



LGPD

para a Advocacia



SÃO PAULO

Subseção
São José
do Rio Preto

Presidente Izabela Fantazia da Silva Rjaili
Vice-presidente Diego Carretero
Secretário-geral Roberto Ribeiro de Almeida
Secretária-adjunta Flaviana de Freitas
Tesoureira Claudionora Elis Tobias

OAB RIO PRETO
Ordem dos Advogados do Brasil - 22ª Subseção
Avenida Brigadeiro Faria Lima, 5853, Vila São José,
São José do Rio Preto/SP,
CEP. 15090-000

Autora **Beatriz Hilkner de Souza** – OAB/SP 411.847
Coordenadora da Comissão de Privacidade e
Proteção de Dados e Encarregada Setorial da
22ª Subseção da Ordem dos Advogados do
Brasil de São Paulo

Autora **Ana Beatriz Neves S. Belati** – OAB/SP - 521.821
Vice Coordenadora da Comissão de Privacidade
e Proteção de Dados da 22ª Subseção da Ordem
dos Advogados do Brasil de São Paulo

Autora **Mirela Vergílio Gênova** – OAB/SP - 361.225
Membra da Comissão de Privacidade e Proteção
de Dados da 22ª Subseção da Ordem dos
Advogados do Brasil de São Paulo

Revisão e **Oreonnilda de Souza** – OAB/SP 294.646
Editoração Membra da Comissão de Privacidade e Proteção
de Dados da 22ª Subseção da Ordem dos
Advogados do Brasil de São Paulo

Versão 2.0 rev., atual. e ampl.
Publicação digital (agosto/2025)

SUMÁRIO

Palavras da Presidente.....	05
<i>Dra. Izabela Fantazia da Silva Rjaili</i>	
Apresentação.....	06
<i>Dra. Oreonnilda de Souza</i>	
LGPD e seus objetivos.....	09
<i>Dra. Beatriz Hilknner de Souza</i>	
Conceitos importantes.....	12
<i>Dra. Beatriz Hilknner de Souza</i>	
Princípios: fundamentos da LGPD.....	15
<i>Dra. Mirela Vergílio Gênova</i>	
Bases legais para tratamento de dados.....	19
<i>Dra. Beatriz Hilknner de Souza</i>	
Compartilhamento de dados pelo(a) advogado(a).....	26
<i>Dra. Beatriz Hilknner de Souza</i>	
Responsabilidade dos(as) advogados(as).....	30
<i>Dra. Beatriz Hilknner de Souza</i>	
Direitos e deveres dos titulares.....	33
<i>Dra. Mirela Vergílio Gênova</i>	
O que fazer em caso de incidente de segurança.....	36
<i>Dra. Mirela Vergílio Gênova</i>	
Boas práticas para advogados(as).....	38
<i>Dra. Beatriz Hilknner de Souza</i>	
Golpe do Falso Advogado.....	43
<i>Dra. Ana Beatriz Neves Silva Belati</i>	
Conteúdo bônus e links úteis.....	46

Palavras da Presidente

Advocacia,

A 22ª Subseção da Ordem dos Advogados do Brasil – Seção São Paulo – São José do Rio Preto, por meio da sua Comissão de Privacidade e Proteção de Dados, liderada pela Dra. Beatriz Hilkner de Souza e Dra. Ana Beatriz Neves Silva Belati, elaborou o presente guia, já em sua segunda edição, com fim de auxiliar as advogadas e advogados na aplicação da LGPD em seu dia-a-dia no escritório.

Nesta segunda edição, a Comissão preocupou-se em trazer um capítulo especial para tratar sobre o “golpe do falso advogado” que, infelizmente, vem crescendo cada vez mais e tem gerado prejuízos para a advocacia e muita preocupação para o Sistema Ordem como um todo (Subseção, Secional e Conselho Federal).

Em todo o guia a advogada e advogado poderá ter acesso as medidas de cautela que devem adotar desde o primeiro atendimento de seus clientes, passando pela coleta, armazenamento e descarte dos dados.

Aproveitamos a oportunidade para informar que nossa Subseção vem seguindo rigorosamente tal legislação e tem se engajado no combate ao “golpe do falso advogado”.

Agradeço a Comissão da LGPD pela iniciativa e trabalho que vem realizando tanto na formação da advocacia quanto na implantação da LGPD na Subseção.

Contem sempre com esta Presidente e sua Diretoria.

Izabela Fantazia da Silva Rjaili

Presidente da OAB São José do Rio Preto

APRESENTAÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709/2018, representa um marco na tutela dos dados pessoais no Brasil, especialmente conferiu mais efetividade ao direito de privacidade, tanto em ambientes on-line quanto em off-line.

Com a entrada em vigor da LGPD, os dados pessoais passam a ter ampla proteção, conferindo, aos seus titulares, maior controle sobre eles ao longo do processo de tratamento, desde a permissão para acesso, correção, exclusão e portabilidade de dados pessoais.

Obrigações legais que, sem dúvidas, proporcionam mais segurança, confiabilidade no tratamento de dados por exigir transparência, ética e informações sobre o tratamento mediante a solicitação do titular.

Durante as reuniões do grupo de estudos da Comissão de Privacidade e Proteção de Dados da 22ª Subseção da Ordem dos Advogados do Brasil surgiu a ideia, materializada em uma proposta, de elaboração de um guia a partir da necessidade premente, em especial, dos jovens advogados(as) no correto tratamento de dados pessoais de seus patrocinados.

Assim, nasceu o “Guia LGPD para Advogados”, com a primeira edição publicada em maio de 2024, com pretensões de auxiliar advogados(as) no cumprimento das obrigações impostas pela LGPD. Todavia com as alterações e inovações legislativas, jurisprudenciais e tecnológicas envolvendo a matéria, especialmente o “golpe do advogado”, uma fraude cada vez mais comum no Brasil, a Comissão de Privacidade e Proteção de Dados promoveu revisões, atualizações e ampliações e, agora, em sua

segunda edição: “LGPD para a Advocacia” contempla uma seção exclusiva sobre esse assunto, indicando meios de proteção e, no caso, de crime consumado, quais as ações necessárias para enfrentamento.

Neste Guia você encontrará definições e esclarecimentos relevantes sobre institutos e atores trazidos pela LGPD como, por exemplos, no que consiste os dados pessoais, quem são seus titulares, como deve ser realizado o tratamento no exercício da advocacia, quem são os operadores, controladores e encarregados de dados e quando é necessário, ou não, o consentimento do titular para tratamento de seus dados. Também são disponibilizados links úteis, modelos de documentos e ferramentas práticas que fortalecerão a atuação profissional da advocacia.

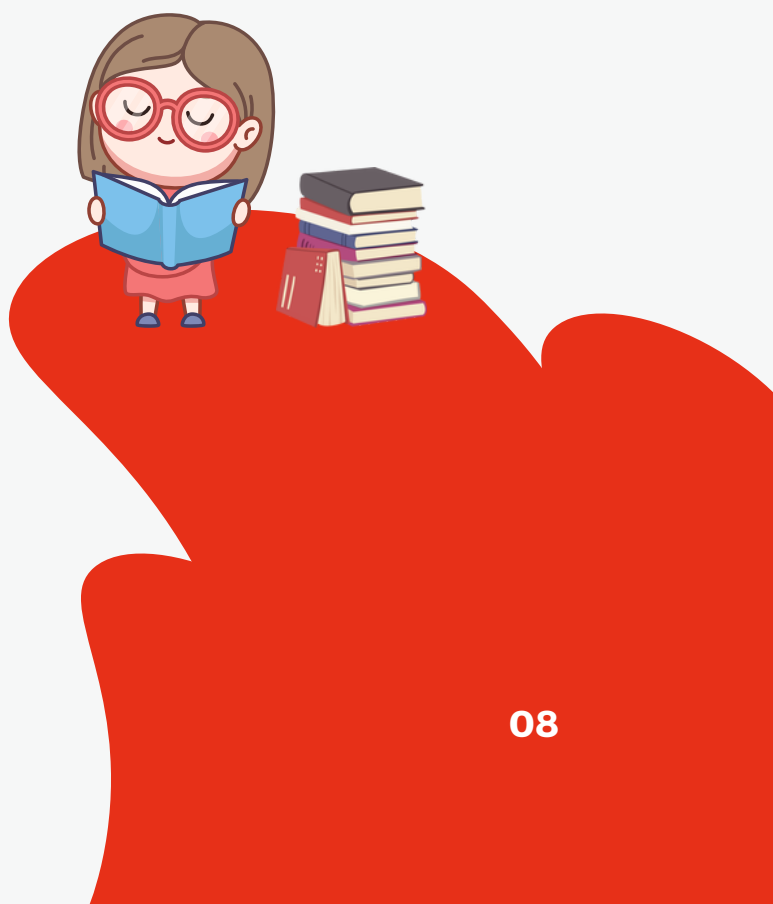
Além disso, abordamos a responsabilidade dos(as) advogados(as) no tratamento de dados pessoais, demonstrando meios eficazes, especialmente quanto à prevenção, em conformidade às exigências da LGPD para que sejam evitadas sanções (advertência, suspensão e bloqueio do tratamento de dados e/ou multas) e no caso de incidente de segurança (tratamento inadequado de dados como o vazamento) quais medidas devem ser adotadas.

Registramos nosso sincero agradecimento ao Presidente da gestão anterior da OAB Rio Preto, Dr. Henry Atique, cujo comprometimento com a inovação e com a proteção dos direitos fundamentais foi essencial para o desenvolvimento da nossa Comissão e o lançamento deste Guia. Seu apoio e visão institucional foram decisivos para que essa iniciativa se tornasse realidade, contribuindo para a capacitação da advocacia frente aos desafios contemporâneos da Era digital.

Estendemos nossos especiais agradecimentos à atual Presidente, Dr.^a Izabela Fantazia da Silva Rjaili, por manter e fortalecer esse projeto com igual dedicação. Sua gestão tem reafirmado o compromisso da Ordem com a atualização e o preparo da advocacia diante das transformações tecnológicas e jurídicas que impactam diretamente o exercício profissional. A continuidade desse apoio demonstra o valor do trabalho coletivo e da responsabilidade institucional na construção de uma advocacia cada vez mais preparada e atuante.

A Comissão de Privacidade e Proteção de Dados da OAB Rio Preto espera contribuir com os(as) colegas advogados(as) no cumprimento desse relevante mister, entregando serviço de qualidade na defesa dos interesses e direitos de nossos clientes de modo ético, transparente e seguro.

Boa leitura!



LGPD E SEUS OBJETIVOS



A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, representa um marco fundamental no ordenamento jurídico brasileiro. Sua promulgação estabeleceu um novo paradigma para a proteção de dados pessoais, elevando-os ao patamar de direito fundamental. O objetivo central do legislador foi criar um ambiente de segurança jurídica e confiança, regulando o tratamento de dados pessoais em todo o território nacional. É crucial entender que essa abrangência inclui tanto o tratamento de dados realizado em meios digitais (online) quanto em meios físicos (offline), um ponto frequentemente mal compreendido.

A LGPD atua diretamente na proteção de direitos essenciais como a privacidade, a liberdade e o livre desenvolvimento da personalidade da pessoa natural. Para alcançar esses propósitos, a Lei estabelece diretrizes claras e responsabilidades para todos aqueles que tratam dados pessoais com finalidade lucrativa, sejam pessoas físicas ou jurídicas, no setor público ou privado.

Dentre os principais objetivos que motivaram a criação da LGPD, destacam-se:

- **Proteger a Privacidade e os Direitos Fundamentais dos Titulares:** O foco principal da Lei é garantir ao indivíduo o controle sobre suas informações pessoais. Isso se traduz no reconhecimento de diversos direitos ao titular dos dados, como o acesso, a correção, a exclusão e a portabilidade de seus dados, assegurando que o cidadão tenha o poder de decidir sobre o uso de suas próprias informações.

- **Promover a Segurança e a Confiabilidade no Tratamento de Dados:** A LGPD impõe uma série de obrigações aos agentes de tratamento (Controladores e Operadores) para que adotem medidas técnicas e administrativas rigorosas. Essas medidas visam proteger os dados contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. A segurança da informação é, portanto, um pilar central da Lei.
- **Estimular a Transparência e a Ética no Uso de Dados:** A lei determina que o tratamento de dados pessoais deve ser realizado de forma clara e compreensível ao titular. Os agentes de tratamento são obrigados a informar como os dados serão coletados, utilizados e para quais finalidades, fomentando uma cultura de ética e prestação de contas (*accountability*) em todas as operações de tratamento.

Ao concretizar esses objetivos, a LGPD visa, também, fomentar um ambiente propício para a inovação e o desenvolvimento tecnológico e econômico no país, ao mesmo tempo em que garante a proteção da dignidade e dos direitos dos cidadãos na era digital.

Para os profissionais do Direito, a LGPD traz impactos significativos, exigindo uma nova postura e aprimoramento contínuo:

- **Atualização Profissional e Conhecimento Especializado:** é imprescindível que advogados(as) se familiarizem com os conceitos, princípios e bases legais da LGPD, aprofundando seus conhecimentos em proteção de dados, segurança da informação e temas correlatos.





- **Adaptação das Práticas Jurídicas e Processos Internos:** escritórios de advocacia e profissionais autônomos devem adaptar suas rotinas para garantir a conformidade. Isso envolve a revisão de contratos, políticas de privacidade, termos de uso, e a adequação de todos os procedimentos que envolvam a coleta, armazenamento e tratamento de dados pessoais.

- **Surgimento de Novas Áreas de Atuação e Oportunidades:** a demanda por profissionais especializados em proteção de dados tem crescido exponencialmente, criando nichos de mercado em consultoria de compliance, análise de conformidade, representação em processos administrativos perante a Autoridade Nacional de Proteção de Dados (ANPD) e litígios judiciais envolvendo a Lei.



A LGPD, portanto, não é apenas um conjunto de regras a serem seguidas, mas um convite à reflexão sobre a responsabilidade no uso da informação. Para os advogados(as), a compreensão e a internalização desses objetivos são cruciais para garantir a defesa dos interesses de seus clientes em conformidade com a legislação e para manter a credibilidade e a ética que são inerentes à nossa profissão.

CONCEITOS IMPORTANTES

Para compreender a LGPD e suas implicações na prática jurídica é fundamental dominar alguns conceitos-chave. A correta identificação e aplicação desses termos são o ponto de partida para qualquer advogado(a) que busque se adequar à Lei.

Conhecer essas definições é o primeiro passo para entender como a LGPD se aplica à rotina do seu escritório:

- **Dado Pessoal:** qualquer informação que se refira a uma pessoa natural identificada (cujo nome, CPF etc., já estão explícitos) ou identificável (cuja identidade pode ser alcançada por meio de outros dados ou combinações de informações).

Exemplos: O nome completo de um cliente, seu e-mail, telefone e endereço residencial.

- **Dado Sensível:** Uma categoria especial de dado pessoal que, por sua natureza, exige proteção ainda maior. Refere-se a informações 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.

Exemplos: um atestado médico de um cliente, informação sobre sua religião, ou dados biométricos usados para acesso. O tratamento de dados sensíveis possui regras mais rígidas na LGPD.

- **Tratamento de Dados:** abrange toda e qualquer operação realizada com dados pessoais. Desde o momento da coleta até a sua eliminação, passando por armazenamento, produção, acesso, uso, classificação, reprodução, comunicação, transmissão, distribuição, processamento, arquivamento, avaliação, controle, modificação, entre outros.

Exemplos: Anotar o nome de um cliente em um formulário, salvar o e-mail em um sistema, compartilhar um documento com dados de processo, ou apagar informações antigas.

- **Titular dos Dados:** é a pessoa natural a quem os dados pessoais se referem. É o indivíduo que é "dono" das informações.

Exemplos: Seu cliente, um colaborador do escritório, ou a parte contrária em um processo.

- **Controlador:** pessoa natural ou jurídica (o escritório de advocacia ou o[a] advogado[a] autônomo[a], nesse caso) a quem compete as decisões referentes ao tratamento de dados pessoais. É quem decide "o que", "como" e "para que" os dados serão tratados.

Exemplo: Você, enquanto advogado(a), decide quais dados coletar de seus clientes para um processo e como eles serão armazenados.

- **Operador:** pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome e de acordo com as instruções do Controlador. O Operador age sob as ordens do Controlador.

Exemplos: Uma empresa de software jurídico que armazena os dados dos seus clientes em nuvem para você, ou um escritório parceiro que te auxilia em um processo e trata dados sob sua supervisão.

- **Encarregado de Dados (DPO - Data Protection Officer):** pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Observação importante: A ANPD publicou em dezembro de 2024 um guia detalhando as funções do Encarregado. Embora seja uma figura crucial para grandes empresas, o Regulamento para Agentes de Tratamento de Pequeno Porte (Resolução ANPD nº 2/2022) prevê flexibilizações para escritórios de advocacia que se enquadrem nos critérios de PME. Mesmo assim, a designação de um ponto focal interno para assuntos de LGPD (que pode ser o próprio advogado[a] titular do escritório ou um colaborador) é uma boa prática para gerenciar as demandas dos titulares e se comunicar com a ANPD se necessário.

- **Anonimização:** processo técnico pelo qual um dado perde a possibilidade de ser associado, direta ou indiretamente, a um indivíduo, por meios razoáveis e disponíveis. Dados anonimizados deixam de ser considerados dados pessoais.

Observação importante: A pseudoanonimização, por sua vez, é a técnica que permite a reversão da desidentificação por meio de informações adicionais mantidas separadamente. Diferentemente da anonimização, dados pseudoanonimizados ainda são considerados dados pessoais e devem ser protegidos pela LGPD. A ANPD tem aprofundado a discussão sobre a efetividade da anonimização e as diferenças entre essas técnicas.

Caso queira aprofundar-se nos estudos, o art. 5º da LGPD possui um rol completo com várias outras definições. No entanto, a compreensão dos "conceitos-chave" acima listados é fundamental e será de grande ajuda no processo inicial de adequação à LGPD do seu escritório.

PRINCÍPIOS: fundamentos da LGPD

A LGPD estabelece, no art. 6º, os princípios fundamentais que devem nortear qualquer tratamento de dados pessoais — inclusive na atividade advocatícia. Esses princípios não são meramente teóricos: eles oferecem a base técnica e ética para a construção de um escritório seguro, transparente e juridicamente adequado.

Muitas vezes esquecidos na prática, os princípios da LGPD são a nossa verdadeira âncora de conformidade. Como advogados(as), temos o dever de compreendê-los e aplicá-los — tanto em nossos escritórios quanto ao orientar clientes em suas atividades.

São 11 (onze) os princípios orientadores. A seguir, explicados com foco na advocacia:

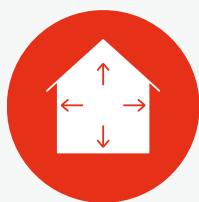
- **Boa-fé:** é o ponto de partida de todo o tratamento de dados. Ainda que você atue sozinho ou com poucos recursos, é essencial demonstrar que adotou medidas razoáveis para proteger os dados pessoais sob sua responsabilidade.



Reduzir o risco a zero é impossível. Mas, evidenciar que o escritório agiu com zelo, intenção legítima e responsabilidade é imprescindível, inclusive para fins de eventual fiscalização.



- **Finalidade:** Por que você está tratando esse dado? Na advocacia, o tratamento de dados deve sempre ter uma finalidade legítima, específica e informada ao cliente ou titular, seja na captação de leads, na coleta de documentos para petições ou no uso de e-mails para enviar atualizações. **É vedado utilizar esses dados para outras finalidades sem nova base legal ou consentimento.**



- **Adequação:** exige que os dados tratados estejam compatíveis com a finalidade declarada. Por exemplo: coletar dados financeiros de um cliente será justificada se forem essenciais à demanda jurídica (como em ações indenizatórias, alimentares, empresariais etc.).



- **Necessidade:** Evite coletar mais do que o necessário. Se você está ajuizando uma ação cível, não há motivo para solicitar dados médicos detalhados, por exemplo. Trate apenas os dados mínimos indispensáveis à atividade jurídica proposta.

- **Transparência:** Como advogados(as), estamos acostumados a atuar com sigilo. Mas a LGPD exige também transparência sobre os tratamentos realizados.



Isso inclui deixar claro: quem trata os dados, para qual finalidade, com que base legal e por quanto tempo. Simples, direto e documentado.



- **Livre acesso:** O titular (seu cliente ou outra parte) tem o direito de saber quais dados você possui, como foram coletados, por quanto tempo serão armazenados e com quem foram, ou serão, eventualmente compartilhados. **Tenha isso organizado. Se ele solicitar, você precisará responder de forma clara, rápida e gratuita.**



- **Qualidade dos dados:** Dados desatualizados ou imprecisos podem prejudicar tanto o processo quanto o relacionamento com o cliente. Mantenha os dados sempre atualizados, completos e relevantes, conforme a necessidade da demanda.



- **Prevenção:** Não basta reagir a incidentes — é preciso atuar preventivamente. Treine sua equipe, revise seus contratos com fornecedores, tenha cláusulas de confidencialidade, formalize orientações internas sobre dados sensíveis. Essa conduta pode evitar prejuízos ao cliente e à sua reputação como profissional.

- **Segurança:** Adotar medidas técnicas e administrativas para proteger dados pessoais é uma obrigação.



Mesmo que você não tenha um servidor próprio, pode (e deve) adotar práticas como: senhas seguras; armazenamento criptografado ou com autenticação; não usar e-mail pessoal para envio de peças sensíveis; assinaturas eletrônicas com certificado; políticas internas mínimas com estagiários e equipe. **A ausência dessas medidas pode ser mais grave que o vazamento em si, aos olhos da ANPD.**



- **Não Discriminação:** Na advocacia, pode surgir o acesso a dados de origem racial, religiosa, política ou de orientação sexual. É fundamental garantir que esses dados não sejam utilizados para tratamento abusivo ou discriminatório, seja na triagem de casos, seleção de clientes, contratos ou ambientes internos.



- **Responsabilização e prestação de contas:** Você, como advogado(a), precisa estar preparado para provar que adotou medidas de conformidade com a LGPD.

Documente: as práticas internas, as cláusulas contratuais de proteção de dados, os fluxos de atendimento com consentimento ou base legal, os termos de uso no site do escritório, os registros de incidentes e respostas. A *accountability* (responsabilidade) é o pilar da advocacia moderna. **Transparência, boa-fé e organização — esses são seus melhores aliados.**

BASES LEGAIS PARA TRATAMENTO DE DADOS

Para que qualquer operação de tratamento de dados pessoais seja lícita e esteja em conformidade com a LGPD, ela deve estar amparada em uma das bases legais previstas nessa Lei. O art. 7º da LGPD apresenta um rol taxativo dessas hipóteses, o que significa que o tratamento de dados só pode ser realizado se houver um enquadramento em uma (ou mais) dessas bases.

Compreender qual base legal se aplica a cada situação é crucial para garantir a conformidade do seu escritório e evitar problemas futuros.

As Bases Legais da LGPD (Art. 7º)

Conforme a LGPD, as bases legais que autorizam o tratamento de dados pessoais são:

- **Consentimento:** o tratamento de dados é permitido pela manifestação livre, informada e inequívoca do titular, para uma finalidade determinada.

Observação importante: O consentimento deve ser específico e transparente. A ANPD tem enfatizado que **não valem "consentimentos genéricos" ou "implícitos"**. Além disso, o titular pode revogar o consentimento a qualquer tempo, de forma facilitada.

- **Obrigação Legal ou Regulatória:** o tratamento é necessário para cumprir uma obrigação imposta por lei ou regulamento (normas, portarias, instruções normativas, entre outros).
 - **Exemplos:** Fornecer dados de colaboradores para órgãos como Previdência Social e e-Social, ou para cumprir determinações judiciais.
- **Execução de Políticas Públicas:** o tratamento é realizado pela Administração Pública para a execução de políticas e atividades previstas em leis ou regulamentos, ou com base em contratos, convênios ou instrumentos congêneres.
- **Realização de Estudos por Órgão de Pesquisa:** o tratamento é necessário para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.
- **Execução de Contrato ou Procedimentos Preliminares:** o tratamento é necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular seja parte.
 - **Exemplo:** Coletar dados de um cliente para formalizar um contrato de prestação de serviços advocatícios, ou para a elaboração de uma procuração.
- **Exercício Regular de Direitos:** o tratamento é necessário para o exercício regular de direitos em processo judicial, administrativo ou arbitral.
 - **Exemplo:** Utilizar dados do cliente ou da parte contrária em uma petição, em documentos de processo administrativo ou em uma arbitragem, quando estritamente necessário para a defesa dos interesses do cliente.



- **Proteção da Vida ou Incolumidade Física:** o tratamento é realizado para a proteção da vida ou da incolumidade física do titular ou de terceiro.
- **Tutela da Saúde:** o tratamento é realizado por profissional de saúde, serviço de saúde ou autoridade sanitária, ou para garantir a proteção à saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.
- **Proteção ao Crédito:** O tratamento é necessário para a proteção do crédito.

Observação: A ANPD incluiu a regulamentação das hipóteses legais de proteção ao crédito em sua Agenda Regulatória 2025-2026.

- **Legítimo Interesse:** o tratamento é realizado para atender a interesses legítimos do controlador ou de terceiro, exceto quando prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Observação importante: O legítimo interesse NÃO É UM "CORINGA". Para utilizá-lo, o(a) advogado(a) precisa demonstrar que o tratamento é realmente necessário para um propósito legítimo e que não viola os direitos e liberdades fundamentais do titular. A ANPD possui um Guia Orientativo sobre Legítimo Interesse que recomenda a elaboração de um Relatório de Legítimo Interesse (RLI) para documentar a análise e justificativa da sua utilização.

Principais Bases Legais Aplicáveis à Advocacia

Considerando as definições da LGPD e a rotina de um escritório de advocacia, algumas bases legais se destacam como as mais frequentemente utilizadas. É crucial que o(a) advogado(a) saiba identificá-las e aplicá-las corretamente:

- **Execução de Contrato ou Procedimentos Preliminares:**

Esta é uma das bases mais robustas e comuns na advocacia. Aplica-se ao tratamento dos dados que são **estritamente necessários** para o cumprimento do contrato de prestação de serviços advocatícios que você tem com seu cliente.



Exemplos práticos:

1. Coleta de dados (nome completo, CPF, endereço, qualificação) do cliente para a celebração do contrato de honorários.
2. Obtenção de dados bancários para o pagamento de honorários ou custas judiciais.
3. Coleta de informações específicas do caso (como documentos, histórico, dados sobre o objeto da demanda) essenciais para a elaboração de peças processuais e a condução do processo.
4. Dados de colaboradores (estagiários, parceiros, associados) para a formalização de seus contratos de trabalho ou parceria.

Ponto de Atenção: Esta base legal só justifica o tratamento de dados que são indispensáveis para a execução do contrato. Dados adicionais, não essenciais ao serviço contratado, podem exigir outra base legal (como o consentimento).

- **Exercício Regular de Direitos:** esta base é fundamental para a atuação contenciosa e consultiva do(a) advogado(a). Permite o tratamento de dados necessário para a defesa dos interesses do cliente, seja em âmbito judicial (processos, recursos), administrativo (procedimentos em órgãos públicos, autarquias) ou arbitral.

Exemplos práticos:

1. Uso de dados do cliente, da parte contrária, de testemunhas ou de terceiros envolvidos no processo para a elaboração de petições, recursos e manifestações judiciais.
2. Tratamento de dados em fase de investigação ou diligências para a busca de provas ou informações relevantes para a defesa do cliente.
3. Apresentação de documentos com dados pessoais em processos administrativos ou em procedimentos arbitrais.

- **Obrigação Legal ou Regulatória:** o(a) advogado(a), assim como qualquer profissional ou empresa, está sujeito a uma série de leis e regulamentos que exigem o tratamento ou o compartilhamento de dados.

Exemplos práticos:

1. Compartilhamento de dados com a Receita Federal para fins fiscais.
2. Envio de informações para órgãos como INSS e e-Social relacionadas à folha de pagamento de colaboradores.
3. Cumprimento de intimações ou determinações judiciais que exijam a apresentação de dados, mesmo que sigilosos.
4. Observância de regras do Conselho Federal e Seccionais da OAB que impliquem o tratamento de dados.

- **Consentimento:** embora seja a base legal mais conhecida, na advocacia, o consentimento deve ser utilizado com cautela e, preferencialmente, quando as outras bases legais não se aplicarem. Ele exige que o titular dê sua permissão de forma clara e específica para uma finalidade determinada. Lembre-se que o consentimento pode ser revogado a qualquer momento pelo titular, o que impacta a continuidade do tratamento dos dados com base nesta hipótese.



Exemplos práticos:

1. Coleta de dados para envio de newsletters informativas sobre o escritório, sem relação direta com a prestação de um serviço específico.
2. Uso de imagem ou depoimento de um cliente para fins de marketing do escritório (desde que não viole o sigilo profissional).
3. Dados coletados para finalidades que vão além do necessário para a execução do contrato ou o exercício de direitos (ex.: pesquisas de satisfação detalhadas, com uso de dados não essenciais).
4. No contexto de procurações, se a procuração descrever de forma específica as finalidades do tratamento de dados para o caso, pode-se entender que há um consentimento implícito ou uma combinação com a base de execução de contrato/exercício regular de direitos. Contudo, para evitar ambiguidades, uma finalidade clara é sempre a melhor prática.

- **Legítimo Interesse:** esta base legal pode ser aplicada em situações em que o tratamento de dados é necessário para fins legítimos do escritório ou de terceiros, desde que os direitos e liberdades fundamentais do titular não sejam comprometidos. Requer um cuidadoso Teste de Proporcionalidade e documentação (um Relatório de Impacto à Proteção de Dados), justificando o interesse, a necessidade e a mitigação dos riscos aos titulares.

Exemplos práticos (com cautela e documentação):

1. Uso de dados de contato de ex-clientes para comunicar mudanças no escritório ou oferecer novos serviços (desde que o interesse do escritório seja legítimo e não exceda as expectativas do titular).
2. Medidas de segurança da informação, como monitoramento de redes internas ou sistemas de acesso, para proteger o escritório e seus dados.
3. Análise de dados internos para melhoria de processos e gestão do escritório, desde que minimizados e, se possível, pseudoanonimizados.

Bases Legais Menos Comuns na Advocacia



É importante notar que algumas bases legais são mais direcionadas a outros setores ou tipos de tratamento e raramente se aplicam diretamente à rotina da maioria dos escritórios de advocacia:

- **Execução de Políticas Públicas:** geralmente aplicável a órgãos governamentais.
- **Realização de Estudos por Órgão de Pesquisa:** específica para instituições de pesquisa.
- **Proteção da Vida ou Incolumidade Física:** casos de emergência extrema.
- **Tutela da Saúde:** exclusiva para profissionais, serviços ou autoridades sanitárias.
- **Proteção ao Crédito:** ligada a atividades de análise e concessão de crédito.

Ao compreender e aplicar corretamente as bases legais, você garante que o tratamento de dados em seu escritório esteja em plena conformidade com a LGPD, construindo uma base sólida para a segurança e a confiança em sua prática profissional.

COMPARTILHAMENTO DE DADOS PELO(A) ADVOGADO(A)

O compartilhamento de dados pessoais é uma prática constante e, muitas vezes, indispensável na rotina da advocacia, sendo essencial para a defesa dos interesses dos clientes e o cumprimento das obrigações profissionais. Seja ao protocolar uma peça processual com informações do cliente no Tribunal, ao colaborar com outro(a) advogado(a) ou ao utilizar softwares e plataformas de gestão, o(a) advogado(a) está, invariavelmente, compartilhando dados.

No entanto, a Lei Geral de Proteção de Dados Pessoais (LGPD) impõe responsabilidades significativas aos profissionais do Direito que realizam esse compartilhamento, exigindo que a proteção dos dados sob sua guarda seja mantida em todas as etapas.

Situações Comuns de Compartilhamento de Dados



Advogados(as) frequentemente compartilham dados pessoais com:

- **O próprio cliente:** para validação de informações, apresentação de pareceres e documentos.
- **Outros profissionais do Direito:** como advogados(as) parceiros(as), correspondentes ou consultores para atuação conjunta em processos ou casos específicos.
- **Poder Judiciário e órgãos administrativos:** para o ajuizamento de ações, apresentação de recursos, petições ou para o cumprimento de diligências e determinações oficiais.
- **Órgãos públicos:** para o cumprimento de obrigações legais, regulatórias ou fiscais (Ex: Receita Federal, Previdência Social).

- **Empresas, instituições e peritos:** para a realização de diligências, obtenção de provas, elaboração de laudos ou pareceres técnicos.
- **Fornecedores de serviços e tecnologias:** como plataformas de gestão de processos, softwares de comunicação, serviços de armazenamento em nuvem, empresas de certificação digital, entre outros.

Deveres do Advogado(a) ao Compartilhar Dados



Ao compartilhar dados, os advogados(as) possuem deveres específicos para garantir a conformidade com a LGPD:

1. Possuir Base Legal Adequada: todo compartilhamento deve estar amparado por uma das bases legais da LGPD (art. 7º), como o exercício regular de direitos, a execução de contrato ou o cumprimento de obrigação legal. O consentimento do titular pode ser necessário em situações específicas, mas não é a única nem sempre a principal base para o compartilhamento inerente à atividade jurídica.

2. Informar o Titular: sempre que possível, o cliente deve ser informado sobre o compartilhamento de seus dados, as finalidades desse compartilhamento e com quem os dados serão compartilhados. A transparência é um princípio-chave da LGPD.

3. Adotar Medidas de Segurança: é imprescindível implementar medidas técnicas e organizacionais que protejam os dados durante o compartilhamento. Além disso, o(a) advogado(a) deve se certificar de que os receptores dos dados (terceiros) também adotem níveis adequados de segurança.

4. Garantir Finalidades Legítimas: o compartilhamento deve ser realizado para finalidades legítimas e compatíveis com aquelas para as quais os dados foram originalmente coletados, sempre em alinhamento com os princípios da LGPD (finalidade, adequação, necessidade, segurança, entre outros).



Ferramentas Essenciais para um Compartilhamento Seguro

Para assegurar um compartilhamento de dados pessoais em conformidade com a LGPD, recomenda-se a utilização das seguintes ferramentas e práticas:

- **Acordos de Confidencialidade (NDAs):** instrumentos jurídicos que garantem a confidencialidade das informações compartilhadas entre as partes. São fundamentais para proteger o sigilo profissional.
- **Contratos de Tratamento de Dados (Data Processing Agreements - DPAs) ou Cláusulas Contratuais Específicas:** a prática de mercado, reforçada pelas diretrizes da ANPD, exige que, ao contratar serviços de terceiros que atuarão como Operadores (tratando dados em nome do seu escritório, como softwares de gestão, serviços de contabilidade, provedores de cloud), o(a) advogado(a) estabeleça formalmente as responsabilidades e obrigações de proteção de dados. Esses contratos ou cláusulas devem definir quem é o Controlador e quem é o Operador, as finalidades do tratamento, as medidas de segurança a serem adotadas, e as condições para a eventual subcontratação.
 - **Atenção à Transferência Internacional de Dados:** se o compartilhamento envolver serviços ou tecnologias com servidores localizados fora do Brasil, é crucial observar a Resolução nº 19/2024 da ANPD, publicada em agosto de 2024, que regulamenta a Transferência Internacional de Dados, exigindo salvaguardas adicionais, como as Cláusulas Contratuais Padrão (CCPs) ou outras garantias. Muitos softwares jurídicos em nuvem podem se enquadrar nesta categoria.



- **Termos de Consentimento (quando aplicável):** documentos específicos que informam o cliente sobre o compartilhamento de seus dados para finalidades que exigem seu consentimento explícito, detalhando a finalidade, com quem será compartilhado e os direitos do titular.
- **Plataformas Seguras de Compartilhamento de Dados:** utilização de ferramentas e tecnologias que ofereçam criptografia, controle de acesso e trilha de auditoria para o envio e recebimento de informações. Evite o compartilhamento de dados sensíveis por e-mails comuns ou meios não criptografados.
- **Políticas Internas Claras:** desenvolver procedimentos internos que orientem os colaboradores sobre como e quando os dados podem ser compartilhados, além de quais medidas de segurança serão adotadas.

Ao adotar essas cautelas, o(a) advogado(a) não apenas cumpre as exigências da LGPD, mas, também, fortalece a confiança de seus clientes e protege a integridade e a segurança das informações sob sua responsabilidade profissional.



RESPONSABILIDADE DOS(AS) ADVOGADOS(AS)

A LGPD impõe novos desafios e responsabilidades aos advogados que atuam como controladores de dados. A compreensão das obrigações e dos riscos envolvidos na gestão de dados pessoais é crucial para garantir sua atuação profissional, o(a) advogado(a) é, na maioria das vezes, o Controlador dos dados pessoais que trata.

Isso significa que é você quem decide "o que", "como" e "para que" os dados dos seus clientes, colaboradores e outros envolvidos serão utilizados. Com essa posição vêm responsabilidades importantes, e a Lei Geral de Proteção de Dados Pessoais (LGPD) deixa isso bem claro.

Não cumprir a LGPD pode trazer consequências sérias para o(a) advogado(a) e para o escritório, incluindo:

- **Multas:** a Autoridade Nacional de Proteção de Dados (ANPD) pode aplicar multas altas.
- **Outras Sanções Administrativas:** como a proibição de tratar certos dados.
- **Processos Judiciais:** clientes ou outras pessoas podem processar você por danos morais ou materiais se os dados deles forem vazados ou usados indevidamente.
- **Dano à Reputação:** quebra de confiança e perda de credibilidade profissional.

Para evitar esses problemas e atuar em conformidade, o(a) advogado(a) tem algumas obrigações essenciais:

1 Proteger os Dados Pessoais

Sua principal responsabilidade é garantir a segurança dos dados que você coleta e armazena. Isso significa ter medidas para evitar que eles sejam acessados por pessoas não autorizadas, perdidos, alterados ou vazados.

- **O que fazer:** implemente as "Boas Práticas" de segurança que detalharemos em outro tópico. Em resumo: proteja seus dispositivos, seja cuidadoso com e-mails e senhas, e use ferramentas de proteção.

2 Respeitar os Direitos dos Titulares dos Dados

Os clientes e outras pessoas cujos dados você trata (os "titulares") têm direitos garantidos pela LGPD. Você deve estar preparado para atender a esses pedidos.

- **O que fazer:** crie um canal fácil para que seus clientes possam perguntar sobre seus dados, pedir para corrigi-los, excluí-los ou saber com quem você os compartilha. Isso será detalhado no tópico "Direitos e Deveres dos Titulares".

3 Ter um Ponto de Contato para LGPD

Mesmo que seu escritório seja pequeno, é fundamental ter alguém (que pode ser você mesmo ou um funcionário) responsável por lidar com assuntos relativos à LGPD. Essa pessoa será o "ponto focal" para dúvidas dos clientes e, se necessário, para atender a ANPD.

- **O que fazer:** Defina quem no escritório será o responsável pela LGPD. Essa pessoa deve conhecer a Lei e ser o contato principal para questões relacionadas a dados pessoais.

4 Agir Rápido em Caso de Problemas (Incidentes de Segurança)

Se acontecer um vazamento de dados ou qualquer incidente de segurança, você tem a responsabilidade de agir rapidamente.

- **O que fazer:** tenha um plano simples sobre como reagir se dados forem comprometidos. Isso inclui tentar conter o problema, investigar o que aconteceu e, se o risco for alto, comunicar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares afetados em até 72 horas.



5 Demonstrar que Está em Conformidade (Accountability)

A LGPD não exige apenas que você cumpra as regras, mas que seja capaz de provar que as cumpre. Isso é o princípio da "Accountability" ou Prestação de Contas.

- **O que fazer:** mantenha um registro e documente as medidas que você toma para proteger os dados. Guarde suas políticas internas, os treinamentos que você faz com sua equipe, e como você lida com as solicitações dos clientes. Essa documentação será sua prova em caso de fiscalização.

Ao entender e assumir essas responsabilidades, o(a) advogado(a) garante uma atuação ética, segura e em total harmonia com a LGPD, fortalecendo sua credibilidade e a confiança de seus clientes.

DIREITOS E DEVERES DOS TITULARES

Com base nos arts. 17 e 18 da LGPD, qualquer titular de dados — incluindo clientes — pode exigir do controlador (no caso, você ou o escritório):

- **Confirmação da existência de tratamento:** O cliente pode solicitar e obter uma resposta clara sobre se seus dados estão sendo tratados.
- **Acesso aos dados:** Direito de obter cópia das informações pessoais tratadas, os motivos e a forma de uso.
- **Correção:** Pode requerer atualização ou correção de dados imprecisos, incompletos ou desatualizados.
- **Anonimização, bloqueio ou eliminação:** Requerer tratamento indevido, excessivo ou desnecessário — inclusive quando o consentimento foi realizado, mas o tratamento deixou de ser legal.
- **Portabilidade:** Pode pedir transferência de seus dados a outro fornecedor/advogado(a) mediante requisição expressa.
- **Eliminação de dados tratados com consentimento:** Caso o cliente revogue o consentimento, pode solicitar exclusão, respeitados os prazos e bases legais contrárias.
- **Informação sobre compartilhamento:** Tem direito a saber com quais terceiros seus dados foram compartilhados.

- **Direito à não prestação ou revogação do consentimento:**
Pode se manifestar contra o tratamento sem violar outras bases legais, ou revogar consentimento dado anteriormente.

DEVERES DO ADVOGADO(A) / ESCRITÓRIO

A LGPD impõe obrigações específicas ao controlador — você — especialmente na preservação dos direitos acima:

1. Responder em até 15 dias

Para confirmação e acesso completos — prazo máximo legal.

2. Garantir atendimento claro, gratuito e acessível

Disponibilize canais eficientes para que os clientes façam solicitações sem barreiras técnicas ou custo.

3. Implementar políticas internas e fluxos de tratamento de dados

4. Adotar medidas técnicas e administrativas

A ausência dessas medidas infirma a boa-fé e aumenta o risco de responsabilização.

5. Nomear encarregado (DPO), quando aplicável

- Em escritórios maiores, ou com tratamento relevante, é recomendável a figura do DPO, atuando como canal com titulares e ANPD.
- Pequenos escritórios dispensam essa formalidade, mas devem manter canais acessíveis aos titulares.

6. Documentar todos os procedimentos

Em cumprimento ao princípio da *accountability*/responsabilidade, registre políticas, contratos, relatórios de impacto, treinamentos, consentimentos, incidentes etc.

7. Responder incidentes e exercer dever de transparência

Informar prontamente os titulares e a ANPD em caso de incidentes que representem risco — além de adotar medidas corretivas eficazes.

Pontos que merecem atenção:

Ao criar contratos ou procurações é uma boa ideia **incluir uma seção específica sobre consentimento**. Isso não apenas deixa claro como lidaremos com os dados, mas, também, estabelece uma base sólida para a confiança entre advogado(a) e cliente.

No dia a dia, é normal que os clientes queiram saber com quem compartilhamos seus dados. Por exemplo, eles podem perguntar sobre tribunais, empresas de software ou outros escritórios de advocacia. Se um cliente decidir mudar para outro(a) advogado(a), garantimos que eles possam levar seus dados consigo, embora devamos estar atentos(as) às **orientações futuras da ANPD, especialmente para empresas menores**.

É fundamental destacar que os direitos do titular de dados não podem ir de encontro às normas de outras leis que exigem a manutenção de informações específicas. Por exemplo, **o(a) advogado(a) pode se recusar a excluir dados de um cliente, colaborador ou parte contrária se houver uma lei que estipule um prazo para armazenamento, como acontece com obrigações trabalhistas, fiscais e previdenciárias, incluindo o e-Social, que dispensa o consentimento para a guarda desses documentos**.

É importante finalizar reforçando que o(a) advogado(a) ou escritório deve adotar medidas de segurança para garantir que seja o próprio titular de dados solicitando informações. Por exemplo, pode-se solicitar que o titular preencha um formulário específico e apresente um comprovante antes de fornecer os dados. No entanto, é recomendável evitar procedimentos excessivamente complicados e burocráticos. O objetivo é garantir a segurança sem tornar o processo demasiadamente complexo.

O QUE FAZER EM CASO DE INCIDENTE DE SEGURANÇA

A própria LGPD, no art. 48, prevê um mecanismo obrigatório nos casos de incidente de segurança com dados pessoais (como destruição, perda, alteração, vazamento ou qualquer forma de tratamento inadequado ou ilícito que possa gerar risco aos direitos e liberdades do titular). Esse mecanismo é conhecido como **DBN – Data Breach Notification**, ou seja, **notificação de violação de dados**.

Sempre que houver um incidente que envolva risco relevante, **será necessário notificar a ANPD** e o titular dos dados por meio de um documento específico.

Esse documento deve conter, no mínimo, as seguintes informações:

- Descrição da natureza dos dados afetados (se são dados gerais, sensíveis etc.);
- Informações sobre os titulares envolvidos (quais dados estão em risco: nome, CPF, telefone, e-mail etc.);
- Medidas técnicas e de segurança existentes antes do incidente (ex.: antivírus, backups, autenticação etc.), respeitando os segredos comercial e industrial;
- Avaliação dos riscos relacionados ao incidente;
- Justificativa da eventual demora na comunicação (caso não tenha sido imediata);
- Medidas que foram ou serão adotadas para reverter ou mitigar os prejuízos.



LINK do formulário oficial de comunicação de incidente (ANPD):

<https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis>



PRAZO PARA COMUNICAÇÃO (Resolução CD/ANPD nº 15 de abril de 2024)

- **Comunicação à ANPD:** a comunicação de incidente de segurança à ANPD deverá ser realizada pelo controlador no prazo de 3 (três) dias úteis, ressalvada a existência de prazo para comunicação previsto em legislação específica. O prazo é contado a partir do conhecimento pelo controlador de que o incidente afetou dados pessoais.
- **Complementação das informações:** as informações poderão ser complementadas, de maneira fundamentada, no prazo de 20 (vinte) dias úteis, a contar da data da comunicação.
- **Comunicação aos titulares:** a comunicação de incidente de segurança ao titular deverá ser realizada pelo controlador no prazo de 3 (três) dias úteis contados do conhecimento pelo controlador de que o incidente afetou dados pessoais.



BOAS PRÁTICAS PARA ADVOGADOS(AS)

Depois de entender suas responsabilidades e os conceitos da LGPD, a pergunta é: "Como coloco isso em prática no meu dia a dia?"

Este tópico é o seu guia com as boas práticas mais importantes e fáceis de implementar para garantir que seu escritório esteja em conformidade com a LGPD. São ações que, com um pouco de disciplina, farão uma grande diferença na segurança dos dados e na confiança dos seus clientes.

1 Conheça e Organize os Dados do Seu Escritório

Para proteger, primeiro você precisa saber quais dados têm e onde estão armazenados.

- **Faça um "Mapa" dos seus Dados:** Pense onde você guarda as informações dos clientes, colaboradores e casos. Está no seu computador? No celular? No e-mail? Em pastas físicas? Num software jurídico? Num serviço de nuvem (como Google Drive ou Dropbox)? Ter clareza sobre esses locais é o primeiro passo.
- **Guarde Somente o Essencial (Minimização):** Antes de coletar um dado, pergunte-se: "Eu realmente preciso dessa informação para o trabalho que vou realizar para o cliente?" Se a resposta for não, a coleta não se justifica, portanto: "não colete". Menos dados significam menos riscos.
- **Defina um Prazo para Guardar (Retenção):** Dados não são para sempre. Pense por quanto tempo você precisa manter as informações de um cliente após o fim do processo ou contrato. Se a Lei ou a finalidade não exigir mais, é hora de descartá-los.

- **Descarte Dados de Forma Segura:** Quando não precisar mais de um documento físico com dados pessoais, triture-o. Para arquivos digitais, apague da lixeira e, se possível, use ferramentas que garantam a exclusão permanente. Se estiver na nuvem, exclua de lá também.

2 Segurança no Dia a Dia: Proteger é um Hábito

A maioria dos incidentes acontece por descuido. Com alguns hábitos simples, você aumenta muito a segurança.

- **Senhas Fortes e Únicas:** Use senhas complexas (mistura de letras maiúsculas, minúsculas, números e símbolos) e diferentes para cada serviço importante (e-mail, software jurídico, banco etc.). Use um gerenciador de senhas se for difícil memorizar.
- **Autenticação de Dois Fatores (2FA):** Ative a autenticação de dois fatores sempre que possível (e-mail, redes sociais, sistemas do escritório). É uma camada extra de segurança que pede um segundo código (geralmente do seu celular) ao fazer login.
- **Antivírus e Softwares Atualizados:** Mantenha seu sistema operacional, antivírus e todos os softwares atualizados. As atualizações corrigem falhas de segurança que podem ser exploradas por criminosos.
- **Cuidado com Clicks Suspeitos:** Desconfie de e-mails, mensagens ou links estranhos. Não clique em nada que pareça duvidoso e nunca compartilhe senhas ou dados pessoais em resposta a essas mensagens.
- **Backup Regular dos Dados:** Faça cópias de segurança (backup) dos seus arquivos importantes regularmente. Guarde-as em um local seguro, preferencialmente na nuvem (com provedor confiável) ou em um HD externo criptografado.

- **Proteção Física do Escritório:** Lembre-se que dados físicos também precisam de proteção. Armazene documentos em armários trancados, não deixe papéis com informações sensíveis expostos e cuide da segurança das instalações (alarmes, câmeras).

3 Transparência e Comunicação com o Cliente

Seja franco(a) sobre como você trata os dados. Isso constrói confiança.

- **Política de Privacidade Simplificada:** Crie um texto curto e objetivo explicando como seu escritório coleta, usa e protege os dados dos clientes. Você pode ter um modelo padrão para entregar ao cliente, disponibilizar no seu site ou em um mural no escritório.
- **Crie um "Canal de Atendimento LGPD":** Indique um e-mail específico (ex.: privacidade@seuescritorio.com.br) ou um telefone para que os clientes possam fazer perguntas sobre seus dados, pedir correções ou solicitar exclusões. Responda a esses pedidos de forma rápida e clara.
- **Converse com o Cliente:** Durante a primeira conversa, explique brevemente por que você precisa de certos dados e como eles serão usados para o caso. É uma forma simples de demonstrar transparência.

4 Tenha um Ponto de Contato e Prepare Sua Equipe

A LGPD é um trabalho em equipe.

- **Seja o "DPO" do Seu Escritório (ou Indique Alguém):** Mesmo que você não precise de um DPO formal, decida quem será o "referencial" da LGPD no escritório. Essa pessoa (que pode ser você mesmo) deve ser a responsável por garantir que as boas práticas sejam seguidas e por tirar dúvidas.

- **Conscientize Sua Equipe:** Faça conversas rápidas e periódicas com estagiários, secretárias e outros(as) advogados(as). Explique a importância da LGPD, os riscos de um vazamento e as regras básicas de segurança. Incentive que qualquer dúvida ou incidente seja reportado imediatamente.
- **Cuidado ao Contratar Softwares e Serviços:** Ao contratar um software jurídico, serviço de armazenamento em nuvem ou qualquer outro prestador que terá acesso aos dados dos seus clientes, verifique se ele também está em dia com a LGPD e se oferece garantias de segurança. Peça um "contrato de tratamento de dados" ou verifique se há cláusulas sobre privacidade no contrato.

5 Documente o que Você Faz (para Provar que Faz)

A LGPD exige que você não só cumpra, mas que possa provar que cumpre.

- **Mantenha Registros Simples:** Não precisa ser um relatório gigante. Registre as medidas de segurança que você implementa, os treinamentos que faz com a equipe, as datas dos backups, e como você atendeu aos pedidos dos clientes sobre seus dados. Isso é sua prova de boa-fé e organização.

Ao adotar essas boas práticas, você estará construindo um escritório mais seguro, transparente e confiável. A conformidade com a LGPD é uma vantagem competitiva e um selo de profissionalismo na advocacia moderna.

- **Conscientize Sua Equipe:** Faça conversas rápidas e periódicas com estagiários, secretárias e outros(as) advogados(as). Explique a importância da LGPD, os riscos de um vazamento e as regras básicas de segurança. Incentive que qualquer dúvida ou incidente seja reportado imediatamente.
- **Cuidado ao Contratar Softwares e Serviços:** Ao contratar um software jurídico, serviço de armazenamento em nuvem ou qualquer outro prestador que terá acesso aos dados dos seus clientes, verifique se ele também está em dia com a LGPD e se oferece garantias de segurança. Peça um "contrato de tratamento de dados" ou verifique se há cláusulas sobre privacidade no contrato.

5 Documente o que Você Faz (para Provar que Faz)

A LGPD exige que você não só cumpra, mas que possa provar que cumpre.

- **Mantenha Registros Simples:** Não precisa ser um relatório gigante. Registre as medidas de segurança que você implementa, os treinamentos que faz com a equipe, as datas dos backups, e como você atendeu aos pedidos dos clientes sobre seus dados. Isso é sua prova de boa-fé e organização.

Ao adotar essas boas práticas, você estará construindo um escritório mais seguro, transparente e confiável. A conformidade com a LGPD é uma vantagem competitiva e um selo de profissionalismo na advocacia moderna.

GOLPE DO FALSO ADVOGADO SAIBA COMO FUNCIONA E COMO SE PROTEGER

O "golpe do advogado" é uma fraude cada vez mais comum no Brasil, na qual criminosos se passam por advogados(as) reais para enganar pessoas — sejam elas clientes ou não. Os golpistas usam nome, número da OAB, foto e, até, áudios clonados do profissional, colocando em risco a segurança das vítimas e a reputação do(a) advogado(a) envolvido.

COMO O GOLPE ACONTECE

1. Falso pagamento liberado – O golpista afirma que há valores disponíveis (ex.: precatórios, indenizações, FGTS), mas que, para recebê-los, é preciso pagar taxas ou honorários antecipados.

- **Exemplo:** “Seu precatório foi liberado. Deposite R\$ 3.200,00 hoje para receber R\$ 80.000 amanhã.”

2. Contato com pessoas que não são clientes – Usando dados vazados, os criminosos entram em contato com qualquer pessoa, mesmo que ela nunca tenha contratado o(a) advogado(a).

- **Exemplo:** “Bom dia, sou o Dr. João Ribeiro. Verificamos que seu CPF consta em uma ação coletiva com valor a ser recebido. Para liberar, basta confirmar seus dados.”

3. Perfis falsos nas redes sociais – Criam contas falsas no Instagram, Facebook ou WhatsApp com fotos e informações clonadas do(a) advogado(a) verdadeiro.

- **Exemplo:** O golpista cria um perfil com foto e nome do(a) advogado(a) real e começa a seguir os clientes, mandando mensagens privadas oferecendo “oportunidades” jurídicas.

4. Uso de deepfakes e clonagem de voz – Alguns golpes usam vídeos e áudios manipulados, tornando a fraude ainda mais convincente.

- **Exemplo:** O cliente recebe um áudio no WhatsApp com a voz clonada do(a) advogado(a) pedindo uma transferência urgente com número de conta bancária fraudulento.

CONSEQUÊNCIAS GRAVES

- Pessoas caem em golpes e perdem dinheiro.
- O(A) advogado(a) real pode ser injustamente responsabilizado ou denunciado à OAB.
- Pode haver danos à imagem profissional e até ações judiciais.

COMO O(A) ADVOGADO(A) PODE SE PROTEGER

- **Reforce a segurança digital** – Ative autenticação em duas etapas (2FA) em WhatsApp, e-mails e redes sociais; use senhas fortes; mantenha antivírus e backups atualizados.
- **Separe a vida profissional** – Use um celular exclusivo para o trabalho.
- **Comunique-se com clareza** – Inclua seus canais oficiais de contato nos contratos e redes sociais, use listas de transmissão e compartilhe dicas de segurança.
- **Crie uma senha verbal** – Combine com o cliente uma palavra-chave que só vocês conhecem. Exemplo: “escada vermelha”.
- **Monitore sua imagem online** – Use ferramentas como Hootsuite, Brand24 ou Mention para rastrear perfis falsos.



ORIENTAÇÕES PARA O CLIENTE

- Desconfie de mensagens pedindo dinheiro, especialmente por WhatsApp.
- Confirme sempre com o(a) advogado(a) pelos contatos oficiais.
- Consulte o nome do(a) advogado(a) no site da OAB: <https://cna.oab.org.br>
- Não forneça dados pessoais nem documentos a contatos não verificados.

FOI VÍTIMA DO GOLPE? O QUE FAZER

- 1. Colete provas** – Prints de mensagens, áudios, contatos usados, contas bancárias, nomes e fotos de perfis falsos.
- 2. Registre um boletim de ocorrência (B.O.)** – De preferência na Delegacia de Crimes Cibernéticos.
- 3. Comunique a OAB** – Informe a Seccional para registrar o caso.
- 4. Denuncie nas plataformas** – WhatsApp: Configurações > Denunciar contato. Redes sociais: Acesse o perfil > Denunciar > Perfil falso.
- 5. Considere uma ação judicial** – Para remover perfis falsos e exigir responsabilização.

DICAS FINAIS

- Advogados(as) devem educar seus clientes sobre como funciona o contato profissional.
- Manter presença digital oficial e atualizada reduz as chances de golpes.
- A prevenção é o melhor caminho: segurança, comunicação clara e atenção constante!

CONTEÚDO BÔNUS e links úteis



Chegamos ao final deste Guia e esperamos que ele tenha sido um passo importante para a sua jornada de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD). É inegável e urgente a necessidade de disseminar informações claras, capacitando advogados(as) a atuarem em total conformidade com a legislação de privacidade.

A implementação de boas práticas no tratamento de dados pessoais não é apenas uma exigência legal; é um diferencial estratégico. Ao atuar como Controlador de dados em consonância com a LGPD, você evita riscos significativos – desde multas administrativas pesadas, passando por ações civis, e em casos mais específicos, até responsabilidades penais. Mais do que isso, garante a proteção dos dados de seus clientes, adota meios robustos de segurança da informação e age com ética e transparência.

Fazer isso fortalecerá substancialmente sua reputação e construirá uma relação de confiança, ainda mais sólida, com seus clientes. Adequar-se à LGPD é uma responsabilidade jurídica que traz benefícios para todos!

Para auxiliá-lo(a) nesta empreitada e facilitar sua jornada rumo ao "compliance com a LGPD", disponibilizamos um material bônus e uma seleção de links úteis que servirão como fontes de consulta e ferramentas práticas.

Modelos de Documentos (Conteúdo Bônus)

Dentro do contexto deste Guia da OAB, você encontrará modelos de documentos essenciais para iniciar ou aprimorar a adequação do seu escritório à LGPD. Esses modelos são ferramentas práticas que podem ser adaptadas à sua realidade.

PACK - MODELOS DOCUMENTOS

Links Úteis

A seguir, uma compilação de links para documentos e páginas oficiais que são referências importantes na LGPD, diretamente da Autoridade Nacional de Proteção de Dados (ANPD) e do Planalto:

- **Guia Orientativo para Segurança da Informação (ANPD):** Um manual detalhado sobre as melhores práticas de segurança para proteger os dados pessoais.
- **Guia Orientativo sobre Cookies e Proteção de Dados Pessoais (ANPD):** Entenda como lidar com cookies em seu site ou plataformas, em conformidade com a LGPD.s.

[ACESSE AQUI](#)

[ACESSE AQUI](#)

- **Agenda Regulatória da ANPD:** Fique por dentro dos temas que a ANPD está priorizando para regulamentação, como a transferência internacional de dados e o legítimo interesse. Este é um recurso dinâmico e essencial para se manter atualizado.

[ACESSE AQUI](#)

- **Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018:** A íntegra da lei para consulta direta, fundamental para qualquer advogado.

[ACESSE AQUI](#)

- **Regulamento para Agentes de Tratamento de Pequeno Porte (Resolução CD/ANPD nº 2/2022):** Entenda as flexibilizações e regras específicas da LGPD para microempresas, empresas de pequeno porte, startups e pessoas físicas que tratam dados.

[ACESSE AQUI](#)

- **Guia Orientativo sobre Tratamento de Dados Pessoais e Legítimo Interesse (ANPD):** Um guia crucial para entender uma das bases legais mais complexas da LGPD.

[ACESSE AQUI](#)

- **Página Oficial da OAB São José do Rio Preto:** Mantenha-se conectado com a sua subseção para mais informações e iniciativas locais sobre LGPD e outras áreas do Direito.

[ACESSE AQUI](#)

