

POLÍTICA INTERNA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

INTRODUÇÃO

O Flávio Lopes Advogados Associados ("Escritório") reconhece a privacidade e a proteção de dados pessoais como elementos fundamentais para o exercício responsável de suas atividades jurídicas e administrativas, pautando sua atuação pela ética, transparência, confidencialidade, segurança da informação e respeito aos direitos dos titulares.

Por meio desta Política Interna de Privacidade e Proteção de Dados Pessoais, o Escritório estabelece seu compromisso institucional com a adoção de práticas de governança e medidas de proteção compatíveis com a natureza de suas operações, observando as disposições da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), a regulamentação da Agência Nacional de Proteção de Dados (ANPD) e os deveres legais, éticos e profissionais inerentes à advocacia.

Esta Política integra as diretrizes institucionais do Escritório e deverá ser observada em conjunto com os demais instrumentos de governança, integridade, privacidade e segurança da informação aplicáveis, conforme sejam aprovados e efetivamente implementados.

A referência a instrumentos complementares não constitui, isoladamente, comprovação de sua existência ou implementação, cuja efetividade deverá ser demonstrada por registros e evidências pertinentes.

I – CONTEXTO E OBJETIVO

O tratamento de dados pessoais está diretamente relacionado às atividades desenvolvidas pelo Flávio Lopes Advogados Associados, abrangendo o relacionamento com clientes, a condução de processos judiciais e extrajudiciais, as atividades de recuperação de crédito, a gestão administrativa e de

profissionais, bem como a contratação e o relacionamento com fornecedores e parceiros.

Nesse contexto, o Escritório poderá tratar informações pessoais de clientes, colaboradores, candidatos, representantes, devedores, credores, partes

processuais e demais pessoas envolvidas nas atividades jurídicas e administrativas, incluindo, quando necessário e legalmente permitido, dados pessoais sensíveis e informações protegidas pelo sigilo profissional.

Esta Política tem como objetivo estabelecer diretrizes, responsabilidades e procedimentos para orientar o tratamento adequado de dados pessoais no âmbito do Escritório, especialmente quanto à coleta, utilização, acesso, armazenamento, compartilhamento, conservação e eliminação dessas informações.

Busca, ainda, promover uma cultura de privacidade e proteção de dados pessoais, orientando os profissionais quanto à adoção de práticas preventivas, à utilização responsável das informações e à identificação e mitigação de riscos associados às atividades de tratamento.

As disposições desta Política aplicam-se aos sócios, advogados, empregados, estagiários e demais profissionais que atuem em nome do Escritório, bem como aos terceiros que tenham acesso a dados pessoais em razão de suas atividades, observadas as responsabilidades e obrigações aplicáveis a cada relação.

Este documento possui natureza interna e não substitui o Aviso de Privacidade destinado aos titulares de dados pessoais, instrumento por meio do qual serão disponibilizadas informações sobre as operações de tratamento realizadas pelo Escritório, nos termos da legislação aplicável.

II – ABRANGÊNCIA OPERACIONAL E APLICAÇÃO

Esta Política abrange as operações de tratamento de dados pessoais realizadas no âmbito das atividades jurídicas, administrativas e institucionais do Flávio Lopes Advogados Associados ("Escritório"), independentemente do meio, formato ou ambiente em que as informações sejam coletadas, consultadas, utilizadas, armazenadas, compartilhadas ou eliminadas.

Suas disposições aplicam-se aos sócios, advogados associados, empregados, estagiários e demais profissionais que atuem em nome do Escritório, incluindo correspondentes jurídicos, fornecedores e prestadores de serviços que tenham

acesso a dados pessoais em razão de suas atividades, observados os respectivos vínculos, contratos e responsabilidades.

2.1. Abrangência das Atividades e Ambientes de Tratamento

As diretrizes desta Política aplicam-se aos dados pessoais tratados em processos judiciais e extrajudiciais, contratos, procurações, documentos físicos, arquivos eletrônicos, sistemas de gestão jurídica, plataformas processuais, correio eletrônico, ferramentas de comunicação e colaboração, dispositivos e demais ambientes tecnológicos utilizados pelo Escritório.

Sua aplicação compreende também as atividades realizadas fora das dependências físicas do Escritório, incluindo trabalho remoto, diligências externas e atuação de correspondentes jurídicos, observadas as condições pertinentes de acesso, confidencialidade, segurança da informação e sigilo profissional.

2.2. Categorias de Dados Pessoais Tratados

No desenvolvimento de suas atividades jurídicas, administrativas e institucionais, o Escritório poderá tratar dados pessoais de clientes, colaboradores, candidatos, representantes, devedores, credores, partes processuais, fornecedores e demais pessoas relacionadas às operações realizadas.

As informações tratadas poderão compreender dados cadastrais e de identificação, informações de contato, dados financeiros e patrimoniais, informações profissionais, familiares, contratuais e processuais, bem como outras categorias pertinentes às finalidades legítimas das atividades desenvolvidas.

Quando necessário e legalmente permitido, o tratamento poderá envolver dados pessoais sensíveis e informações protegidas pelo sigilo profissional, observadas as hipóteses legais aplicáveis e as medidas de proteção adequadas.

O detalhamento das categorias de dados pessoais, das respectivas finalidades, das fontes de coleta, das hipóteses legais, dos compartilhamentos e dos demais elementos pertinentes deverá constar do **Registro de Operações de Tratamento de Dados Pessoais (ROPA)** e, quando adotado como instrumento complementar, do **Inventário de Dados Pessoais**.

Esses registros deverão refletir as operações efetivamente realizadas pelo Escritório e ser atualizados sempre que ocorrerem alterações relevantes nos processos, sistemas ou atividades de tratamento.

2.3. Fontes de Coleta e Obtenção de Dados Pessoais

Os dados pessoais poderão ser obtidos diretamente dos titulares, de clientes, representantes, partes envolvidas nas demandas jurídicas, correspondentes, fornecedores e demais terceiros legitimamente relacionados às atividades do Escritório.

Também poderão ser utilizados dados provenientes de processos judiciais, documentos públicos, bases cadastrais e outras fontes legitimamente acessíveis, desde que sua coleta e utilização estejam vinculadas a finalidades determinadas e fundamentadas nas hipóteses legais aplicáveis.

A disponibilidade pública de determinada informação não afasta a necessidade de observância dos princípios e das demais disposições da LGPD, especialmente quanto à finalidade, adequação e necessidade do tratamento.

As fontes de obtenção de dados pessoais deverão ser identificadas e documentadas nos registros das operações de tratamento, conforme aplicável, permitindo a rastreabilidade das informações e a avaliação de sua adequação às finalidades estabelecidas.

2.4. Tratamento de Dados Pessoais Sensíveis

No exercício de suas atividades, o Escritório poderá tratar dados pessoais sensíveis, especialmente quando presentes em documentos processuais, demandas trabalhistas, informações de saúde ocupacional ou outras situações relacionadas à prestação de serviços jurídicos e à gestão de profissionais.

O tratamento dessas informações deverá estar fundamentado em uma das hipóteses legais previstas no art. 11 da LGPD, conforme a natureza da operação, incluindo, quando aplicável, o cumprimento de obrigação legal ou regulatória, o exercício regular de direitos em processos judiciais, administrativos ou arbitrais e o consentimento específico e destacado do titular, quando essa for a base legal adequada.

Deverão ser adotadas medidas de proteção proporcionais à natureza das informações e aos riscos envolvidos, incluindo restrições de acesso, deveres de confidencialidade, mecanismos de segurança da informação e observância do sigilo profissional.

O Escritório não realiza, como prática institucional, a coleta deliberada de dados pessoais sensíveis por meio de seu site. Eventuais informações dessa natureza recebidas espontaneamente por canais eletrônicos deverão ser avaliadas quanto à necessidade, à finalidade e à existência de fundamento legal para seu tratamento, com adoção das providências cabíveis.

O envio voluntário de dados pessoais sensíveis pelo titular não dispensa a identificação da hipótese legal aplicável nem autoriza sua utilização para finalidades incompatíveis com aquelas legitimamente estabelecidas.

As operações que envolvam dados pessoais sensíveis deverão ser identificadas nos registros de tratamento pertinentes, permitindo a avaliação dos riscos associados e a definição de medidas de proteção compatíveis com sua natureza e criticidade.

III – GLOSSÁRIO

Para facilitar a compreensão e a aplicação desta Política, são apresentados a seguir os principais conceitos relacionados à proteção de dados pessoais, acompanhados de exemplos pertinentes às atividades desenvolvidas pelo Flávio Lopes Advogados Associados.

As definições previstas na legislação aplicável prevalecerão sobre os exemplos apresentados, que possuem caráter exclusivamente ilustrativo.

Termo	Significado e aplicação no Escritório
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável, como nome, CPF, endereço ou contato de cliente ou devedor.
Dado pessoal sensível	Dado sobre saúde, origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, vida sexual, dado genético ou biométrico vinculado a pessoa; pode constar de autos ou documentos trabalhistas.
Titular	Pessoa natural a quem se referem os dados, incluindo clientes, empregados, candidatos, devedores, credores e partes de processos.
Tratamento	Qualquer operação com dados pessoais, como coletar, consultar, classificar, armazenar, compartilhar, atualizar ou eliminar documentos e cadastros.
Controlador	Agente que decide as finalidades e os elementos essenciais do tratamento; por exemplo, o Escritório ao administrar seus colaboradores.
Operador	Agente que trata dados em nome de um controlador, conforme as instruções legítimas recebidas. A qualificação depende da atividade concreta.
Encarregado	Pessoa indicada para atuar como canal de comunicação entre controlador, titulares e ANPD, quando aplicável; não se confunde automaticamente com o responsável operacional interno.

ANPD	Agência Nacional de Proteção de Dados, autoridade responsável pela regulação e fiscalização da proteção de dados pessoais no Brasil.
Base legal	Hipótese autorizadora prevista na LGPD para cada finalidade, como obrigação legal, exercício regular de direitos ou execução de contrato, conforme o caso.
Consentimento	Manifestação livre, informada e inequívoca para finalidade determinada; não constitui fundamento obrigatório ou universal dos serviços jurídicos.
Anonimização	Processo pelo qual o dado deixa de ser associado a pessoa identificável com meios técnicos razoáveis e disponíveis; ocultar o nome nem sempre basta.
Compartilhamento	Disponibilização ou comunicação de dados a outra parte, como cartório, correspondente ou prestador de tecnologia, quando legitimamente necessária.
Suboperador	Terceiro contratado por operador para auxiliá-lo no tratamento em nome de controlador, sujeito à análise da cadeia contratual.
Transferência internacional	Transferência de dados pessoais para país estrangeiro ou organismo internacional, inclusive por determinados serviços tecnológicos.
Incidente de segurança	Ocorrência confirmada que comprometa confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais; suspeitas também devem ser reportadas para avaliação.
ROPA	Registro das operações de tratamento de dados pessoais, com finalidades, categorias de dados, agentes, compartilhamentos e demais informações pertinentes.
RIPD	Relatório de Impacto à Proteção de Dados Pessoais, elaborado quando cabível para avaliar riscos aos direitos e liberdades dos titulares e medidas de mitigação.
LIA	Avaliação documentada sobre a adequação do legítimo interesse como base legal, considerando finalidade, necessidade, expectativas dos titulares e salvaguardas.
Privacidade desde a concepção e por padrão	Incorporação de proteção de dados no planejamento de novos fluxos e limitação inicial de coleta, uso e acesso ao necessário.

IV – PAPÉIS NO TRATAMENTO DE DADOS PESSOAIS

O Flávio Lopes Advogados Associados poderá atuar como **controlador ou operador de dados pessoais**, conforme a natureza das atividades desenvolvidas, as finalidades do tratamento e o grau de autonomia na definição dos elementos essenciais de cada operação, observadas as disposições da Lei nº

13.709/2018 (LGPD), os instrumentos contratuais aplicáveis e as particularidades inerentes ao exercício da advocacia.

A identificação desses papéis deverá considerar as decisões efetivamente tomadas pelo Escritório em cada atividade de tratamento, não se limitando à denominação atribuída às partes nos respectivos instrumentos contratuais.

4.1. Atuação como Controlador de Dados Pessoais

O Escritório atuará na condição de **controlador** quando determinar as finalidades e os elementos essenciais do tratamento de dados pessoais, especialmente nas atividades relacionadas a:

- a) Gestão de empregados, estagiários, candidatos e demais profissionais vinculados ao Escritório;
- b) Cadastro, relacionamento e administração de clientes, fornecedores, prestadores de serviços e correspondentes jurídicos;
- c) Gestão administrativa, financeira, contábil, fiscal e contratual;
- d) Relacionamento institucional e comercial, incluindo a administração do site institucional e das redes sociais;
- e) Gestão dos canais de comunicação, integridade, privacidade e segurança da informação;
- f) Execução de atividades jurídicas nas quais o Escritório determine, de forma autônoma, as finalidades e os elementos essenciais do tratamento, observados os deveres legais, éticos e profissionais aplicáveis.

4.2. Atuação como Operador de Dados Pessoais

O Escritório atuará na condição de **operador** quando realizar operações de tratamento de dados pessoais em nome de um cliente que atue como controlador, observando suas instruções legítimas e documentadas, os limites estabelecidos na relação contratual e as obrigações legais aplicáveis.

Essa condição poderá ocorrer, por exemplo, em atividades de apoio operacional, tratamento de bases cadastrais, organização de informações ou execução de procedimentos relacionados à prestação dos serviços contratados, desde que o Escritório não determine autonomamente as finalidades e os elementos essenciais do respectivo tratamento.

A atuação como operador não afasta a independência técnica, o sigilo profissional e as demais prerrogativas e obrigações inerentes ao exercício da advocacia, nos termos da Lei nº 8.906/1994 (Estatuto da Advocacia e da OAB).

4.3. Identificação e Registro das Responsabilidades

A definição do papel desempenhado pelo Escritório deverá considerar as características concretas de cada atividade de tratamento, especialmente as finalidades envolvidas, as decisões efetivamente tomadas, os fluxos de dados pessoais e as responsabilidades atribuídas às partes.

As disposições contratuais deverão ser consideradas nessa avaliação, sem prejuízo da análise da realidade operacional, uma vez que a simples qualificação contratual das partes não determina, isoladamente, sua condição de controlador ou operador perante a LGPD.

O enquadramento identificado deverá ser documentado no **Registro de Operações de Tratamento de Dados Pessoais (ROPA)**, permitindo a rastreabilidade das atividades e a adequada definição das responsabilidades.

Nas operações em que atuar como operador, o Escritório deverá observar as instruções legítimas do controlador e assegurar que a contratação de eventuais suboperadores respeite as condições legais e contratuais aplicáveis, incluindo, quando exigida, a autorização do cliente e a adoção de medidas adequadas de confidencialidade e segurança da informação.

V – PRINCÍPIOS

As operações observarão finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização. Na prática, devem ser evitados, entre outros, o envio de peças ao destinatário errado, o acesso a carteiras de clientes sem necessidade e o uso de dados de um processo para finalidade não autorizada.

VI – HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS

Cada finalidade de tratamento deverá ter base legal identificada e documentada no ROPA, conforme os arts. 7º e 11 da LGPD. O consentimento não será presumido como base geral da advocacia; exercício regular de direitos, obrigação legal, execução contratual, proteção do crédito e legítimo interesse serão avaliados conforme o contexto, os titulares envolvidos e os limites legais.

O uso de legítimo interesse, inclusive para localização e atualização de contatos, dependerá de avaliação específica de finalidade, necessidade, expectativas dos titulares, impactos e salvaguardas, com registro da conclusão quando aplicável. A hipótese não poderá fundamentar tratamento de dados sensíveis.

VII – FORMAS DE COLETA

- **Site institucional:** coleta de dados em formulários e tecnologias de navegação efetivamente utilizadas, conforme inventário técnico e Aviso de Privacidade. Cookies não essenciais, quando existentes, deverão ter fundamento e mecanismo de escolha adequados. Prazos de retenção de registros de acesso serão definidos segundo o papel do provedor, o serviço prestado e a legislação aplicável; não se presume obrigação geral de seis meses ao Escritório.
- **E-mail e ferramentas de comunicação e colaboração** (como Outlook, Teams, SharePoint e Gmail): acesso a dados pessoais informados pelo Titular nas mensagens e arquivos trocados.
- **Documentos físicos:** contratos, procurações, currículos, petições, cópias de autos, entre outros.
- **Fontes de terceiros e públicas:** sistemas eletrônicos de processos judiciais, diários oficiais, bases da Receita Federal, bureaus e bases cadastrais de fornecedores especializados, desde que a lei o permita e para finalidades específicas.
- **Redes sociais:** informações fornecidas pelo Titular em contato por perfis do Escritório.

VIII – COMPARTILHAMENTO COM TERCEIROS E SUBOPERADORES

O Flávio Lopes Advogados Associados poderá realizar o compartilhamento de dados pessoais com terceiros quando necessário ao desenvolvimento de suas atividades jurídicas, administrativas e institucionais, desde que observadas as finalidades legítimas do tratamento, as hipóteses legais aplicáveis, as obrigações contratuais e os deveres de confidencialidade e sigilo profissional inerentes à advocacia.

O compartilhamento deverá observar os princípios da finalidade, adequação, necessidade, segurança e prevenção, restringindo-se às informações pertinentes e proporcionais à finalidade pretendida.

8.1. Compartilhamento de Dados Pessoais

O compartilhamento de dados pessoais poderá ocorrer, conforme a natureza da atividade e as obrigações legais e contratuais aplicáveis, com clientes, órgãos do Poder Judiciário, autoridades públicas, cartórios, correspondentes jurídicos, prestadores de serviços tecnológicos e outros destinatários necessários à execução das atividades do Escritório.

As informações compartilhadas deverão limitar-se ao necessário para o cumprimento da finalidade específica, observadas as condições de segurança, confidencialidade e proteção de dados pessoais pertinentes.

8.2. Gestão de Terceiros e Suboperadores

O Escritório deverá manter inventário dos fornecedores, prestadores de serviços e demais terceiros que tenham acesso a dados pessoais em razão das atividades contratadas, contemplando, conforme aplicável, a identificação dos serviços prestados, as categorias de dados tratados, os papéis e responsabilidades das partes, os ambientes de armazenamento e as medidas de proteção adotadas.

A contratação de terceiros que realizem operações de tratamento de dados pessoais deverá considerar os riscos envolvidos, a natureza das informações acessadas e as obrigações legais e contratuais pertinentes.

Quando o Escritório atuar na condição de operador, a contratação de eventuais suboperadores deverá observar as instruções legítimas do controlador e as condições estabelecidas nos respectivos instrumentos contratuais, incluindo a necessidade de autorização prévia, quando aplicável.

O acesso de correspondentes jurídicos, parceiros e prestadores de serviços deverá ser limitado às informações necessárias à execução de suas atividades, observados os deveres de confidencialidade, sigilo profissional e segurança da informação.

8.3. Rankings e Publicações Especializadas

O Escritório poderá participar de rankings jurídicos, diretórios profissionais, pesquisas de mercado e publicações especializadas destinadas à avaliação, ao reconhecimento e à divulgação institucional de sua atuação.

Nessas situações, o eventual compartilhamento de informações relacionadas a clientes, representantes ou contatos profissionais deverá observar as finalidades específicas da divulgação, as hipóteses legais aplicáveis, os compromissos de confidencialidade e, especialmente, os deveres éticos e de sigilo profissional inerentes à advocacia.

A identificação de clientes como referências profissionais, bem como o compartilhamento de seus dados de contato com instituições responsáveis por rankings e publicações especializadas, dependerá de **autorização prévia e específica do cliente**, observadas as demais condições legais e profissionais aplicáveis.

Sempre que possível e compatível com a finalidade pretendida, deverão ser

priorizadas informações agregadas ou anonimizadas, evitando-se a divulgação desnecessária de dados pessoais, informações processuais ou conteúdos protegidos pelo sigilo profissional.

8.4. Diretrizes Gerais de Compartilhamento

O Escritório não comercializa dados pessoais e não realiza compartilhamentos para finalidades incompatíveis com aquelas que justificaram sua coleta ou utilização, salvo quando houver fundamento legal adequado para o novo tratamento.

Todo compartilhamento deverá observar as responsabilidades do Escritório enquanto controlador ou operador, conforme a natureza da atividade, e ser realizado de forma proporcional, segura e compatível com as obrigações legais, contratuais e profissionais aplicáveis.

IX – TRANSFERÊNCIA INTERNACIONAL

Antes de contratar ou utilizar serviço que permita transferência internacional de dados, inclusive acesso remoto por fornecedor localizado no exterior, o Escritório verificará a existência do fluxo, os países envolvidos, a hipótese legal aplicável e o mecanismo previsto na regulamentação da ANPD. Restrições contratuais dos clientes deverão ser respeitadas e documentadas.

X – DIREITOS DOS TITULARES E CANAL DE ATENDIMENTO

O Flávio Lopes Advogados Associados assegurará, quando atuar na condição de controlador de dados pessoais, o atendimento aos direitos dos titulares previstos na Lei nº 13.709/2018 (LGPD), especialmente em seus arts. 18 e 20, observadas as condições e limitações legais aplicáveis, as particularidades das atividades jurídicas desenvolvidas e os deveres de confidencialidade e sigilo profissional inerentes à advocacia.

Entre os direitos assegurados aos titulares, destacam-se a confirmação da existência de tratamento, o acesso aos dados pessoais, a correção de informações incompletas, inexatas ou desatualizadas, a anonimização, o bloqueio ou a eliminação de dados nas hipóteses legalmente previstas, a obtenção de informações sobre compartilhamentos, a oposição ao tratamento irregular, a revogação do consentimento, quando aplicável, e a solicitação de revisão de decisões tomadas unicamente com base em tratamento automatizado, observadas as disposições legais pertinentes.

10.1. Canal de Privacidade

O Escritório disponibiliza o endereço eletrônico privacidade@flaviolopes.adv.br como canal institucional de comunicação com o Encarregado pelo Tratamento de Dados Pessoais, **Leonardo Cantalino**, destinado ao recebimento de solicitações, dúvidas e manifestações relacionadas à privacidade, à proteção de dados pessoais e ao exercício dos direitos dos titulares.

As informações referentes ao Encarregado e ao respectivo canal de contato deverão constar do Aviso de Privacidade e ser divulgadas nos meios institucionais do Escritório, de modo a assegurar transparência e facilitar a comunicação com os titulares de dados pessoais.

10.2. Procedimentos e Prazos Internos de Atendimento

As solicitações recebidas pelo Canal de Privacidade serão registradas em controle próprio, contendo, quando aplicável, a data de recebimento, a identificação do solicitante, o direito exercido, o responsável pelo atendimento, as providências adotadas e a data de conclusão.

Para assegurar a adequada gestão das solicitações, o Escritório adotará os seguintes procedimentos e prazos internos:

a) Registro da solicitação: realizado a partir do recebimento do pedido, para fins de acompanhamento e rastreabilidade;

b) Verificação de identidade: realizada mediante procedimentos proporcionais e seguros, limitados às informações necessárias à identificação do requerente e à prevenção de acessos indevidos;

c) Confirmação de recebimento: encaminhada ao solicitante em até **2 (dois) dias úteis**, como prazo interno de atendimento administrativo;

d) Encaminhamento ao controlador: quando o Escritório atuar como operador, a solicitação será encaminhada ao respectivo controlador, preferencialmente em até **2 (dois) dias úteis**, observados os prazos e procedimentos contratuais aplicáveis;

e) Análise e tratamento da solicitação: realizados pelo Encarregado, com apoio das áreas responsáveis, considerando a natureza do pedido, a finalidade do tratamento, a base legal aplicável e eventuais restrições legais ou profissionais;

f) Registro da conclusão: as providências adotadas, as respostas encaminhadas e as eventuais justificativas de impossibilidade de atendimento serão documentadas em controle próprio.

Os prazos internos estabelecidos neste item possuem natureza exclusivamente operacional e destinam-se à organização das atividades do Escritório, **não substituindo, ampliando ou afastando os prazos legais e regulamentares aplicáveis.**

10.3. Prazos Legais e Regulamentares

O atendimento às solicitações dos titulares observará os prazos previstos na LGPD e na regulamentação expedida pela Agência Nacional de Proteção de Dados (ANPD), conforme a natureza do direito exercido e as características da operação de tratamento.

Em relação aos pedidos de confirmação da existência de tratamento e de acesso aos dados pessoais, serão observadas as disposições do art. 19 da LGPD, segundo o qual:

a) A confirmação da existência de tratamento ou o acesso aos dados pessoais, em formato simplificado, deverá ser providenciado imediatamente, quando aplicável;

b) A declaração clara e completa deverá ser fornecida no **prazo de até 15 (quinze) dias**, contado da data do requerimento do titular, observados os requisitos legais pertinentes.

Para os demais direitos previstos na LGPD, serão observados os prazos específicos eventualmente estabelecidos pela legislação e pela regulamentação aplicável, sem prejuízo do dever de prestar informações adequadas e de justificar eventual impossibilidade de atendimento.

Quando a solicitação envolver dados tratados pelo Escritório na condição de operador, deverão ser observadas as instruções legítimas do controlador, as responsabilidades contratuais e os prazos aplicáveis à respectiva operação, sem prejuízo da cooperação necessária ao atendimento dos direitos dos titulares.

Eventuais negativas, limitações ou impossibilidades de atendimento deverão ser devidamente fundamentadas e comunicadas ao solicitante, quando cabível, especialmente nas hipóteses relacionadas ao cumprimento de obrigações legais ou regulatórias, ao exercício regular de direitos em processos judiciais, administrativos ou arbitrais e à preservação do sigilo profissional da advocacia.

XI – ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS E GOVERNANÇA

O Flávio Lopes Advogados Associados designa **Leonardo Cantalino, sócio do Escritório**, como Encarregado pelo Tratamento de Dados Pessoais, responsável por atuar como canal de comunicação entre o Escritório, os titulares de dados pessoais e a Agência Nacional de Proteção de Dados (ANPD), observadas as atribuições previstas na Lei nº 13.709/2018 (LGPD) e na regulamentação aplicável.

Compete ao Encarregado, entre outras atribuições, receber e acompanhar solicitações dos titulares, prestar esclarecimentos, orientar os profissionais do Escritório quanto às boas práticas de privacidade e proteção de dados pessoais e apoiar a gestão de questões relacionadas ao cumprimento da legislação.

O canal de privacidade constitui o meio institucional destinado ao recebimento de solicitações, dúvidas e manifestações relacionadas ao tratamento de dados pessoais e ao exercício dos direitos dos titulares, devendo ser divulgado no Aviso de Privacidade e nos demais meios institucionais pertinentes.

A governança de privacidade e proteção de dados pessoais permanecerá sob a responsabilidade dos sócios administradores, com o apoio do Encarregado e dos profissionais envolvidos nas atividades de tratamento, observadas as competências e responsabilidades de cada função.

A designação do Encarregado não afasta as responsabilidades legais do Escritório enquanto agente de tratamento de dados pessoais.

XII – SEGURANÇA DA INFORMAÇÃO

O Flávio Lopes Advogados Associados adotará medidas técnicas e administrativas de segurança da informação adequadas à natureza dos dados pessoais tratados, aos riscos envolvidos e às particularidades das atividades jurídicas desenvolvidas, observados os princípios da necessidade, segurança, prevenção e responsabilização previstos na Lei nº 13.709/2018 (LGPD), bem como os deveres de confidencialidade e sigilo profissional inerentes à advocacia.

As medidas de segurança deverão ser estabelecidas e aprimoradas de forma proporcional ao porte, à estrutura organizacional, aos recursos tecnológicos disponíveis e à criticidade das operações de tratamento realizadas pelo Escritório.

Para tanto, serão observadas as seguintes diretrizes:

a) Controle de acesso: o acesso a sistemas, documentos e informações que contenham dados pessoais deverá ser concedido de acordo com as atribuições e

necessidades profissionais de cada usuário, observando o princípio do menor privilégio. Sempre que aplicável, serão utilizados perfis de acesso individualizados e mecanismos de restrição por cliente, processo ou atividade. As permissões deverão ser revisadas periodicamente, de acordo com os riscos identificados e as características dos sistemas utilizados, bem como atualizadas ou revogadas tempestivamente em situações de desligamento, alteração de função ou encerramento da necessidade de acesso.

b) Autenticação e proteção de credenciais: deverão ser adotadas práticas adequadas de gerenciamento de senhas e proteção das credenciais de acesso, priorizando mecanismos de autenticação em múltiplos fatores (MFA) nos sistemas que disponibilizem essa funcionalidade, especialmente aqueles utilizados para comunicação eletrônica, gestão de processos jurídicos e armazenamento de informações em nuvem. As credenciais de acesso deverão ser pessoais e intransferíveis.

c) Proteção de dispositivos e redes: os equipamentos utilizados para o tratamento de dados pessoais deverão contar com medidas de proteção compatíveis com os riscos envolvidos, incluindo atualização de sistemas e aplicativos, ferramentas de proteção contra códigos maliciosos, bloqueio de tela e, quando tecnicamente viável e necessário, criptografia de dispositivos. O acesso remoto deverá ocorrer por meio de conexões adequadamente protegidas, evitando-se a utilização de redes públicas ou desprotegidas para o tratamento de informações confidenciais.

d) Armazenamento e transmissão de informações: os dados pessoais e documentos relacionados às atividades do Escritório deverão ser armazenados, preferencialmente, em sistemas e ambientes institucionais autorizados, observadas as medidas de segurança disponíveis. O uso de contas pessoais, serviços particulares de armazenamento ou dispositivos removíveis para tratamento de informações profissionais deverá ser evitado e, quando excepcionalmente necessário, submetido à autorização e às orientações de segurança pertinentes. O compartilhamento de documentos deverá ocorrer por canais apropriados, com atenção à identificação dos destinatários e à confidencialidade das informações.

e) Cópias de segurança: o Escritório deverá adotar procedimentos de realização de cópias de segurança das informações relevantes para a continuidade de suas atividades, considerando os recursos tecnológicos disponíveis, a criticidade dos dados e os riscos de perda ou indisponibilidade. A periodicidade dos backups, as condições de armazenamento e os procedimentos

de recuperação deverão ser definidos conforme as necessidades operacionais, observadas as diretrizes de retenção e proteção de dados pessoais.

f) Registro e monitoramento: sempre que os sistemas utilizados disponibilizarem funcionalidades de registro de acessos, alterações ou outras operações relevantes, tais recursos deverão ser considerados como mecanismos de apoio à segurança, à rastreabilidade e à apuração de eventuais incidentes. O monitoramento será realizado de forma proporcional aos riscos e às funcionalidades tecnológicas disponíveis, respeitados os limites legais aplicáveis.

g) Confidencialidade e sigilo profissional: sócios, advogados, empregados, estagiários, correspondentes e demais profissionais que tenham acesso a dados pessoais deverão observar os deveres de confidencialidade, sigilo profissional e uso adequado das informações. Sempre que pertinente, essas obrigações deverão ser formalizadas por meio de instrumentos contratuais, termos de confidencialidade ou outros documentos aplicáveis, sem prejuízo das obrigações legais e éticas inerentes ao exercício da advocacia.

h) Proteção de documentos físicos e ambientes de trabalho: documentos físicos contendo dados pessoais ou informações confidenciais deverão ser mantidos em locais apropriados, com acesso restrito às pessoas autorizadas. Deverão ser adotadas práticas de organização, guarda e descarte seguro, evitando-se a exposição indevida de informações em mesas, impressoras, salas de reunião e demais ambientes de trabalho.

i) Trabalho remoto: o tratamento de dados pessoais fora das dependências físicas do Escritório deverá observar medidas adequadas de confidencialidade e segurança, incluindo a proteção dos dispositivos utilizados, a utilização de conexões seguras e a prevenção de acesso indevido por terceiros. Os profissionais deverão adotar cuidados específicos para evitar a exposição de documentos, comunicações e informações protegidas pelo sigilo profissional.

j) Utilização de ferramentas de inteligência artificial: o uso de ferramentas de inteligência artificial nas atividades do Escritório deverá observar critérios de segurança, confidencialidade, necessidade e proteção de dados pessoais. A inserção de informações pessoais, processuais ou confidenciais nessas ferramentas dependerá de avaliação prévia quanto à adequação da solução, às condições de tratamento dos dados e aos riscos envolvidos, observadas as orientações internas e as obrigações contratuais e profissionais aplicáveis. Os resultados produzidos por essas ferramentas deverão ser submetidos à análise crítica e à revisão humana, especialmente quando utilizados na elaboração de documentos, manifestações ou atividades jurídicas.

k) Continuidade das atividades: o Escritório deverá adotar medidas proporcionais para reduzir os impactos decorrentes de falhas tecnológicas, indisponibilidade de sistemas, perda de informações ou outros eventos que possam comprometer a continuidade dos serviços jurídicos. Essas medidas poderão incluir procedimentos de recuperação de arquivos, utilização de cópias de segurança, definição de responsáveis e alternativas operacionais para situações de contingência, conforme os riscos identificados e a estrutura disponível.

12.1. Implementação, Acompanhamento e Melhoria Contínua

As diretrizes estabelecidas neste capítulo deverão orientar a implementação, a manutenção e o aprimoramento dos controles de segurança da informação do Escritório, observadas as responsabilidades dos profissionais envolvidos e as características das atividades desenvolvidas.

A efetiva adoção das medidas de segurança deverá ser acompanhada de forma proporcional aos riscos identificados, podendo ser demonstrada por registros, documentos, configurações de sistemas, procedimentos internos ou outras evidências compatíveis, sem exposição desnecessária de informações pessoais ou protegidas pelo sigilo profissional.

Eventuais fragilidades ou oportunidades de melhoria identificadas deverão ser avaliadas e, quando pertinente, registradas em instrumento de acompanhamento próprio, com definição de prioridades, responsáveis e prazos compatíveis com a criticidade dos riscos e a capacidade operacional do Escritório.

A previsão das medidas nesta Política constitui diretriz institucional e não representa, isoladamente, comprovação de sua efetiva implementação, a qual deverá ser verificada conforme os controles e recursos existentes.

XIII – GESTÃO DE INCIDENTES DE SEGURANÇA

Considera-se suspeita de incidente qualquer evento que possa afetar a confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais; sua comunicação interna deve ocorrer mesmo antes de confirmação.

- a) **Reporte Interno:** integrantes do Escritório deverão informar imediatamente suspeitas ao ponto focal definido através do e-mail privacidade@flaviolopes.adv.br, preservando evidências e evitando ações isoladas que prejudiquem a apuração;
- b) **Avaliação:** o responsável designado, com apoio técnico e jurídico, registrará o ocorrido, conterá os efeitos possíveis, identificará os dados e

titulares afetados e avaliará riscos, danos e responsabilidades;

- c) **Comunicação ao Cliente:** quando houver dados tratados em nome de cliente, o Escritório observará os prazos contratuais aplicáveis e fornecerá informações disponíveis para a avaliação do controlador, sem presumir prazo uniforme de **24 (vinte e quatro horas)** para todos os contratos;
- d) **Comunicação à ANPD e aos titulares:** quando o Escritório for controlador e o incidente se enquadrar nas hipóteses regulamentares de comunicação, serão observados os requisitos e prazos da Resolução CD/ANPD nº 15/2024 e eventuais atualizações. Quando atuar como operador, apoiará o controlador conforme contrato e legislação.
- e) **Registro:** os incidentes e as medidas adotadas serão documentados e preservados pelo prazo legal ou regulamentar aplicável, observadas as obrigações contratuais e a necessidade de proteção das evidências;
- f) **Melhoria:** após o tratamento, serão registradas as causas identificadas, medidas corretivas e eventuais necessidades de atualização de processos e treinamento.

XIV – RETENÇÃO E ELIMINAÇÃO

A retenção observará finalidade, obrigações legais e profissionais, prazos prescricionais, exercício regular de direitos, sigilo e contratos. A tabela de temporalidade deverá ser validada pelos responsáveis do Escritório, contemplando documentos processuais, dados administrativos, e-mails, arquivos temporários, cópias de segurança e devolução ou eliminação ao final de contratos. Nenhum prazo será considerado aprovado apenas por constar de minuta.

XV – PRIVACIDADE DESDE A CONCEPÇÃO E RELATÓRIO DE IMPACTO

Novas atividades, ferramentas, integrações, fornecedores, automações e usos de inteligência artificial deverão ser avaliados quanto à necessidade, finalidade, bases legais, segurança e impactos à privacidade antes de sua adoção, proporcionalmente ao risco.

A necessidade de RIPD será avaliada e documentada por atividade, considerando natureza dos dados, escala, tecnologias, cruzamento de bases e potenciais impactos aos titulares, inclusive em operações de recuperação de crédito. A decisão fundamentada deverá indicar se é necessária elaboração de RIPD completo, o qual dependerá de análise específica; esta Política não declara a existência de relatórios ainda não apresentados ou validados.

XVI – TREINAMENTO E CONSCIENTIZAÇÃO

O Escritório promoverá orientação e treinamentos proporcionais às funções e aos riscos, abrangendo sigilo profissional, princípios e bases legais, solicitações de titulares, compartilhamento, phishing, incidentes, retenção e uso de IA. Participação, conteúdo e data deverão ser registrados. Periodicidade e reciclagem serão definidas e acompanhadas pelos sócios, sem afirmar a realização de treinamentos anteriores sem evidência.

XVII – RESPONSABILIDADES

A implementação, a observância e o aprimoramento das diretrizes estabelecidas nesta Política constituem responsabilidades compartilhadas entre os profissionais que atuam em nome do Flávio Lopes Advogados Associados, observadas as atribuições de cada função e a natureza das atividades desenvolvidas.

17.1. Sócios Administradores

Compete aos sócios administradores aprovar esta Política e suas atualizações, assegurar o apoio institucional às práticas de privacidade e proteção de dados pessoais, definir responsabilidades internas e disponibilizar recursos proporcionais à estrutura e às necessidades operacionais do Escritório.

Cabe-lhes, ainda, acompanhar os principais riscos, pendências e oportunidades de melhoria identificados, apoiando a implementação das medidas necessárias à proteção das informações tratadas.

17.2. Encarregado pelo Tratamento de Dados Pessoais

Compete ao Encarregado pelo Tratamento de Dados Pessoais, **Leonardo Cantalino**, atuar como ponto de contato institucional entre o Escritório, os titulares de dados pessoais e a Agência Nacional de Proteção de Dados (ANPD), observadas as atribuições previstas na LGPD e na regulamentação aplicável.

No exercício de suas funções, caberá ao Encarregado receber e encaminhar solicitações e manifestações relacionadas à proteção de dados pessoais, orientar os profissionais quanto às práticas de privacidade, apoiar a manutenção dos registros pertinentes e acompanhar, em articulação com os responsáveis

envolvidos, o tratamento de ocorrências e incidentes relacionados a dados pessoais.

Sua atuação deverá ocorrer de forma compatível com a estrutura organizacional do Escritório, sem afastar as responsabilidades legais e operacionais atribuídas aos controladores, operadores e demais profissionais envolvidos nas atividades de tratamento.

17.3. Responsável por Sistemas e Suporte Técnico

Compete ao profissional ou prestador responsável pelos sistemas e pelo suporte técnico apoiar a implementação, a manutenção e o acompanhamento das medidas de segurança da informação sob sua responsabilidade, incluindo, conforme aplicável, a gestão de acessos, a proteção de dispositivos, a realização de cópias de segurança e os procedimentos de recuperação de informações.

Deverá, ainda, comunicar tempestivamente eventuais falhas, vulnerabilidades ou ocorrências que possam comprometer a segurança dos dados pessoais, colaborando com a adoção das medidas corretivas pertinentes.

17.4. Advogados e Responsáveis pelas Atividades de Tratamento

Compete aos advogados e demais profissionais responsáveis pelas atividades jurídicas e administrativas observar as diretrizes desta Política, identificar e comunicar as operações de tratamento realizadas em suas respectivas áreas e assegurar que o acesso, a utilização, o compartilhamento e a conservação de dados pessoais estejam vinculados a finalidades legítimas e necessidades profissionais.

Deverão, igualmente, preservar o sigilo profissional, observar os critérios de segurança aplicáveis e colaborar com a identificação e o tratamento de riscos relacionados às informações sob sua responsabilidade.

17.5. Demais Colaboradores, Estagiários e Terceiros

Compete aos empregados, estagiários, correspondentes jurídicos, prestadores de serviços e demais terceiros que tenham acesso a dados pessoais em razão de suas atividades utilizar as informações exclusivamente para finalidades

autorizadas, observar os deveres de confidencialidade e adotar os cuidados necessários à proteção de documentos, sistemas e credenciais de acesso.

Esses profissionais deverão comunicar prontamente ao Encarregado ou aos responsáveis internos competentes quaisquer ocorrências, suspeitas de incidentes ou situações que possam comprometer a privacidade, a confidencialidade ou a segurança dos dados pessoais tratados pelo Escritório.

XVIII – SANÇÕES

O descumprimento desta Política será analisado de forma proporcional, observados os vínculos contratuais, as normas profissionais, o contraditório quando aplicável e a legislação vigente. O dever de sigilo subsiste após o encerramento da relação com o Escritório.

XIX – VIGÊNCIA E REVISÃO

Esta Política entrará em vigor a partir de sua aprovação formal pelos sócios administradores do Escritório. Será revisada periodicamente e sempre que alterações relevantes nos processos de tratamento, na legislação, nos riscos identificados ou nas exigências contratuais justificarem sua atualização. O histórico de versões, as alterações e eventuais pendências de implementação serão registrados em controle próprio.

O histórico de versões, as alterações realizadas e as eventuais pendências de implementação serão devidamente registradas e acompanhadas em instrumento de controle próprio, de modo a assegurar a rastreabilidade, a atualização contínua e o aprimoramento das práticas de privacidade e proteção de dados pessoais do Escritório.

Versão / data	3.0 · outubro de 2026
Aprovação	Sócios administradores do Flávio Lopes Advogados Associados
Próxima revisão	Outubro de 2027
Histórico	1.0 – Política inicial (seções I a III). 2.0 – inclusão dos itens II e VII a XVII e adequação do tratamento por papel (controlador/operador), suboperadores, retenção e incidentes.