empresa para outra. O escritório (advogado) deve fornecer os dados em um formato estruturado e comum. É muito comum no dia a dia da advocacia a portabilidade ocorrer em caso de substabelecimento para outro colega.

6.6. Eliminação dos dados pessoais tratados com o consentimento

Se o titular dos dados consentiu com o tratamento, mas mudou de ideia e não quer mais que a empresa trate seus dados pessoais, ele pode solicitar a eliminação desses dados. No entanto, há situações em que esse direito não pode ser exercido, como quando a empresa precisa conservar os dados para cumprir obrigação legal ou regulatória.

7. EXERCÍCIO DOS DIREITOS DOS TITULARES

7.1. De que maneira os titulares de dados poderão exercer seus direitos?

Para exercer os direitos, conforme estabelecido na própria LGPD, o titular de dados (ou seu representante legalmente constituído) primeiramente deve formalizar requerimento expresso diretamente ao controlador, responsável pelo tratamento dos dados pessoais.

Nesse contato direto com o controlador por meio dos canais oficiais, é possível que as solicitações do titular de dados sejam prontamente atendidas. Caso o titular não tenha sua solicitação atendida, pode apresentar petição à ANPD, com a comprovação da solicitação não solucionada pelo controlador.

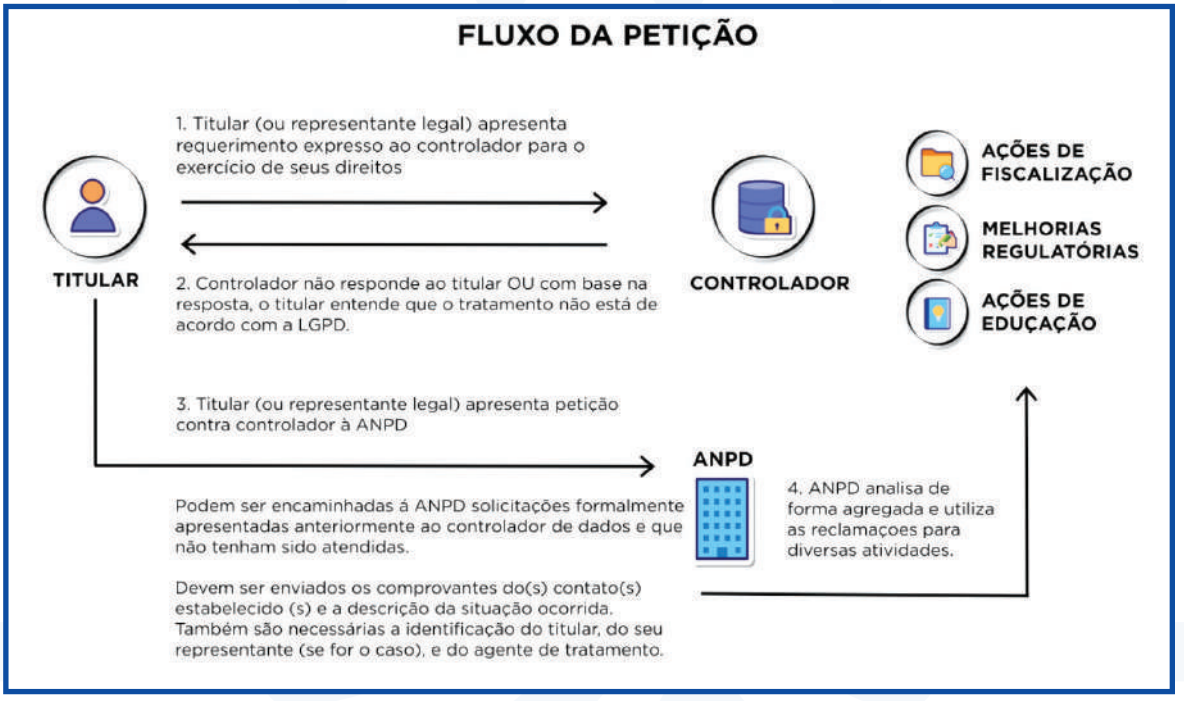
Ao apresentar petição à ANPD, a LGPD estabelece a necessidade de que o titular envie comprovante do requerimento apresentado ao controlador de dados. Assim, ao formalizar solicitação por meio dos canais oficiais do controlador, é recomendável que o titular de dados guarde os dados do contato, como, por exemplo, número de protocolo, orientações recebidas, mensagens e e-mails.

Também são necessárias a identificação do titular, do seu representante (se for o caso), e do agente de tratamento.

Caso o controlador não atenda as demandas solicitadas deve ser utilizado o Peticionamento Eletrônico.

(https://super.presidencia.gov.br/controlador_externo.php?acao=usuario_externo_logar&acao_origem=usuario_externo_gerar_senha&id_orgao_acesso_externo=0)

7.2. Entenda o fluxo da petição:



Fonte: Site ANPD.

8. ENCARREGADO DE DADOS NA ADVOCACIA

8.1. Papel do encarregado de dados na advocacia

O Encarregado de Proteção de Dados é a "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)", conforme preconiza o art. 5º, inciso VIII, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

O encarregado de dados é responsável por supervisionar a implementação e a aplicação das políticas de privacidade e proteção de dados da empresa, bem como garantir que os processos e procedimentos relacionados à coleta, armazenamento, processamento e compartilhamento de dados pessoais estejam em conformidade com as leis de proteção de dados aplicáveis.

O Encarregado também é o ponto de contato entre a empresa e as autoridades reguladoras de proteção de dados e deve estar sempre atualizado sobre as mudanças nas leis e regulamentos de proteção de dados, a fim de garantir que a empresa esteja sempre em conformidade.

Suas atividades são definidas pelo art. 41, §2º, da mesma norma.

8.2. O Escritório de advocacia é obrigado a contratar um encarregado de dados?

Mas afinal, o escritório de advocacia é obrigado a contratar um encarregado de dados?

Na nossa opinião, depende:

A Resolução CD/ANPD nº2/2022 de 27 de janeiro de 2022, o qual é o regulamento de aplicação da Lei Geral de Proteção de Dados

Pessoais para tratamento de pequeno porte na Seção IV, art. 11 preceitua que os agentes de pequeno porte não são obrigados a indicar o encarregado pelo tratamento dos dados pessoais exigidos no art. 41 da LGPD, porém os que não indicarem, obrigatoriamente devem disponibilizar um canal de contato com o titular para atender o dispositivo no art. 41 § 2º, I da Lei.

Vale ressaltar que, a indicação de encarregado de dados por parte dos agentes de pequeno porte, será considerada política de boas práticas e governança conforme dispõe o art. 52, §1º, IX da LGPD.

A mesma resolução trouxe exceções de benefícios de tratamento jurídico onde não poderão se beneficiar do tratamento jurídico diferenciado previsto no regulamento os agentes de tratamento de pequeno porte que realizem tratamento de alto risco para os titulares, sendo considerado tratamento de alto risco de dados pessoais aqueles que atenderem de forma cumulativa pelo menos um dos critérios gerais e específicos indicados no artigo 4º da resolução supracitada.

Ou seja, se for um advogado autônomo com um escritório pequeno, ou que esteja trabalhando em home office sozinho, não há a necessidade de contratar um encarregado de dados, porém deverá obrigatoriamente ter um canal de comunicação que atenda o titular de dados (o cliente).

Já se estivermos falando de um escritório de grande porte e que trate dados de alto escala, o mesmo deve contratar o encarregado de dados para estar em consonância com a lei.

Fonte: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpdn-2-de-27-de-janeiro-de-2022-376562019

9. COMO O ADVOGADO/ESCRITÓRIO DEVE PROTEGER OS DADOS

O projeto de adequação é o meio pelo qual o controlador/advogado utiliza para garantir o cumprimento dos requisitos normativos e de segurança da informação estabelecidos na lei, demonstrando clareza, responsabilidade e confiança com as informações e documentos fornecidos pelos titulares/clientes.

9.1. O que é projeto de adequação?

O projeto de adequação à LGPD é um conjunto de ações que permitem que o gestor do escritório de advocacia esteja de acordo com a Lei Geral de Proteção de Dados.

Nota-se que é um **conjunto de ações**, não apenas um ato isolado. Não são só documentos, não é só política de privacidade, não são apenas medidas de segurança da informação, não é apenas utilização de software.

Um projeto de adequação deve ser feito de forma personalizada, moldado à realidade e às necessidades específicas do escritório de advocacia. O objetivo do projeto é fomentar a mudança de cultura no escritório, incluindo uma nova cultura voltada à proteção de dados.

9.2. Etapas do projeto de adequação

Não existe uma regra específica quanto a essa questão, porém para que possa ter uma organização e metodologia geralmente são utilizadas as seguintes etapas:

A) CONSCIENTIZAÇÃO – Objetivo dessa fase é mostrar a importância da lei e sua aplicabilidade na prática.

B) MAPEAMENTO – O objetivo dessa fase é mapear os dados para que seja possível identificar as principais exposições e contingências do escritório. Todo o fluxo de dados deverá ser analisado e descrito:

- Qual a origem do dado?
- Qual a categoria do dado?
- Qual a finalidade de tratamento?
- Ele é compartilhado com alguém? Se sim, quem? Por quê?
- Qual o período de retenção daquele dado?
- Qual a hipótese de tratamento daquele dado?
- Qual a categoria? (dado comum, sensível, criança, adolescente, idoso)
- Onde o dado fica armazenado?
- Quais colaboradores têm acesso? Por que possuem acesso?

C) GAP ANALYSIS – Objetivo nessa fase é de identificação dos principais pontos de desconformidade com a legislação, apontando as soluções e mitigar os riscos através do mapeamento de dados realizado na fase anterior. Nesta fase é realizado um relatório de impacto onde tem a finalidade de mensurar os riscos existentes e identificar as providências tomadas pelo controlador.

D) PLANEJAMENTO – Objetivo nessa fase é planejar a forma de execução das soluções propostas na fase anterior, priorizando às áreas que contêm mais riscos.

E) IMPLEMENTAÇÃO – Objetivo nessa fase é colocar a prática no plano de ação, incluindo a elaboração de todos os documentos que se fizerem necessários. Momento esse que será realizado a política de privacidade, código de conduta, aditivos contratuais etc;

F) MONITORAMENTO – Objetivo nessa fase é manter o monitoramento constante do cumprimento das diretrizes estabelecidos no programa de governança em proteção de dados, fazer as atualizações que se fizerem necessárias para garantir que o escritório se mantenha em conformidade.

9.3 Medidas administrativas, técnicas e de segurança da informação que deverão ser observadas

Neste tópico, citaremos algumas medidas simples e que fazem toda diferença no dia a dia do escritório de advocacia:

- ✓ Envio consciente e responsável de e-mail: quando for encaminhar e-mail para mais de uma pessoa, prefira sempre colocar em cópia oculta, afinal e-mail é um dado pessoal;
- ✓ Cuidado com e-mails suspeitos: tenha cuidado ao abrir e-mails de remetentes desconhecidos ou suspeitos, eles podem conter vírus ou *phishing*;
- ✓ Atualize seu software: mantenha seu software atualizado com as atualizações de segurança mais recentes;
- ✓ Use um software antivírus: instale um *software* antivírus confiável em seu computador e mantenha-o atualizado para ajudar a proteger seus arquivos contra vírus e outras ameaças;
- ✓ Proteja sua conexão *Wi-Fi*: certifique-se de que sua conexão *Wi-Fi* esteja protegida com uma senha forte e que a criptografia WPA2 esteja ativada;
- ✓ Utilizar criação de backups dos dados armazenados, de preferência que o mesmo esteja na nuvem;
- ✓ Criação de senhas fortes – senhas devem conter combinação de caracteres especiais, letras maiúsculas, minúsculas e números, evitando utilizar dados pessoais ou palavras comuns;
- ✓ Habilitar a verificação de senhas em duas etapas, sempre que disponível, principalmente em sistemas de armazenamento em nuvem e aplicativos de mensagens;

- ✓ Desconfiar de links recebidos por aplicativos de mensagens;
- ✓ Fotos digitais de processos e documentos: após tirar cópias digitais de processos judiciais ou extrajudiciais, bem como de documentos pessoais é importante tomar cuidado com a forma como essas fotos serão armazenadas. Ao utilizar um celular cuidado para que essas informações não sejam armazenadas em local de fácil acesso, alguns serviços de armazenamento em nuvem já permitem salvar o documento diretamente neles, sempre que possível escolha essa opção. Se não for possível, após transferir as imagens para um local seguro, lembre-se de excluir do dispositivo;
- ✓ Uso de *Whatsapp*: apesar de ser muito exigido atualmente pelos clientes, o envio de documentos com dados pessoais e dados pessoais sensíveis deve ser evitado, mesmo quando utilizamos um aplicativo que informa utilizar criptografia de ponta a ponta. Como se sabe, não existem garantias de que o documento enviado ou as informações compartilhadas são de fato seguras ou que não sejam armazenadas (ainda que temporariamente) em locais com alto risco de incidentes. Não é incomum uma pessoa enviar, por engano, um documento ou informação para terceiro que não era o destinatário, essa situação, por si só, já caracteriza um incidente de segurança;
- ✓ Redes Sociais: cada vez mais advogados e escritórios postam fotos de documentos ou processos em suas redes sociais como forma de gerar conteúdo. Além de questões éticas que devem ser analisadas, há também elementos que podem caracterizar incidente de segurança de dados. Evite postar fotos de documentos de clientes em redes sociais, mesmo se o processo judicial ou administrativo for público;
- ✓ Não compartilhe informações pessoais de seus clientes: não compartilhe informações pessoais como documentos, imagens, dados sensíveis ou informações de cartão de crédito, com ninguém on-line, lembre-se que nenhum tribunal, polícia federal, polícia civil, faz ligação telefônica ou requisita por e-mail informações de seus clientes;
- ✓ Mantenha a privacidade em mente: sempre que possível, evite armazenar informações prolongadas, como informações de cartão de crédito ou documentos de identificação, em seu computador. Se você precisar armazenar essas informações, criptografe-os;
- ✓ Seja cuidado ao usar computadores públicos: se precisar usar um computador público, tenha cuidado ao inserir informações pessoais e sempre saia de todas as contas quando terminar.

10. DÚVIDAS QUE PODEM SURGIR SOBRE A LGPD NOS ESCRITÓRIOS DE ADVOCACIA

10.1. O escritório ainda possui muitos documentos físicos, o quê fazer?

Para que o tratamento de dados pessoais seja realizado de maneira transparente e segura, garantindo a privacidade e a proteção dos direitos dos titulares dos dados, é importante redobrar a atenção aos documentos físicos, uma vez que podem conter informações pessoais sensíveis, como dados relacionados à saúde, documentos fiscais, contábeis, imagens e informações em petições iniciais de processos em segredo de justiça, claro, além de todos os dados que identificam o cliente.

Visando garantir a proteção desses dados, é importante que os escritórios de advocacia implementem medidas de segurança física, como o processamento adequado em locais de acesso restrito e o uso de métodos de identificação de acesso.

Além disso, a LGPD prevê, em algumas circunstâncias, a necessidade de consentimento expresso dos titulares dos dados para o tratamento de suas informações, mesmo que já tenham sido coletadas anteriormente. Assim, caso o escritório de advocacia ainda possua documentos físicos contendo dados pessoais, é importante verificar se possui autorização expressa dos titulares para o tratamento desses dados e, caso contrário, obtenha essa autorização antes de continuar usando essas informações.


@jemastock

Existe um entendimento errado em relação aos documentos físicos, a lei tutela os dados físicos e digitais, sem distinção, desta forma, a LGPD não proíbe que o escritório

de advocacia tenha arquivos físicos. A lei se aplica tanto a dados pessoais em formato digital quanto em formato físico, portanto, não há proibição para a manutenção de documentos em papel.

No entanto, a LGPD estabelece que é necessário garantir a segurança dos dados pessoais tratados, independentemente de seu formato, e tomar medidas para evitar acidentes de fuga, perda, acesso não autorizado ou destruição.

Caso o escritório precise se desfazer de documentos físicos contendo dados pessoais sensíveis, é importante que isso seja feito de forma segura, utilizando métodos que garantam a destruição completa e definitiva dos documentos.

Além disso, a LGPD determina que os titulares dos dados pessoais têm direito de solicitar a exclusão de seus dados tratados pelo escritório, seja em formato digital ou físico, desde que não haja motivo legal para a manutenção desses dados. Portanto, o escritório de advocacia deve estar preparado para atender as aulas e garantir a segurança na exclusão dos dados em formato físico.

10.2. Como manter os arquivos físicos seguros?

Para manter os arquivos físicos seguros e em conformidade com a LGPD, é importante adotar as seguintes medidas:

1 **Armazenamento adequado:** é importante armazenar os documentos em local seguro e controlado, de preferência em armários ou gavetas trancados, com acesso restrito apenas aos funcionários autorizados. Além disso, é importante evitar o armazenamento de documentos em áreas de acesso público, por exemplo, não deixar processos ou documentos expostos em mesas ou em máquinas fotocopiadoras;

2 **Controle de acesso:** é importante estabelecer políticas de acesso aos documentos, identificando quem tem autorização para acessá-los e em quais circunstâncias. É possível adotar medidas como o controle de acesso físico ao local de armazenamento, o registro de entrada e saída dos documentos e a identificação de quem acessou cada documento;

3 **Rastreamento do acesso:** registrar e rastrear o acesso aos documentos, identificando quem acessou cada documento e quando. Isso pode ser feito por meio de um sistema de registro de acesso ou por meio de um registro manual;

4 **Monitoramento de possíveis exposições:** monitorar as possíveis exposições ou tentativas de acesso não autorizado aos documentos, estabelecendo protocolos de segurança e ações preventivas para minimizar esses riscos;

5 **Descarte seguro:** quando for necessário descartar documentos físicos, é importante fazê-lo de maneira segura, através de trituradora, evitando, assim, a reconstituição do documento.

10.3. O escritório tem obrigação de digitalizar todos os documentos?

Não, a LGPD não obriga o escritório de advocacia a digitalizar todos os documentos. No entanto, a digitalização pode ser uma alternativa para facilitar a gestão e garantir a segurança dos dados pessoais contidos nos documentos, desde que sejam adotadas medidas de segurança para proteger esses dados.

A digitalização de documentos pode trazer benefícios para o escritório, como a redução do espaço físico necessário para o armazenamento, a facilidade de acesso e a possibilidade de fazer backups e cópias de segurança. No entanto, é importante garantir que a digitalização seja feita de forma segura, garantindo a integridade e confidencialidade dos dados pessoais.

Caso o escritório opte pela digitalização dos documentos, é importante adotar medidas de segurança, como o uso de softwares de criptografia, o armazenamento em servidores seguros, o controle de acesso aos documentos digitalizados e a realização de backups regulares. Além disso, é importante verificar se a digitalização de documentos é permitida para determinados tipos de processos ou documentos, de acordo com as normas protegidas pela Ordem dos Advogados do Brasil (OAB) e outros órgãos reguladores.

Vale lembrar que, caso opte pela digitalização de documentos, o escritório de advocacia deve adotar medidas de segurança para garantir a proteção desses dados, seguindo os mesmos princípios de segurança aos documentos físicos. Isso inclui medidas como o armazenamento em local seguro e controlado, o controle de acesso, o rastreamento do acesso, a utilização de criptografia para proteger os dados, entre outras medidas.

Além disso, a LGPD exige que os dados pessoais sejam retidos apenas pelo tempo necessário para a finalidade para a qual foram coletados, portanto, é importante avaliar a necessidade de manter tanto os documentos físicos quanto os digitais, de acordo com as exigências da legislação.

10.4. Como manter os arquivos digitais seguros?

Manter arquivos digitais seguros é fundamental para proteger informações pessoais, profissionais e confidenciais de ameaças digitais, como *hackers* ou compartilhamento indevido de informações. O escritório de advocacia, como controlador dos dados pessoais de seus clientes, deverá tomar todas as medidas necessárias para manter os arquivos digitais seguros, conforme mencionado no item 10.2.

10.5. O escritório deve inserir cláusula de proteção de dados nas procurações e/ou contratos de honorários?

A lei estabelece regras para o tratamento de dados pessoais e sensíveis, e sua aplicação é obrigatória para empresas e organizações que coletam, armazenam, tra-

tam e guardam dados pessoais de terceiros. Portanto, os escritórios de advocacia, que também lidam com informações pessoais e sensíveis de seus clientes, estão sujeitos à lei. Desta forma, é importante que os escritórios de advocacia incluam cláusulas de proteção de dados em seus contratos, procurações e demais documentos usados em suas atividades.

Destarte, a inserção de cláusulas da LGPD em contratos e procurações é uma medida importante para garantir a transparência e a conformidade do escritório de advocacia com a lei, além de proteger os direitos e a privacidade dos titulares dos dados.

É importante destacar que apenas inserir cláusulas relacionadas à Lei Geral de Proteção de Dados não é suficiente para garantir a conformidade com a legislação. O escritório de advocacia também deve seguir outros requisitos, como implementar medidas técnicas e organizacionais planejadas para proteger os dados pessoais dos clientes, tanto na execução do contrato, quanto nas situações em que necessita do consentimento adequado para o tratamento de dados e manter um registro de todas as atividades de processamento de dados.

Além disso, é importante lembrar que a LGPD se aplica a qualquer tipo de dados pessoais, incluindo informações relacionadas a clientes, funcionários e estagiários do escritório de advocacia.

Por fim, recomenda-se que o escritório de advocacia busque assessoria jurídica especializada ou estude a lei e desenvolva um projeto de adequação, para garantir que todas as medidas necessárias sejam tomadas no cumprimento da LGPD e proteger os dados pessoais de seus clientes e funcionários.

10.6. Caso o escritório compartilhe dados dos clientes, quais medidas devem ser tomadas?

Se o escritório de advocacia compartilhar dados dos clientes com terceiros, é importante tomar medidas para garantir a conformidade com a lei. Algumas medidas que podem ser aceitas incluem:

- Obter o consentimento adequado: antes de compartilhar dados pessoais dos clientes, o escritório deve obter o consentimento expresso e específico deles. O consentimento deve ser informado, livre, inequívoco e revogável a qualquer momento;
- Implementar medidas de segurança: o escritório de advocacia deve implementar medidas técnicas e organizacionais para garantir a segurança dos dados pessoais dos clientes durante o compartilhamento, isso pode incluir criptografia de dados, restrição de acesso e monitoramento de atividades;
- Garantir a conformidade dos terceiros: o escritório deve verificar se os terceiros, como por exemplo, escritórios de contabilidade, escritórios que atuam como correspondentes, audiencistas, estão em conformidade com a LGPD. Isso pode ser feito por meio de contratos que incluem cláusulas de proteção de dados e pela avaliação da política de privacidade e segurança dessas empresas ou pessoas físicas;
- Manter registros de compartilhamento: o escritório deve manter um registro de todas as atividades de compartilhamento de dados pessoais dos clientes, incluindo os terceiros envolvidos, a fim de verificar as medidas de segurança adotadas;
- Notificar os clientes: em alguns casos, o escritório de advocacia pode ser obrigado a notificar os clientes sobre o compartilhamento de seus dados pessoais com terceiros, especialmente se houver riscos de privacidade e segurança desses dados.

É importante lembrar que o compartilhamento de dados pessoais dos clientes deve ser realizado com cautela e apenas quando necessário para a prestação dos serviços de advocacia.

10.7. Quando o escritório possui site, quais medidas precisam ser observadas?

Se o escritório de advocacia possui um site, é importante tomar medidas para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD) e proteger os dados pessoais dos visitantes do site. Algumas medidas que podem ser tomadas, incluem:

Fornecer informações claras sobre o tratamento de dados: disponibilizar informações claras e transparentes sobre o tratamento de dados pessoais no site, através do aviso de privacidade, aviso e política de cookies;

Disponibilizar aviso e política de privacidade: disponibilizar aviso de privacidade e política de privacidade clara, que detalhe as informações e explique como os dados pessoais dos visitantes do site serão tratados;

Disponibilizar aviso e política de *cookies*: Ao começar a navegação, o usuário, cliente do escritório ou não, deverá ser informado de maneira clara, quais cookies o site coleta, assim como possibilidade de gerenciamento;

Nomear um encarregado de proteção de dados: O escritório deve nomear um encarregado de proteção de dados para garantir a conformidade com a LGPD e atuar como ponto de contato para questões relacionadas à proteção de dados. A informação de meio de contato com o encarregado de dados também deve ser informado de forma clara no site, através de e-mail para garantir o cumprimento dos direitos dos titulares de dados – artigo 18 da lei;

É importante lembrar que a LGPD se aplica a qualquer tipo de dados pessoais, incluindo informações relacionadas aos visitantes do site. Portanto, é crucial que o escritório de advocacia esteja em conformidade com a lei, para evitar danos aos titulares. O escritório pode buscar assessoria jurídica especializada para garantir que todas as medidas necessárias sejam tomadas para garantir a conformidade com a LGPD e proteger os dados pessoais dos titulares ao navegar no site.

10.8. É necessário realizar treinamentos no escritório?

Sim, assim como em qualquer projeto de adequação, é importante realizar treinamentos no escritório de advocacia para conscientizar os colaboradores sobre a Lei Geral de Proteção de Dados e garantir sua conformidade. Alguns dos benefícios dos treinamentos em LGPD incluem:

- ✓ **Conscientização sobre a importância da privacidade e segurança dos dados pessoais dos clientes:** os treinamentos ajudam os colaboradores e estagiários a entender a importância da privacidade e segurança dos dados pessoais dos clientes e adotar medidas para protegê-los;
- ✓ **Conhecimento sobre as obrigações legais:** os treinamentos ajudam os colaboradores e estagiários a conhecerem suas obrigações legais relacionadas à proteção de dados pessoais, incluindo o dever de confidencialidade e a necessidade de obter consentimento adequado, quando necessário;
- ✓ **Melhoria das práticas internas:** os treinamentos ajudam a identificar as áreas de risco para o tratamento de dados pessoais e a adoção de medidas preventivas para minimizar os riscos;
- ✓ **Redução de riscos legais e financeiros:** os treinamentos ajudam a reduzir os riscos legais e financeiros associados à não conformidade com a lei, incluindo multas e danos à confiança.

Os treinamentos em LGPD devem ser realizados regularmente e adaptados ao público-alvo, considerando as funções e responsabilidades de cada área, caso o escritório tenha vários setores, como RH, marketing, diretoria, advogados e estagiários.

11. DESCUMPRIMENTO DA LEI

O descumprimento da Lei Geral de Proteção de Dados pode gerar consequências negativas para empresas e indivíduos e com os escritórios de advocacia, não poderia ser diferente. A inobservância dos requisitos legais podem resultar em:

- **MULTAS:** A LGPD prevê multas que podem chegar a 2% do faturamento da empresa até, limitado a um total de R$50 milhões por infração. As multas podem ser aplicadas tanto pelo órgão regulador quanto pelo meio de ações de julgamento movidas por indivíduos dependentes, quando algum dos direitos dos titulares não for observado;

- **PERDA DE CREDIBILIDADE:** o descumprimento da LGPD pode causar danos à reputação da empresa, especialmente se houver divulgação pública do incidente;

- **AÇÕES JUDICIAIS:** os titulares que tiverem seus direitos violados, têm o direito de entrar com ações judiciais por danos morais e materiais, o que pode levar a um aumento dos custos para o escritório. Além disso, o Ministério Público pode ajuizar ações civis públicas e as empresas podem ser responsabilizadas pelo dano causado;

- **SUSPENSÃO DAS ATIVIDADES:** em casos mais graves, o órgão regulador pode determinar a suspensão das atividades da empresa por tempo determinado, até que sejam tomadas medidas para garantir a proteção de dados;

- **PROIBIÇÃO DE ATIVIDADES:** a LGPD também prevê a possibilidade de proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados pessoais.

É fundamental que as empresas e indivíduos estejam em conformidade com a LGPD para evitar paralisação das atividades, prejuízos financeiros e reputacionais.

12. SANÇÕES

O artigo 52 da Lei Geral de Proteção de Dados, estabelece uma série de sanções administrativas que podem ser aplicadas em casos de violação de suas disposições. Essas sanções visam incentivar o cumprimento da legislação de proteção de dados pessoais, bem como garantir a proteção dos direitos dos titulares de dados.

12.1. Sanções administrativas

Advertência: é uma forma mais branda de sanção e pode ser aplicada em casos de infrações de menor gravidade. A autoridade de proteção de dados pode notificar o infrator e orientá-lo a corrigi-lo;

Multa simples: a multa simples pode ser aplicada em casos de infrações mais graves, mas que não geram prejuízos diretos aos titulares de dados (2% do faturamento da empresa, limitada a R$ 50 milhões por infração);

Multa diária: a multa diária pode ser aplicada quando a infração continuar ocorrendo após a aplicação de uma multa simples ou quando há uma obrigação de fazer ou não fazer descumprida (1% do faturamento da empresa, limitada a R$ 50 milhões por infração);

Publicização da infração, que pode ser feita por meio de comunicação pública da infração cometida pela empresa;

Bloqueio ou eliminação dos dados pessoais, que podem ser determinados pelo órgão competente em caso de infração à LGPD;

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 parcial 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 parcial ou total do exercício de atividades relacionadas ao tratamento de dados pessoais. Esta proibição pode ser aplicada em casos extremos, quando a empresa demonstrar falta de compromisso com a proteção dos dados pessoais .

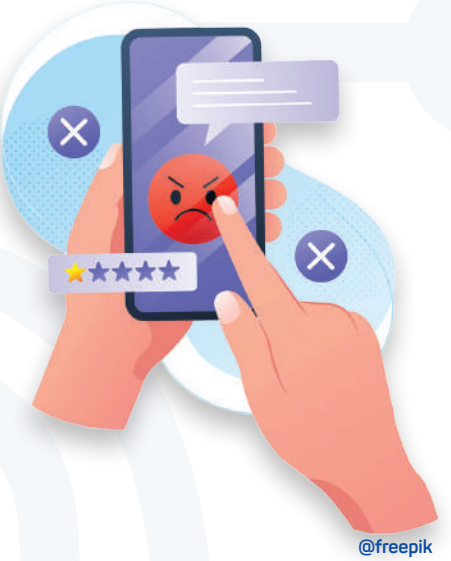
É importante ressaltar que a aplicação das sanções administrativas previstas na LGPD é responsabilidade da Autoridade Nacional de Proteção de Dados (ANPD), que deve levar em consideração a gravidade e a reiteração das infrações, o porte econômico da empresa, a boa-fé do infrator, entre outros fatores. Além disso, as empresas têm o direito de defesa, apresentando provas, objetivando demonstrar conformidade.

12.2. Sanções cíveis

Além das sanções administrativas, o titular de dados também pode ter seu direito garantido na esfera cível em caso de descumprimento de seus direitos. O titular pode ajuizar ação de indenização por danos morais e materiais causados por descumprimento às determinações da Lei Geral de Proteção de Dados, desde que demonstre o prejuízo causado.

Vale ressaltar que as sanções cíveis podem ser aplicadas de forma disciplinar ou em conjunto com as instruções administrativas previstas na LGPD.

13. DANO REPUTACIONAL



O dano reputacional pode ser compreendido como um dano invisível, pois não está expresso na lei. Sabemos que muitas empresas ainda não se adequaram à LGPD ou não estão seguindo suas diretrizes corretamente, o que pode levar a sérios danos reputacionais e financeiros. O descumprimento legal pode resultar em multas e outras sanções previstas no artigo 52, da LGPD, mas o dano reputacional é ainda mais grave, pois afeta diretamente a confiança dos clientes e parceiros de negócios.

Quando uma empresa/escritório de advocacia é responsável por um vazamento ou uso indevido de dados pessoais, a repercussão negativa pode se intensificar rapidamente nas redes sociais, na imprensa e em outros meios de comunicação. Isso pode levar a uma perda significativa de clientes e receitas, bem como a danos à imagem e confiança no escritório.

Por isso, é fundamental que as empresas estejam atentas às obrigações da LGPD e implementem medidas efetivas para proteger os dados pessoais dos clientes. Isso inclui medidas técnicas e organizacionais, como a adoção de políticas claras de privacidade, a realização de auditorias e monitoramento da segurança dos dados, a adoção de medidas e controle de acesso, entre outras.

É importante ressaltar que o dano reputacional por descumprimento da LGPD é um dano invisível, mas que pode causar diversas consequências para as empresas. Muitas vezes, as empresas subestimam o impacto do descumprimento da LGPD em sua imagem, porém, isso pode ser extremamente prejudicial em longo prazo. Em um escritório de advocacia, a confiança do cliente é a peça fundamental da relação entre advogado e cliente, sem ela, torna-se impossível a continuidade da prestação de serviço.

O resultado da falta de confiança gera uma série de consequências negativas, como a perda de clientes, a dificuldade em atrair novos clientes, a queda na prestação de serviço e no faturamento, a desvalorização do escritório e até mesmo interposição de processos por danos morais ou materiais.

14. RESPONSABILIDADE SOLIDÁRIA

A lei, em seu artigo 42, estabelece a responsabilidade solidária entre controlador e operador no tratamento de dados pessoais. Isso significa que tanto o controlador, que é a pessoa física ou jurídica responsável pelas decisões referentes ao tratamento de dados pessoais, quanto o operador, que é a pessoa física ou jurídica que realiza o tratamento de dados em nome do controlador, são responsáveis pela proteção dos dados pessoais dos titulares.

A responsabilidade solidária implica que, em caso de infração à LGPD, tanto o controlador quanto o operador poderão ser responsabilizados e sancionados pela autoridade competente, de acordo com as disposições da LGPD.

A LGPD estabelece que o controlador deve garantir, por meio de contrato ou de outro instrumento legal, que o operador também esteja adequado à lei, especialmente no que se refere à proteção de dados pessoais.

Dessa forma, a responsabilidade solidária na LGPD tem o objetivo de garantir a proteção dos dados pessoais dos titulares, incentivando uma maior colaboração entre controlador e operador na implementação de medidas de segurança e privacidade.

Importante enfatizar, que a inclusão de uma cláusula de responsabilidade unilateral em um contrato não exclui a responsabilidade solidária das partes envolvidas (controlador e operador), inclusive em relação ao cumprimento da Lei Geral de Proteção de Dados.

É importante ressaltar que a LGPD não permite a transferência da responsabilidade exclusivamente para o controlador ou o operador de dados. As partes devem cumprir com suas obrigações e responsabilidades protegidas na lei, independentemente do que estejam previstos em contratos entre elas.

15. PLANO DE GESTÃO CONSTANTE

A Lei Geral de Proteção de Dados estabelece uma série de regras e diretrizes para a proteção e tratamento de dados pessoais de titulares no Brasil. Uma demonstração de boa prática definida pela lei é a implementação de um plano de gestão constante, que tem como objetivo garantir a conformidade das empresas com as exigências da LGPD em relação à proteção de dados.

O plano de gestão constante deve ser uma estratégia contínua que envolve a implementação de medidas técnicas, administrativas e organizacionais para garantir a privacidade e segurança dos dados pessoais que são coletados e tratados pela empresa/escritório. Isso inclui a criação de políticas internas, a definição de processos de gerenciamento de dados e adoção de tecnologias adotadas para a proteção dessas informações.

Entre as principais etapas do plano de gestão constante da LGPD, podemos destacar:

- Treinamento e conscientização: capacitar funcionários e estagiários do escritório sobre a importância da proteção de dados pessoais e como lidar com essas informações;
- Monitoramento e revisão: realizar auditorias e revisões periódicas para garantir que as medidas de segurança aceitas estejam funcionando de acordo e avalie a necessidade de ajustes e melhorias;
- Atenção às publicações das resoluções da ANPD: por se tratar de uma lei relativamente nova, vários aspectos procedimentais serão tratados através de resoluções, portanto, manter-se atualizado é fundamental;
- Atendimento aos titulares de dados;
- Continuidade das medidas adotadas no projeto de adequação.

Dentre as etapas do plano de gestão constante, algumas merecem destaque, vejamos:

15.1. Atendimento aos titulares de dados.

O artigo 18 da Lei Geral de Proteção de Dados dispõe sobre o direito dos titulares de dados que deverão ser atendidos.

Art. 18. O titular dos dados pessoais tem o direito de obter do controlador, em relação aos dados do titular por ele tratado, a qualquer momento e mediante requisição:

I	confirmação da existência de tratamento;
II	acesso aos dados;
III	correção de dados incompletos, inexatos ou desatualizados;
IV	anonimização, bloqueio ou eliminação de dados necessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V	portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observação dos segredos comerciais e industriais, de acordo com a regulamentação do órgão controlador;
VI	eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII	informação das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados;
VIII	informação sobre a possibilidade de não consentimento e sobre as consequências da negativa;
IX	revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

A Lei Geral de Proteção de Dados prevê que as empresas/escritórios de advocacia devem disponibilizar aos titulares de dados canais de comunicação claros e acessíveis para o exercício de seus direitos. Isso significa que as empresas devem informar aos titulares de dados quais são seus direitos e como eles podem exercê-los, além de garantir que essas solicitações sejam atendidas de forma eficiente e eficaz.

Se o escritório de advocacia possui site, o atendimento aos titulares de dados pode ser realizado por meio de diversos canais de comunicação disponibilizados na página, tais como e-mail ou formulário de contato.

O escritório deve disponibilizar no site informações específicas sobre os dados pessoais que coleta, a finalidade do tratamento desses dados, a base legal, os direitos dos titulares de dados e como eles podem exercê-los. O site do escritório também deve possuir uma Aviso de Privacidade objetiva e acessível, que especifique quais dados são coletados, como são tratados, com quem são compartilhados e quais medidas de segurança são adotadas para protegê-los.

No que diz respeito ao atendimento aos titulares de dados, o escritório deve garantir que todas as requisições recebidas sejam respondidas de forma eficiente e no prazo determinado (15 dias), seguindo as diretrizes da Lei Geral de Proteção de Dados.

Para isso, é recomendado que o escritório tenha um profissional responsável pela gestão e proteção de dados, que esteja apto a responder aos questionamentos dos titulares de dados e garantir o cumprimento das obrigações previstas na LGPD.

O atendimento aos titulares de dados é um requisito fundamental da conformidade com a LGPD e pode impactar diretamente a confiança do escritório junto aos seus clientes. Por isso, é essencial que o escritório leve essa questão a sério e adote as medidas necessárias para garantir um atendimento transparente, ágil e eficaz.

15.2. Continuidade das medidas adotadas no projeto de adequação

Para garantir a continuidade do projeto de continuidade à LGPD, é importante adotar algumas medidas fundamentais. Dentre várias, podemos destacar:

- Capacitar os funcionários/estagiários: todos os funcionários e estagiários do escritório devem ser capacitados para que possam compreender a importância da proteção de dados pessoais e saber como agir para garantir a conformidade com a lei;
- Monitorar e revisar o plano de ação: monitorar regularmente as medidas adotadas durante o projeto de adequação, a fim de garantir que as determinações do projeto sejam atendidas. Além disso, o plano de ação deve ser examinado periodicamente para que se possa identificar novos riscos e fazer ajustes necessários;
- Realizar auditorias internas: o escritório pode se beneficiar da realização de auditorias internas para verificar a evolução das medidas adotadas para seguir a LGPD e garantir a conformidade contínua com as obrigações legais;
- Acompanhamento das jurisprudências: a LGPD é uma lei recente e ainda está em fase de adaptação e interpretação pelos tribunais brasileiros. É importante acompanhar de perto as decisões judiciais relacionadas à LGPD e estar atento às possíveis mudanças nas interpretações e exigências legais.

Essas medidas são fundamentais para garantir a continuidade do projeto e para proteger os dados pessoais dos titulares, garantindo assim, o cumprimento legal.

16. CONCLUSÃO

A Lei Geral de Proteção de Dados é uma lei que afeta a todos e acreditamos que todas as informações contidas neste material são um passo importante rumo ao melhor desenvolvimento da advocacia em tempos de profunda digitalização da vida humana.

A Primeira Comissão de Proteção de Dados da OAB/RJ – Leopoldina tem por objetivo disseminar a cultura de proteção de dados de maneira a avançarmos na construção dessa nova realidade que se apresenta à advocacia.

Menos dados, mais transparência, e vamos juntos propagar a cultura de proteção de dados pessoais!

REFERÊNCIAS

BRASIL, Constituição da República Federativa do Brasil de 1988. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.ht m. BRASIL, Decreto-Lei 5.452, de 1° de maio de 1943. Aprova a Consolidação das Leis do Trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm.

Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

Fluxograma de Petição do titular disponibizada no site da ANPD (https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/peticao-de-titular-contra-controlador-de-dados)

Resolução CD/ANPD nº 02 – Publicada em 27 de janeiro de 2023 https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD – Lei Geral de Proteção de Dados Pessoais Comentada. 4º Edição. Ed. Revista dos Tribunais, 2022.

GUIA DA LGPD APLICADO A ESCRITÓRIOS DE ADVOCACIA – OAB Campinas. 2021. Disponível em: https://oabcampinas.org.br/wp-content/uploads/2021/12/Guia-LGPD_Advocacia.pdf

GUARIENTO, Daniel Bittencour; e MARTINS, Ricardo Maffeis. Qual o papel dos advogados enquanto agentes de tratamento de dados: controladores ou operadores? 2020. Disponível em: <https://www.migalhas.com.br/coluna/impressoes-digitais/336001/qual-o-papel-dos-advogados-enquanto-agentes-de-tratamento-de-dados--controladores-ou-operadores>

COMISSÃO DE INOVAÇÃO, TECNOLOGIA E PROTEÇÃO DE DADOS – OAB ALAGOAS. Cartilha Lei Geral de Proteção de Dados para Escritórios de Advocacia. Disponível em: https://www.oab-al.org.br/app/uploads/2023/09/pdf_20220923_195050_0000.pdf

NICODEMOS, Renata. Desafios e impactos da LGPD na rotina dos escritórios de advocacia. 2022. Disponível em: <https://analise.com/opiniao/desafios-e-impactos-da-lgpd-na-rotina-dos-escritorios-de-advocacia>

LEI GERAL DE PROTEÇÃO DE DADOS

– Infográficos de fixação –

Material elaborado por:
Fernanda Aparecida Pina Sanan.
Isabela Coelho da Matta Cardoso.
Juliane Rocha Naegele.
Larissa Alves Carneiro.

LEI GERAL DE PROTEÇÃO DE DADOS

– Lei nº 13.709/2018 (regras para o tratamento de dados (físico ou digital).
– Constituição Federal – EC nº 115, art. 5º, LXXIX (direito fundamental).

APLICAÇÃO DA LEI

Pessoa Física.

Qualquer operação de tratamento.

Pessoa Jurídica.

APLICAÇÃO. TERRITORIAL

- Lei nº 13.709/2018, art.3º, I.

Dados tratados em território nacional.

EXCEÇÕES

art.4º, I, II, III e IV.

1. Fins particulares não econômicos;

2. Segurança pública, defesa nacional, segurança do estado ou atividades de investigação e repressão penal;

3. Fins jornalísticos, artísticos e acadêmicos;

4. Provenientes de fora do território nacional.

DADOS

Dado Pessoal

Informação relacionada a pessoa física que a identifique ou possa identificá-la; (art. 5º, I).

Dado Sensível

Origem racial, étnica, religião, opinião política, filiação sindical, organização de caráter religioso, político ou filosófico, dado de saúde, vida sexual, genético ou biométrico (art. 5º, II);

Dado Anonimizado

Não pode ser identificado; (art.5º, III);

Dado Pseudonimizado

Técnica que impossibilita a associação direta ou indireta a um indivíduo (precisa de informação adicional mantida em segurança para identificação.

Tratamento de Dados

Toda operação realizada com os dados pessoais (art. 5º , X);

SUJEITOS DA LGPD

Titular de Dados

- ✓ Pessoa Física
- ✓ Art. 5º, V

Controlador

- ✓ Pessoa Física ou Pessoa Jurídica
- ✓ Decide como os dados serão tratados
- ✓ Art. 5º, VI

Operador

- ✓ Pessoa Física ou Pessoa Jurídica
- ✓ Realiza o tratamento em nome do controlador
- ✓ Art. 5º, VII

Encarregado de Dados – DPO

- ✓ Pessoa indicada pelo controlador
- ✓ Atua como canal de comunicação entre os titulares e a ANPD
- ✓ Art. 5º, VIII

ANPD

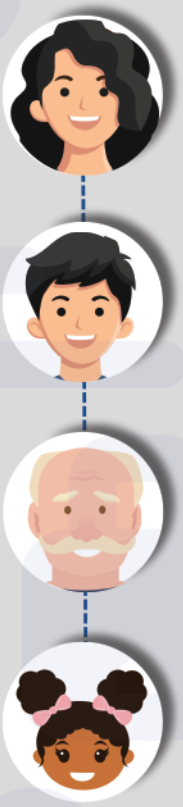
– Autoridade Nacional de Proteção de Dados.
– Natureza regulatória, fiscalizatória e sancionatória;

PRINCÍPIOS

Lei nº 13.709/2018.
Art. 06.

DIREITO DOS TITULARES

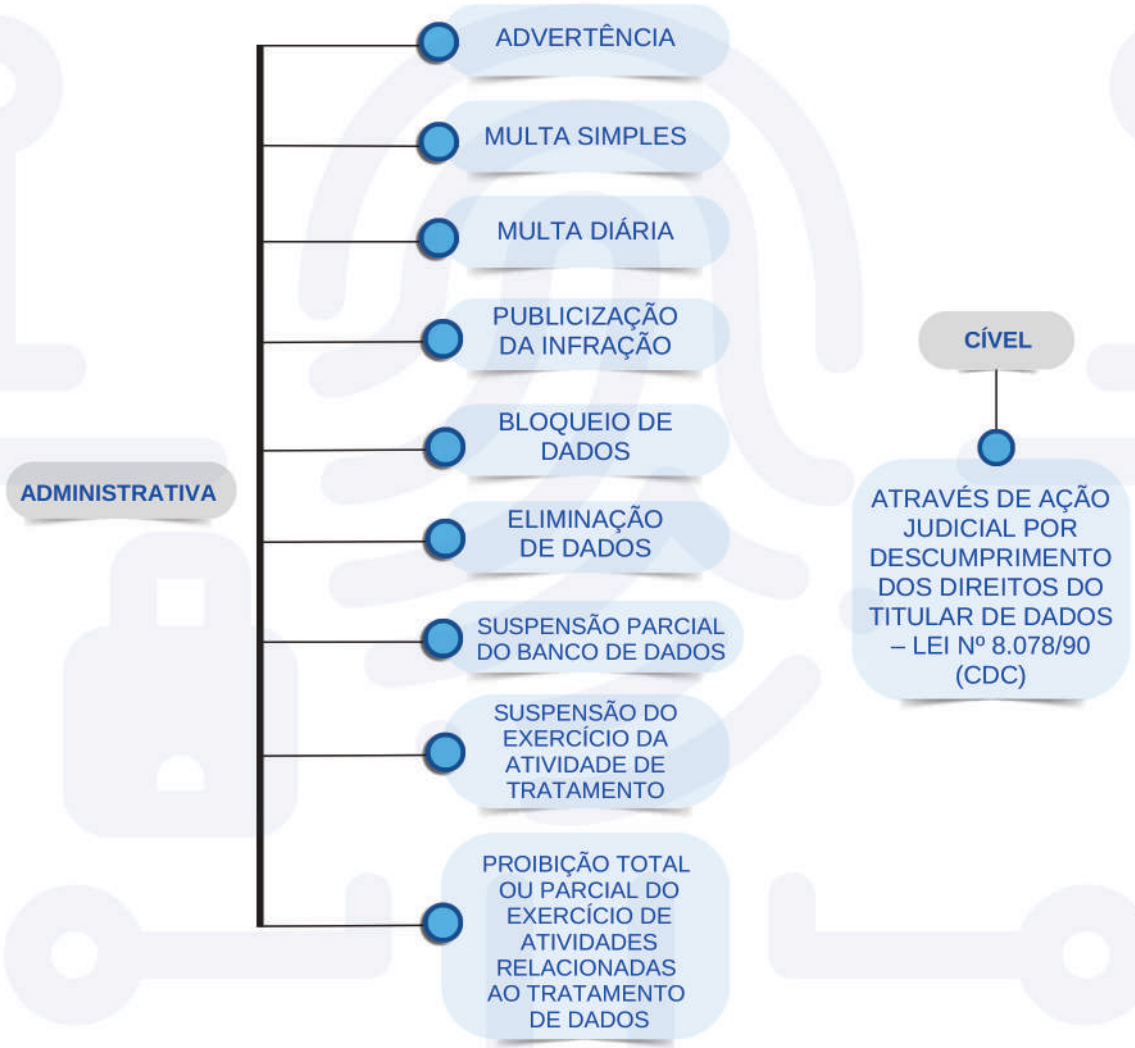
Lei nº 13.709/2018.
Art. 18.



- ✓ Confirmação da existência do tratamento
- ✓ Acesso aos dados
- ✓ Correção dos dados incompletos, inexatos ou desatualizados
- ✓ Anonimização, bloqueio ou eliminação dos dados desnecessários
- ✓ Portabilidade dos dados a outro fornecedor de serviço ou produto
- ✓ Revogação do consentimento
- ✓ Informações sobre compartilhamento de dados e a finalidade
- ✓ Informação sobre a possibilidade de não fornecer consentimento e as consequências da negativa
- ✓ O responsável deverá fornecer critérios da decisão automatizada, já que os dados pessoais não podem ser usados em prejuízo do titular
- ✓ A defesa dos interesses do titular poderá ser exercida em juízo, individual ou coletivamente

SANÇÕES

Lei nº 13.709/2018.
Art. 52.



ENTENDA AS FASES DO PROJETO DE ADEQUAÇÃO (SUGESTÃO)

ETAPAS

01

- Reunião Kick off.
- Nomeação DPO.
- Conscientização.

02

- Mapeamento (planilha).
- Quais áreas devem ser mapeadas? (levantamento de dados por setores diversos, classificação dos dados, finalidade, base legal, prazo de retenção).
- Análise de Contratos.
- Análise de site e redes sociais.

03

- Gap analysis (identificar pontos de tratamento vulnerável).
- Quais os problemas foram identificados?

04

- Planejamento.
- Estabelecer ordem de prioridade com maior risco.

05

- Implementação (produção de documentos).
- Ato da elaboração de documentos.
- Aditivos Contratuais (para terceirizados e colaboradores).
- Política de Privacidade.
- Código de conduta.
- Política de segurança da informação.
- Aviso de privacidade (site).
- Aviso e política de cookies (site).
- Termos de uso (site).

06

- Monitoramento (constante) - através do Encarregado de Dados.
- Atendimento aos titulares – através do Encarregado de Dados.

A LEI GERAL DE PROTEÇÃO DE DADOS

NOS ESCRITÓRIOS DE ADVOCACIA

O Guia Orientativo – A Lei Geral de Proteção de Dados nos escritórios de advocacia, idealizado com dedicação pela 1ª Comissão de Proteção de Dados e Privacidade da 58ª OAB/RJ – Leopoldina, se destina a ser o norte para os advogados que buscam compreender e aplicar a Lei Geral de Proteção de Dados em sua prática jurídica. Um trabalho minucioso, realizado com profundo carinho por profissionais dedicadas a disseminar a cultura de proteção de dados e que possuem uma missão clara: oferecer ajuda e direcionamento à classe dos advogados em meio ao complexo cenário da LGPD.

Este guia é uma ferramenta essencial, abrangendo desde os conceitos fundamentais até a aplicação prática da lei. Com clareza e abordagem prática, estamos comprometidas em capacitar os profissionais do direito a enfrentarem questões de privacidade e proteção de dados, garantindo que possam representar seus clientes de forma eficaz e ética nessa era digital.

O conhecimento é a chave, e este guia é o seu companheiro confiável nessa jornada!

ISBN: 978-85-5963-168-5

priint impressõesinteligentes