



Cartilha

LEI GERAL DE PROTEÇÃO DE DADOS PARA ESCRITÓRIOS DE ADVOCACIA





LEI GERAL DE PROTEÇÃO DE DADOS PARA ESCRITÓRIOS DE ADVOCACIA

OAB ALAGOAS

Presidente

Vagner Paes Cavalcanti Filho

Vice-Presidente

Natália França Von Sohsten

COMISSÃO DE INOVAÇÃO, TECNOLOGIA E PROTEÇÃO DE DADOS

DIRETORIA

Presidente

Nathalia Fernanda L. Cuellar Peixoto

Vice-Presidente

Junielle Mayara M. C. de Castro

Secretária-Geral

Ana Carolina de Almeida Salvador

Secretária-Adjunta

Ariane Ferreira Ferro

COORDENAÇÃO

Leticia Guedes Freire

MEMBROS

Alberto Alves de Melo Neves

André Ribeiro de Noronha

Gabriela Buarque Pereira Silva

Hannah Teixeira Oliveira Rangel

Isabelle de Melo Nolasco

Izaac Duarte de Alencar

Jéssica Caroline Ramos Correia

João Rafael Ribeiro Araújo

José Elio Ventura da Silva

Lilian Crystiane da Silva Cirino

Lucas José de Moura Carneiro

Maria Natali Oliveira Medeiros

Nathalia Maria Cardoso Aciole

Newton Cavalcante Souza

Pedro Marcelo da Costa Mota

Rafaella Louyse Sant'Ana dos Santos

Thulio Eduardo da Cruz Peixoto



SUMÁRIO

1. A importância da LGPD para os escritórios de advocacia	2
2. Cuidados na atuação.....	3
3. Aplicação das bases legais.....	4
4. O fluxo interno do escritório	6
5. Preparando sua equipe	9
6. Dicas de segurança	11



A presente cartilha é um documento informativo para fomentar a cultura de privacidade e proteção de dados pessoais e estimular os advogados a iniciarem o processo de adequação à LGPD dentro dos seus próprios negócios antes mesmo de prestar o serviço de orientação jurídica em proteção de dados aos seus clientes.

Todo plano deve ser encarado como um conjunto de medidas contínuas, a serem realizadas pelos agentes de tratamento. Enquanto as atividades do seu escritório estiverem ativas, o programa não tem fim. O monitoramento deve ser constante, pois sempre haverá novos serviços, processos internos serão modificados, novos colaboradores admitidos, novas sociedades se formarão, necessitando da adoção de práticas novas no processo.

QUEM SÃO OS AGENTES?

TITULAR

É toda pessoa natural a quem se referem os dados, como os clientes, associados, estagiários, colaboradores, testemunhas de processos, entre outros.

CONTROLADOR

É o sócio do escritório, a quem compete as decisões referentes ao tratamento de dados pessoais.

ENCARREGADO

É o responsável pela comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), é como um porta-voz do escritório, conhecido como Data Protection Officer (DPO).

OPERADOR

É a pessoa que realiza o tratamento dos dados em nome do controlador, podendo ser o advogado associado, estagiário, secretária e até mesmo colaboradores da área do TI ou marketing.





A IMPORTÂNCIA DA LGPD PARA ESCRITÓRIOS DE ADVOCACIA

Após identificar todos os atores para o processo de adequação, é preciso compreender que, dentre as inúmeras obrigações do nosso **Código de Ética e Disciplina da OAB**, temos o dever de proteger as informações privilegiadas que recebemos em função do exercício das atividades da advocacia, bem como resguardar o sigilo em depoimento judicial.

Dessa maneira, a obrigação de confidencialidade disposta com a LGPD chega com outra abrangência, a de proteger os direitos fundamentais de liberdade e privacidade do titular dos dados pessoais. Tal perspectiva não pode ser confundida com o sigilo profissional previsto nas regras da Ordem, visto que vai além do sigilo, trata-se de como são tratados esses dados pessoais, qual nível de segurança que os cercam e como eles podem participar do desenvolvimento da profissão.

Aplicam-se aos:

- ✓ Meios de comunicação (aplicativos e softwares de gestão);
- ✓ Divulgação do escritório (redes sociais, materiais impressos);
- ✓ Pastas físicas contendo documentos de clientes;
- ✓ Sistemas de segurança (física ou virtual).





CUIDADOS NA ATUAÇÃO

A LGPD exige que o profissional demonstre a adoção de todas as medidas possíveis em sua atuação, respeitando os princípios da lei e utilizando-se das tecnologias disponíveis para atingirem o mais próximo da conformidade. Além de implementar um **programa de gestão em governança em privacidade** em seu ambiente de trabalho, em que a organização e registro das atividades devem ser uma prioridade, é preciso se atentar aos seguintes pontos:



Sigilo e proteção das informações privilegiadas dos clientes (desde a primeira consultoria à finalização do processo, incluindo relatórios internos do escritório).



Utilizar-se de documentos preventivos, com cláusulas expressas sobre a LGPD, como Termo de Confidencialidade, contrato de prestação de serviços e um manual de políticas internas do escritório.



Para os serviços terceirizados ou realizados em parcerias com outros advogados, o cliente precisa estar previamente ciente desse compartilhamento. Dica: elaborar um termo de responsabilidade e sigilo com o profissional terceirizado.



A partir disso, seu ambiente deve ser alimentado pelos objetivos de negócios do escritório de advocacia e todas as execuções operacionais de rotina. É valioso planejar uma estratégia considerando a privacidade e proteção de dados, desmistificando a premissa de que estar em conformidade é só fazer alterações contratuais.

“**LGPD é muito mais que jurídico, é gestão!**”

Fique atento em todas as suas atividades, na elaboração de contratos, pareceres jurídicos, no curso de diligências e nas ações judiciais ou administrativas, em praticamente tudo haverá tratamento de dados pessoais. Na relação com seus colaboradores, prestadores de serviços terceirizados e parceiros, a LGPD estará presente. Não tem como fugir, **adeque seu escritório e continue atuando regularmente.**



APLICAÇÃO DAS BASES LEGAIS

Para iniciar a adequação de toda a documentação do escritório, é preciso se enquadrar às 10 possibilidades trazidas pelas bases legais contidas no **art. 7º** da LGPD, que vão muito além do consentimento do titular.

- Consentimento;
- Cumprimento de obrigação legal;
- Execução de política pública;
- Realização de estudos/pesquisa;
- Execução ou criação de contrato;
- Exercício regular de direitos;
- Proteção da vida;
- Tutela da saúde;
- Legítimo interesse;
- Proteção do crédito.



Nesse sentido, a base legal é caracterizada por ser uma justificativa capaz de **legitimar e autorizar** o tratamento de dados, de forma regulamentada. Mas como escolher a base legal mais adequada para a aplicação em seus contratos?

É recomendável que as cláusulas contratuais sejam inseridas levando em consideração as particularidades de cada caso. Por isso, trouxemos aqui, brevemente, algumas bases mais usuais nos casos dos escritórios de advocacia:



Execução ou criação de contrato

Os dados pessoais podem ser utilizados para executar ou preparar um contrato do qual o titular seja parte, a pedido do titular. Essa base, na maioria das vezes, será a mais utilizada pelos escritórios de advocacia, já que o tratamento de muitos dados pessoais é necessário para o cumprimento dos contratos com os clientes.

Exercício regular de direito

Prevê a hipótese de tratamento de dados por parte do controlador em situações que fazem parte de processos judiciais, administrativos ou arbitrais. O objetivo da base legal é permitir o acesso à justiça e consequentemente o direito à produção de provas entre as partes de um processo. Será a base mais utilizada pelo advogado.



Cumprimento de obrigação legal ou regulatória

É voltada para tratar os dados de acordo com as exigências de outras legislações vigentes, como a obrigação legal de entregar a Declaração de Imposto de Renda Retida na fonte (DIRF) relativo a seus funcionários.



BÔNUS: Legítimo interesse

É uma das bases legais mais genéricas e flexíveis previstas na LGPD. Essa autorizadora permite tratamento de dados quando este se fizer necessário para proteger o interesse de terceiros ou do controlador, desde que não sejam violados os direitos fundamentais e a liberdade do titular. Por isso, o legítimo interesse não pode ser utilizado para justificar o tratamento de dados pessoais sensíveis, pois, se este for o fundamento, a ANPD (órgão fiscalizador) pode solicitar ao controlador o relatório de impacto à proteção de dados pessoais.

Consentimento

Refere-se à permissão do titular de dados para que ocorra o tratamento para uma finalidade previamente informada, não podendo ser genérica, devendo a cláusula ser destacada e com finalidade específica. Por isso, é considerado um autorizador temporário, podendo ser revogado a qualquer momento, mediante manifestação expressa do titular. Portanto, recomenda-se a utilização de forma residual, quando não for possível enquadrar as outras bases legais, pois precisa estar posicionada de forma expressa, inequívoca, específica e livre.



O FLUXO INTERNO DO ESCRITÓRIO

Durante todo o fluxo interno, a lei exige que sejam mantidos os registros das atividades de tratamento de dados pessoais, registrando o funcionamento do ciclo de vida do dado pessoal. Esse exercício será feito em todas as atividades do escritório, na elaboração dos serviços, no departamento de marketing, sistemas, serviços terceirizados, entre outros.



É crucial que, após realizar o mapeamento de todos os tipos de dados pessoais coletados (através de planilhas ou softwares de gestão), o escritório elabore uma **política de retenção de dados**, isto é, organize internamente qual será o tempo de retenção dos dados coletados, de acordo com as demandas específicas do escritório, delimitando: quais são os dados coletados, quem são seus titulares, o período de retenção e o fundamento jurídico para a retenção destes dados.

Através do relatório de diagnóstico, compreendendo o risco e como será montado o plano de ação (etapas para a adequação), a implementação começará envolvendo toda a equipe do escritório simultaneamente, adequando **sistemas, documentos e processos**.



Lembrando sempre, que cabe ao **programa de governança**, analisar e determinar quais as necessidades de ações sistêmicas, particulares e que devem ser consideradas, para que qualquer incidente não derrube a estrutura de governança em privacidade.

Vejamos o passo a passo à seguir:



Importante lembrar que o tratamento dos dados pelo escritório não será para sempre, pois a Lei determinou, no art. 15, quatro hipóteses de **término do tratamento**, ressalvado pela autorização do art. 16, quando:

- A finalidade específica for alcançada ou os dados deixarem de ser necessários;
- Há o fim da prestação do serviço;
- O titular solicita a exclusão ou a revogação do consentimento (resguardado o interesse público); ou
- Houver determinação da ANPD.



PREPARANDO A SUA EQUIPE

Agora que você conhece as etapas necessárias que devem ter o tratamento de dados do escritório, trouxemos algumas recomendações para auxiliar a preparação da sua equipe e iniciar o programa de governança:

Invista em treinamento

Nomeie um encarregado de dados

Reforce a segurança

Estruture o Programa de Governança

Firme Termo de Confidencialidade

Monitore o seu trabalho



Conscientizar sobre a importância da proteção de dados pessoais é o primeiro passo para uma governança corporativa eficiente e consolidar boas práticas.

Nomear o **encarregado de dados** é essencial para criar um canal de comunicação eficiente e seguro.

Invista em **programas internos de integridade**, a fim de se evitar desgastes jurídicos, financeiros e, inclusive, à reputação do escritório

É essencial **mapear e identificar os riscos** existentes, bem como elaborar documentos acessórios, como: a política de privacidade, os aditivos nos contratos de trabalho e de honorários, entre outros.

A responsabilidade do controlador na proteção e sigilo dos dados coletados deve refletir na atuação dos agentes de tratamento - sócios, advogados, estagiários, secretários, colaboradores e parceiros, dessa forma a utilização do **termo de confidencialidade** é imprescindível.

É aconselhável sempre **revisar as práticas**, atualizar os treinamentos do time e planejar em conjunto a revisão e o melhoramento da gestão legal do escritório.



DICAS DE SEGURANÇA



Por fim, um destaque especial para os controles ou medidas de segurança, por serem ferramentas que gerenciam o risco com intuito de identificar e mitigar.

As senhas, os tokens e os certificados digitais são medidas, também chamadas de controles de segurança, que garantem a confidencialidade dos ativos de interesse, incluindo-se, neste escopo, os dados pessoais. Diante disso, é importante estar sempre atento às seguintes medidas:





LGPD PARA ESCRITÓRIOS DE ADVOCACIA



Senhas e tokens

- Não compartilhe senhas e tokens;
- Ative a autenticação por dois fatores;
- Limite o acesso ao banco de dados de cada setor do escritório;



Sistemas e redes

- Sempre utilize sistemas operacionais originais e atualizados (Windows, MacOS ou Linux);
- Instalar e atualizar softwares de antivírus e antimalwares;
- Realizar periodicamente o backup dos dados relevantes;
- Utilizar canais seguros para comunicação externa, utilizando a tecnologia de VPN (rede virtual privada);
- Não conectar e utilizar redes públicas/abertas para realizar downloads ou envio de dados e documentos do escritório.



Armazenamento e descarte

- Utilize tecnologia de criptografia para proteção dos arquivos sigilosos e importantes, tanto para o armazenamento quanto o envio;
- Descarte os documentos físicos apropriadamente (picotamento ou incineração);
- Se o documento for digitalizado e não mais necessário mantê-lo, devolva ao cliente.



Segurança da informação

- Estruturar um sistema integrado de gestão de risco em segurança da informação, para gerenciar incidentes, vazamento de dados e realizar gestão de crise;
- Contratar um profissional em Segurança da Informação para auxiliar na criação, monitoramento e documentação de um Sistema de Gestão de Segurança da Informação (SGSI);
- Treinamento constante de todos que compõem os quadros do escritório para conscientização sobre Segurança da Informação;
- Se houver um incidente, alerte às partes interessadas o que houve e quais impactos isso pode resultar, bem como quais medidas serão adotadas para conter, erradicar e recuperar o controle da situação.



Portanto, o protocolo de adequação precisará ser formado de acordo com a realidade e a obrigação de cada atividade exercida pelos profissionais em cada etapa ou ação acima, que deve ser estabelecida na **Política de Segurança da Informação**



MENSAGEM DA COMISSÃO

A presente cartilha procurou abordar os aspectos principais acerca da parte prática da implementação da Lei Geral de Proteção de Dados nos escritórios de advocacia.

A Lei nº 13.709/2018 veio para garantir que toda a sociedade tenha seus direitos fundamentais de liberdade e de privacidade protegidos, já que os dados são os ativos intangíveis mais valorizados na atualidade. Na Era do capitalismo de vigilância, agir de forma preventiva é o primeiro passo.

Desta forma, esperamos que você, advogado, inicie o quanto antes a implementação do programa de adequação à LGPD no seu ambiente de trabalho, criando uma cultura de proteção de dados no seu escritório. Não seja um apagador de incêndios!

Por isso, indicamos que os envolvidos na adequação do escritório estudem, se qualifiquem, para que possam se aprofundar no tema, fazer a sua implementação e ainda poder orientar seus clientes

Start nas adequações!

