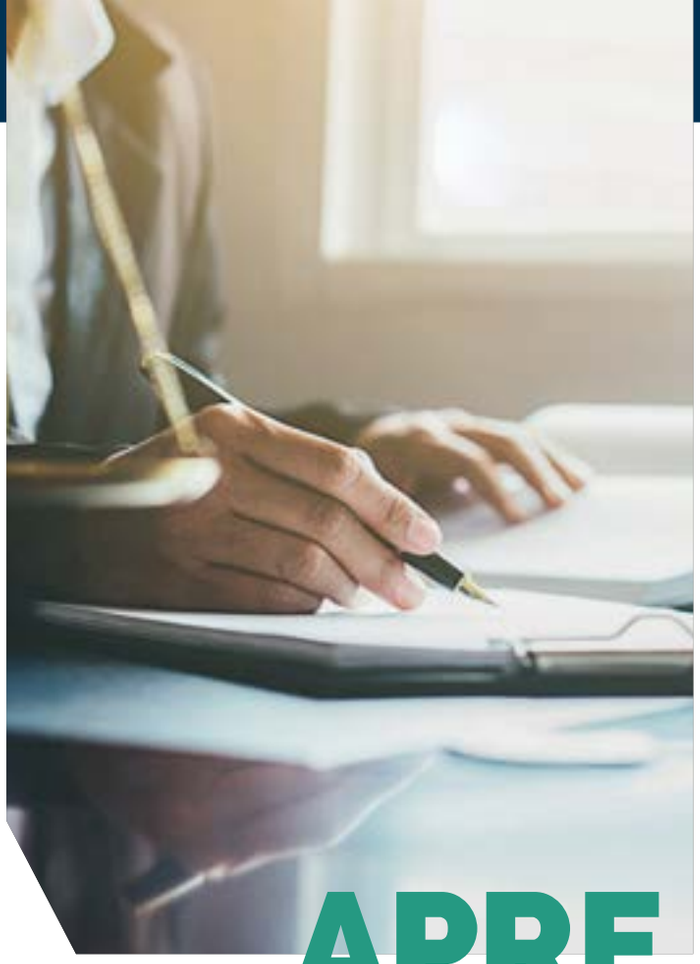
Guia da **LGPD** na Advocacia

SUMÁRIO



APRESENTAÇÃO

A LGPD e os escritórios de Advocacia

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), também conhecida como “LGPD”, é a primeira norma a regular, de maneira exclusiva e centralizada, o tema da privacidade e proteção de dados no Brasil. Ao contrário do senso comum, ela não se aplica somente a empresas de ramos específicos, mas sim a todos aqueles que, em alguma medida, tratam dados pessoais para fins econômicos — o que inclui os escritórios de Advocacia.

Para a área da Advocacia, é especialmente importante e desafiador estar em conformidade com a nova regulação. Não apenas por falarmos de operadores do direito mas, também, pelo fato de a Advocacia ser uma área centrada no uso de dados pessoais no seu cotidiano, independentemente do campo de atuação do escritório. São informações pessoais relativas a clientes, processos, contratos, colaboradores, prestadores de serviço, entre tantos outros.

Por isso, todo o processo de adequação deve levar em consideração todos esses fatores, a fim de estabelecer uma rota apropriada para um gerenciamento mais seguro, transparente e eficiente desses dados pessoais.

Pensando no contexto especial da Advocacia, apresentamos, em parceria com o escritório Opice Blum, Bruno e Vainzof Advogados Associados, este Guia da LGPD na Advocacia, com orientações gerais sobre como conduzir o processo de adequação do seu escritório de Advocacia à LGPD.

Todas as orientações aqui contidas são baseadas em aspectos tanto regulatórios quanto práticos na condução de processos de adequação à LGPD. Assim, este Guia não pretende ser um material exaustivo ou definitivo, visto que a própria regulação de proteção de dados no Brasil está em constante evolução e a Autoridade Nacional de Proteção de Dados vem trabalhando arduamente para regulamentar suas lacunas. Por isso, é altamente aconselhável utilizar estas orientações em caráter recomendatório, sempre considerando as especificidades do contexto em que seu escritório está inserido (porte, área de atuação, entre outros fatores).

Boa leitura!

Aspectos Gerais e Definições Essenciais

Aspectos gerais e principais conceitos da LGPD

APLICAÇÃO MATERIAL

A Lei incide apenas sobre as informações relativas a **uma pessoa natural identificada ou identificável** (art. 1º).

Ou seja, a proteção da Lei **não se estende** a dados de pessoas jurídicas, documentos sigilosos ou confidenciais, segredos de negócio, planos estratégicos, algoritmos, fórmulas, patentes ou outros documentos e informações que não sejam estritamente relacionados a dados pessoais.

DEVER DE OBSERVAÇÃO

A lei deverá ser observada por pessoas físicas ou pessoas jurídicas (de direito público ou privado) que tratem dados pessoais (art. 3º, caput).

SUPORTE DOS DADOS

Os dados pessoais protegidos podem estar inseridos tanto em meios físicos (armário e fichário, por exemplo) como em meios digitais (rede) (art. 1º).

APLICAÇÃO TERRITORIAL

Aplica-se sempre que o tratamento de dados pessoais for **realizado no território brasileiro** ou se a atividade envolver **oferecimento de produtos ou serviços** a pessoas que se encontram no território nacional ou, ainda, se os dados pessoais tiverem sido **coletados em território nacional** (art. 3º).

VIGÊNCIA E SANÇÕES

A LGPD está em vigor desde 18 de setembro de 2020 (art. 65, II) e suas sanções administrativas entrarão em vigor em **1º de agosto de 2021** (art. 65, I–A).

REGULAMENTAÇÃO POSTERIOR

Alguns pontos relevantes da lei serão regulamentados pela ANPD em breve (Portaria nº 11, de 27 de janeiro de 202).

Exceções à aplicação da LGPD

Nos termos do art. 4º da LGPD, as disposições da Lei não são aplicáveis às seguintes hipóteses:

- Tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos (art. 4º, I)
- Dados provenientes de fora do território nacional, que não sejam objeto de comunicação ou uso compartilhado de dados com agentes de tratamento brasileiros (art. 4º, IV)
- Tratamento de dados pessoais realizado para fins exclusivamente jornalísticos e artísticos, ou acadêmicos (art. 4º, II)
- Tratamento realizado em prol da segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, III)
- Dados provenientes de fora do território nacional, que forem objeto de transferência internacional com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (art. 4º, IV)

Fundamentos e princípios legais

Fundamentos

A LGDP possui os seguintes fundamentos (art. 2º):

- Respeito à privacidade
- Autodeterminação informativa
- Liberdade de expressão, de informação, de comunicação e de opinião
- Inviolabilidade da intimidade, da honra e da imagem
- Desenvolvimento econômico e tecnológico e inovação
- Livre iniciativa, livre concorrência e defesa do consumidor
- Direitos humanos e livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais

Princípios
LPGD,art. 6º

- **Boa fé**
- **Finalidade**: os dados somente deverão ser tratados para propósitos legítimos, específicos explícitos e informados aos titulares de dados pessoais
- **Adequação**: compatibilidade entre os dados utilizados e as finalidades do tratamento
- **Necessidade**: minimização dos dados. Utilização dos dados estritamente necessários para determinada finalidade
- **Qualidade dos dados**: os dados tratados deverão ser claros, exatos, relevantes e atualizados
- **Transparência**: acesso facilitado, pelo titular, a informações pertinentes ao tratamento de seus dados
- **Segurança**: adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais
- **Prevenção**: adoção das medidas razoáveis ao alcance do controlador para prevenir o tratamento inadequado de dados e eventuais danos aos titulares
- **Livre Acesso**: garantia aos titulares do acesso a informações sobre o tratamento e à integralidade dos dados
- **Não discriminação**: não utilização dos dados para fins discriminatórios, ilícitos ou abusivos
- **Responsabilização e prestação de contas**: demonstração da adoção de medidas eficazes ao cumprimento das normas de proteção de dados

Espécies de dados pessoais

Dados pessoais “simples”(art. 5º, I)

Qualquer informação que identifique uma pessoa natural ou que possa levar a sua identificação. Por exemplo: CPF; Título de Eleitor; Número de inscrição na OAB; RG; Nome; Hábitos de Consumo; Profissão; Sexo; Idade; entre outros.

Dados pessoais sensíveis (art. 5º, II)

Dados sobre origem racial ou étnica; saúde, vida sexual; genética; biometria; religião; opinião política; informações sobre filiação a sindicato ou a organização de caráter religioso, filosófico ou político. Vale ressaltar que dado pessoal inferido também recebe o mesmo tratamento do dado pessoal sensível. Essa é a hipótese, por exemplo, quando a partir dos hábitos de consumo pode-se inferir dados sobre saúde ou religião.

Dado anonimizado

Dado relativo a titular que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento.
Por não identificar um indivíduo, não é dado pessoal para os fins da LGPD.

Dado pseudonimizado

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

Agentes de tratamento

CONTROLADOR

- Pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.
- Determina as finalidades e os meios de tratamento dos dados pessoais e é o responsável pelo enquadramento das atividades de tratamento nas bases legais adequadas.
- É possível a controladoria conjunta, quando mais de um controlador estiver envolvido no tratamento de dados para atingir finalidades comuns (Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, p. 12).

OPERADOR

- Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador.
- Embora detenha certa discricionariedade para execução de tarefas no escopo de sua atuação, não possui competência decisória sobre os elementos essenciais do tratamento de dados pessoais.

SOBRE EMPREGADOS E PREPOSTOS DOS AGENTES DE TRATAMENTO

- Não são considerados agentes de tratamento autônomos — isto é, controladores ou operadores — os indivíduos colaboradores, funcionários, servidores, sócios, administradores e outras pessoas naturais que atuarem em subordinação ou integrarem a pessoa jurídica, controladora ou operadora. Os colaboradores, em geral, atuam como parte do agente de tratamento, e não de maneira independente em relação a ele.

RESPONSABILIDADES DOS AGENTES DE TRATAMENTO

- A responsabilidade será determinada de acordo com o papel exercido pelo agente de tratamento no âmbito das atividades de tratamento dos dados pessoais.
- **Responsabilidade solidária do Operador (LGPD, art. 42, § 1º, I)** é prevista para casos de danos causados em razão de tratamento irregular realizado por operador ao descumprir as obrigações da Lei ou por não observar as instruções lícitas do controlador.

Na medida em que, em razão da natureza de determinada atividade, um escritório de Advocacia tiver autonomia e independência na atividade de tratamento de dados pessoais para o desempenho de suas funções, ele figurará como Controlador.

Hipóteses Permissivas de Tratamento de Dados

A LGPD não proíbe o tratamento de Dados Pessoais, mas limita a algumas hipóteses previstas nos artigos 7º e 11

Para Dados Pessoais (art. 7º)

Dentre as 10 bases legais permissivas para o tratamento de Dados Pessoais (art. 7°, I a X), destacamos:

- Consentimento (art. 7°, I);
- Cumprimento de obrigação legal ou regulatória (art. 7°, II);
- Execução de um Contrato ou procedimentos preliminares ao contrato (art. 7°, V);
- Exercício regular de direitos em processos judiciais, administrativos ou arbitrais (art. 7°, VI);
- Atendimento aos interesses legítimos do controlador ou de terceiro (art. 7°, IX).

Para Dados Pessoais Sensíveis (art. 11)

Dentre as 08 bases legais permissivas para o tratamento de Dados Pessoais Sensíveis (art. 11, I e II), destacamos:

- Consentimento (art. 11, I);
- Cumprimento de obrigação legal ou regulatória (art. 11, II, a);
- Exercício regular de direitos, inclusive em contrato (art. 11, II, d);
- Garantia da prevenção à fraude e à segurança do titular (art. 11, II, g).

Para Dados de crianças e adolescentes (art. 14)

Regra Geral: O tratamento de dados de crianças e adolescentes deve ser realizado em seu melhor interesse (art. 14, caput);

- Dados de crianças (12 anos incompletos): necessário o consentimento de um dos pais ou responsável legal (art. 14, § 1º).
- Consentimento: deverá ser livre, informado, inequívoco, específico e em destaque;
- Transparência: deve ser exercida de forma simples, clara e acessível (art. 14, § 6º).

Exceção: O consentimento para tratamento de dados de crianças não precisará ser coletado quando: a coleta for necessária para contatar os pais ou o responsável legal; os dados forem utilizados uma única vez e sem armazenamento; os dados forem utilizados para proteção da criança; os dados não forem compartilhados com terceiros (art. 14, § 3º).

Direitos dos Titulares de Dados

O controlador deverá viabilizar que o titular obtenha, de forma gratuita:

- Confirmação da existência do tratamento (art. 18, I);
- Acesso aos dados (art. 18, II);
- Correção de dados incompletos, inexatos ou desatualizados (art. 18, III);
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (art. 18, IV);
- Portabilidade dos dados (art. 18, V);
- Eliminação dos dados tratados com o consentimento (art. 18, VI);
- Informação das entidades públicas e privadas com as quais os dados foram compartilhados (art. 18, VII);
- Informação sobre a possibilidade de não fornecer consentimento (art. 18, VIII);
- Revogação do consentimento (art. 18, IX);
- Revisão das decisões automatizadas (art. 20).

Considerações Adicionais:

- O Controlador poderá deixar de prover o direito do Titular se: (i) não for agente de tratamento responsável; (ii) por outras razões razoáveis e justificáveis (art. 18, § 4º)
- As respostas para as solicitações de confirmação da existência do tratamento e acesso aos dados tratados devem ser oferecidas de forma imediata, quando em formato simplificado, ou no prazo de até 15 dias (art. 19, II);
- Quanto aos demais direitos, a lei não especificou os prazos para atendimento.
  No momento, estima-se que a ANPD publicará orientações ou regulamentações mais específicas no segundo semestre de 2022.

Segurança e Boas Práticas

Segurança

- Os agentes de tratamento devem adotar medidas de segurança técnica e organizacional razoáveis (Art. 46, caput);
- A LGPD não dispõe sobre quais padrões de segurança são considerados razoáveis. A ANPD regulamentará a questão (Art. 46, § 1º);
- Incidentes de Segurança: podem ser entendidos como acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de dados pessoais.

Caso o Incidente acarrete em risco ou dano relevante ao titular, o Controlador deverá notificar a ANPD e ao titular afetado (art. 48), em prazo razoável conforme regulamentado pela ANPD. Atualmente, a ANPD recomenda o prazo de 2 dias úteis.

Boas práticas

Os Agentes de Tratamento deverão:

- Adotar um Programa de Governança em Privacidade e Proteção de Dados condizente com o art. 50, § 2º, I, com a implementação de Políticas e Procedimentos que o evidenciem;
- Demonstrar a efetividade do Programa de Governança em Privacidade e Proteção de Dados (Art. 50, § 2º, II);
- Evidenciar as medidas de segurança adotadas;
- Assegurar que seus Operadores (ou sub-operadores) atuem com segurança, confidencialidade e que esteja em conformidade com as obrigações contratuais e legais;
- Assegurar que os dados serão tratados em respeito aos princípios consagrados, e pelo prazo que for necessário ao alcance das finalidades pretendidas (Art. 16).

Sanções administrativas

A aplicação das sanções administrativas é uma das competências da Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República (art. 55-A). Estas sanções entrarão em vigor em 1º de agosto de 2021 (art. 65, i-A)

O art. 52 da LGPD traz como sanções administrativas:

- advertência (art. 52, I);
- multa de até 2% do faturamento, limitada a R$ 50.000.000,00 por infração (art. 52, II);
- multa diária (art. 52, III);
- publicização da infração (art. 52, IV);
- bloqueio dos dados até a regularização (art. 52, V);
- eliminação dos dados (art. 52, VI);
- suspensão parcial do funcionamento do banco de dados por 6 meses prorrogáveis por igual período até a regularização da atividade (art. 52, X);
- suspensão da atividade de tratamento de dados por 6 meses prorrogáveis por igual período (art. 52, XI);
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (art. 52, XII).

Metodologia para aplicação das sanções

ANPD regulamentará a metodologia para cálculo do valor base das sanções pecuniárias (art. 53). Espera-se que a regulação seja publicada ainda este ano, conforme a agenda regulatória da ANPD (Portaria nº 11, de 27 de janeiro de 2021).

A ANPD considerará os seguintes parâmetros e critérios na aplicação da multa:

- gravidade e natureza das infrações;
- boa-fé e cooperação do infrator;
- vantagem obtida com a infração;
- condições econômicas do infrator;
- reincidência e gravidade do dano causado;
- adoção de mecanismos e procedimentos internos de proteção de dados;
- adoção de política de boas práticas e governança;
- pronta adoção de medidas corretivas;
- proporção entre a gravidade da infração e a intensidade da sanção.

A LGPD no dia a dia do escritório

O tratamento de dados pessoais está presente em muitas atividades do cotidiano do escritório de Advocacia. Com a vigência da LGPD, todas elas, em alguma medida deverão passar por algum tipo de conformidade ou adaptação. Veja, a seguir, alguns exemplos de atividades relativamente comuns e quais medidas geralmente são necessárias para adequá-las à LGPD:

Prospecção de clientes

Sendo uma as atividades mais comuns e importantes para o negócio dos escritórios, a prospecção de clientes necessita, entre outros aspectos, de uma base legal adequada. Para os titulares de dados, é altamente recomendado adotar medidas de transparência e garantir o opt-out, caso o indivíduo não deseje mais receber comunicações do escritório.

Relação com os colaboradores

Os colaboradores, independentemente do seu modelo de contratação, são titulares de dados. Para que eles tenham visibilidade sobre como o escritório trata seus dados, é necessário ter um Aviso Interno de Privacidade, bem como realizar treinamentos de advogadas, advogados e colaboradores sobre as práticas de proteção de dados do escritório.

Relação com os clientes

Os contratos celebrados com clientes devem ter atenção especial no processo de adequação do escritório, sobretudo se há dados pessoais (i.e. informações de pessoas físicas) envolvidos. Entre outras medidas relevantes, será necessário incluir cláusulas de proteção de dados e procedimentos para definir os papéis de agentes de tratamento (controlador ou operador) desempenhados por cada uma das partes.

Boletins, newsletters, clippings e afins

Muitos escritórios mantêm o envio de e-mails com notícias e eventos relevantes para seus clientes. Esta atividade necessita de uma base legal adequada (geralmente o consentimento ou o legítimo interesse), bem como de medidas de transparência. A depender do caso, também é importante prover mecanismos de opt-in ou opt-out eficientes.

Arquivo morto e bases de dados

É comum que os escritórios acumulem anos de processos e contratos, repletos de dados pessoais. Para maior segurança dos titulares e do próprio escritório, recomenda-se que esses arquivos e bases de dados sejam saneados periodicamente, para evitar o acúmulo de dados desnecessários. Uma política de retenção de dados ajuda a determinar por quanto tempo os dados devem ser mantidos.

Novas contratações e banco de talentos

Nos novos contratos, é importante incluir nos novos contratos cláusulas de proteção de dados e promover onboardings e treinamentos sobre as práticas de proteção de dados do escritório. Caso o escritório mantenha um banco de talentos, recomenda-se que esta base de dados também seja saneada regularmente.

A seguir abordaremos como estes pontos podem ser endereçados de maneira sistematizada, por meio do Processo de Adequação

O processo de adequação

Em um olhar: **o que muda e o que permanece?**

MUDA

Atendimento/Relacionamento com os Titulares (clientes, sócios/as, advogados/as, funcionários/as, dentre outros)

- Todos os dados pessoais precisarão ser tratados de forma compatível com a nova legislação;
- Deve ser observada a garantia de transparência ao titular dos dados com relação a tratamento de seus dados;
- Devem ser oferecidas informações claras, adequadas e facilmente acessíveis acerca do tratamento, como por exemplo: a finalidade do tratamento; sua forma e duração; a identificação do controlador e seu contato; o eventual uso compartilhado de dados e quais as finalidades desse compartilhamento; as responsabilidades dos agentes que realizarão o tratamento; os direitos atribuídos pela LGPD aos titulares (art. 9°);
- Deve ser disponibilizado aos titulares de um canal facilitado, sem custo, para encaminhar requisições relacionadas aos seus direitos garantidos pela LGPD.

Em um olhar: **o que muda e o que permanece?**

MUDA

Atividades envolvendo tratamento de dados pessoais

- As atividades de tratamento dos dados deverão ser identificadas e registradas pelos escritórios, com o objetivo de garantir que estejam aderentes aos princípios da LGPD e fundamentadas em uma das hipóteses autorizadoras do tratamento;
- Procedimentos e políticas internas deverão ser implementados para garantir que o tratamento de dados pessoais nas atividades realizadas pelos escritórios esteja aderente às regras da legislação e regulamentação sobre o tema.

Integração entre as áreas do escritório (jurídico, tecnologia e administrativo)

- A necessidade de tratamento multidisciplinar sobre o tema, mais do que nunca, tornará imprescindível a integração dos corpos jurídico, de tecnologia, administrativo e pessoal, para mitigar os riscos de eventuais infrações da LGPD que possam impactar negativamente o escritório.

Em um olhar: **o que muda e o que permanece?**

PERMANECE

- O dever de confidencialidade dos escritórios em relação às informações que venham a ter acesso em decorrência de suas atividades.

> “O Sigilo profissional é inerente à profissão, impondo-se o seu respeito [...]” (Art. 25, Código de Ética, OAB).

- Zelo no trato de quaisquer dados pessoais que possam ser tratados, incluindo, mas não se limitando, dados pessoais de clientes.

> “(...) proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (art. 1º, LGPD)

O que precisa ser feito?

A seguir, listaremos as principais medidas abordadas no Processo de Adequação. Elas não estão em alguma ordem específica, portanto, podem ser adotadas pelo escritório na ordem de sua conveniência, ou que melhor se adapte ao seu contexto. Não obstante, é altamente recomendado implementá-las integralmente até o final do processo.

1

Implementação de uma estrutura de governança em privacidade e proteção de dados adequada às atividades do escritório, de acordo com suas suas características e prioridades, incluindo a constituição de um Comitê de Privacidade e a nomeação de um Encarregado, na hipótese de ainda não tê-lo;

2

Mapeamento das atividades de tratamento ou atualização do mapeamento pré-existente, atribuindo as bases legais que autorizem o tratamento dos Dados Pessoais e identificando possíveis pontos de desconformidade das atividades em relação aos princípios legais;

3

Avaliação do nível de maturidade dos processos internos existentes em relação ao cumprimento da LGPD;

4

Identificação dos riscos apurados nas atividades de tratamento e na avaliação do nível de maturidade do Programa de Governança em Privacidade do escritório;

O que precisa ser feito?

5

Preparativos internos: criação ou revisão de políticas e procedimentos para a formalização do Programa de Privacidade, considerando as características do escritório e as peculiaridades das atividades de tratamento de dados pessoais realizadas;

6

Criação de canais de comunicação que uma vez divulgados, possam concentrar o atendimento aos titulares de dados e órgãos reguladores competentes;

7

Criação de materiais orientativos e de conscientização de sócios, advogadas e advogados associados e colaboradores;

8

Treinamentos para a capacitação e reciclagem, de tempos em tempos, para sócios, advogadas e advogados associados e colaboradores que estarão incumbidos do tratamento de dados pessoais;

8

Estabelecimento de um roteiro de monitoramento constante, que ditará as regras para as atualizações do programa de governança e privacidade, reavaliação do nível de maturidade dos processos internos, acompanhamento da implementação das medidas mitigatórias de riscos e das atividades de tratamento e sua adequação ao que dispõe a LGPD.

Panorama geral do Processo

Treinamento
Capacitação das áreas envolvidas

Mapeamento
Identificar os procedimentos que utilizam dados pessoais

Maturidade e avaliação
Análise de maturidade e posterior verificação dos riscos atuais

Plano de ação
Medidas para corrigir os riscos mitigados

Implementação
Implementação do Plano de Ação e revisão constante

Processo sob medida
Antes que se inicie o processo de adequação, é necessário avaliar, entre outros aspectos relevantes: o porte do escritório, o escopo de suas operações, o perfil de seus clientes e fornecedores.

Engajamento da alta liderança
A maneira mais eficiente de se implementar o processo de adequação é com o envolvimento de todos, inclusive sócios e demais responsáveis pela administração e direção do escritório. Para além de estarem sujeitos às novas regras, os membros da alta liderança também têm papel fundamental nas decisões sobre como implementar tais regras da maneira mais adequada para o escritório.

Capacitação dos colaboradores envolvidos
O processo de adequação é complexo e necessita do comprometimento de todos os envolvidos para que seja conduzido de maneira eficiente e tempestiva. O objetivo destas sessões iniciais de capacitação é mostrar aos colaboradores qual será seu papel (por exemplo, como preencher os formulários de mapeamento, as características das operações relevantes para adequação, entre outros). Além disso, mesmo após a etapa de adequação, tudo o que for construído e implementado deverá permanecer e serão os colaborados e demais membros do escritório responsáveis para garantir a aderência à cultura de proteção de dados e o funcionamento correto do Programa de Privacidade do escritório.

O Processo de Adequação

PREPARATIVOS | TREINAMENTO | AVALIAÇÃO | PLANO DE AÇÃO

Nomeação de um Encarregado e criação de Comitê Interno de Privacidade e Proteção de Dados

- O Comitê será responsável pelas tarefas exigidas para um plano de implementação, incluindo a classificação das informações, a revisão dos provedores de tecnologia, a definição das políticas de comunicação e tratamento de dados, bem como a utilização das medidas razoáveis de segurança.
- Idealmente, será formado por um ou mais sócios (a depender do tamanho do escritório) e representantes das principais áreas envolvidas no tratamento de dados, como as de TI e de RH.
- Será necessário definir uma equipe multidisciplinar para o desenvolvimento e implementação do projeto de adequação.

Sobre o Encarregado ou DPO (Data Protection Officer)
A Lei determina a obrigação de nomear um Encarregado, bem como, a depender do tamanho do escritório, uma equipe que lhe dê suporte. O Encarregado precisa ter autonomia no desempenho de suas funções e ser independente perante as demais áreas do escritório, inclusive em relação à Diretoria Executiva. Devem ser evitado o acúmulo de funções capazes de gerar conflitos de interesses (art. 41).

Identificação das áreas internas

- Será necessário identificar as partes e áreas internas que tratam ou têm interesse em tratar dados pessoais. Este estudo não precisa ser aprofundado, mas deve ser abrangente o suficiente para abarcar todas as áreas do escritório em que, em alguma medida, há tratamento de dados pessoais. Em geral, quando se fala de escritórios de Advocacia, serão muitas, senão todas as áreas do escritório, tais como: Jurídico, Administrativo, Financeiro, Contato com Cliente, Gestão de Pessoas, TI, Compliance, entre outras.

Aspectos regulatórios

- O Comitê de Proteção de Dados deverá efetuar um estudo regulatório de todas as normas relevantes para o âmbito de atuação do escritório, tanto no trato dos clientes, quanto para com seus colaboradores e fornecedores.

- **Sobre a ANPD.** Muitos pontos importantes sobre a aplicação da ANPD serão regulados pela Autoridade Nacional de Proteção de Dados. Recentemente, a Autoridade divulgou sua agenda regulatória para o biênio de 2021-2022, com ênfase para temas como regulação do tratamento para pequenas e médias empresas, diretrizes para definição dos papéis de agentes de tratamento e procedimentos de notificação e resposta a incidentes de dados pessoais. Até lá, as únicas exceções de aplicabilidade foram abordados anteriormente neste Guia.

Capacitação das áreas envolvidas no processo de adequação

- Para otimização do processo, recomenda-se conduzir sessões de treinamento (realizados de forma periódica) e conforme Política de Treinamentos e Capacitação para colaboradores e áreas relacionadas ao tratamento de dados pessoais com o objetivo de tornar a jornada de adequação mais eficiente.

Escopos da capacitação. Idealmente, as sessões de treinamento terão dois escopos:

no curto prazo, orientar os colaboradores sobre seu envolvimento no processo de adequação (por exemplo, como preencher os formulários das operações de tratamento de sua respectiva área);

no médio e longo prazo, instruir os colaboradores sobre as novas políticas que serão implementadas com a adequação à LGPD.

Análise de maturidade dos processos internos

- **Identificação das atividades de tratamento de dados.** É o que comumente chamamos de Mapeamento de Dados. O escritório deverá identificar e registrar as atividades de tratamento de dados que realiza. É importante a construção dessa documentação para que seja possível atribuir as bases legais adequadas para cada atividade, identificar possíveis pontos de desconformidade e realizar análises de risco. A manutenção e atualização periódica deste mapeamento permitirá o monitoramento regular de tais atividades, a fim de garantir a conformidade com as regras de proteção de dados e a eficácia do Programa de Privacidade.
- **Verificação prévia do nível de adequação necessária.** Ao realizar uma análise preliminar das operações envolvidas, bem como a capacitação prévia dos colaboradores envolvidos, é possível identificar o nível atual de adequação do escritório à LGPD e os principais pontos de desconformidade que demandarão um plano de ação específico.

Programa de Governança em Privacidade e Proteção de Dados

De forma exemplificativa, portanto, não exaustiva, inserido no Plano de Ação deverão estar:

- **Verificação dos contratos firmados com terceiros.** Recomenda-se revisar os contratos firmados com terceiros, incluindo clientes e prestadores de serviços, para averiguar se possuem cláusulas relacionadas a proteção de dados e, simultaneamente, criar um banco de cláusulas, para garantir a escalabilidade.

- **Garantia de Sigilo.** Recomenda-se registrar todos os terceiros envolvidos em atividades de tratamento de dados pessoais e firmar, com tais terceiros, termos de compromisso e confidencialidade, a fim de que comprometam-se, inclusive, a cumprir regras contidas nas Políticas e Procedimentos do escritório, bem como na legislação em vigor, observando, naturalmente, a natureza da relação que conecta o escritório com tais terceiros.

> **Customização específica**
>
> Todo o processo de adequação será especialmente desenhado para o nível de maturidade do escritório. Desse modo, a implementação poderá ser de diferentes níveis de complexidade e profundidade a depender das áreas analisadas. Quanto mais madura a área, menor será o nível de intervenção.

- **As demais advogadas e advogados do escritório (associadas, associados, contratadas e contratados**) têm obrigação de sigilo, nos termos do Código de Ética ao qual estão submetidos, em relação aos dados de clientes. Neste ponto, é recomendável que sejam firmados termos de confidencialidade para garantir que manterão sigilo em relação a todos os dados pessoais que vierem a tratar (inclusive dados de colegas e demais funcionários do escritório), destinando o tratamento apenas ao alcance das finalidades pré-estabelecidas.

Elaboração dos documentos mínimos do Programa de Governança

- **Código de Conduta e Políticas Internas.** O Programa de Governança deve contar com documentos sobre as condutas e normas gerais de privacidade, incluindo:
    - Código de Conduta
    - Política Institucional de Privacidade e Proteção de Dados
    - Política de Retenção (ou Eliminação) de Dados
    - Política de Resposta a Incidentes

- **Modelos de documentos importantes para conformidade e, ainda, como medida de boa prática.** Exemplificativamente, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que conterá a descrição dos processos de tratamento de dados que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas de salvaguarda e mitigação de tais riscos (art. 5º, XVII); e o LIA – Legitimate Interest Assessment – que servirá como um teste de balanceamento, por meio do qual poderá ser avaliada a viabilidade da adoção da base legal do Legítimo Interesse.

- **Avisos de privacidade.** Os Avisos de Privacidade — Interno e Externo — devem conter informações adequadas para garantir a transparência do escritório para com o titular de dados. Estes Avisos devem ser amplamente divulgados e posicionados em locais de fácil acesso no site do escritório e em sua rede interna.

- **Criação de canais de comunicação.** Os canais de comunicação devem ser específicos para recepcionar questões referentes à privacidade e proteção de dados, tais como:
    - Ofícios de órgãos públicos;
    - Requisições de titulares de dados;
    - Informações relacionadas a incidentes de segurança.

Checklist do Processo de Adequação

Há Políticas e Procedimentos bem definidos que englobam todos os cenários relacionados ao tratamento de dados pessoais realizados?	Há planos de resposta e remediação a incidentes de segurança?	Há evidências do cumprimento de políticas internas e de normas e boas práticas relativas a proteção de dados pessoais?
Os dados foram inventariados e são monitorados para assegurar conformidade?	Há registro das atividades de tratamento de dados e de eventuais terceiros envolvidos?	Foram adotadas as salvaguardas necessárias com base em processo de avaliação sistemática de impactos e riscos à privacidade?
Há mecanismos de auditoria/controle internos e externos?	Há meios para estabelecer uma atuação transparente e de confiança com o titular? (elaboração de Avisos de Privacidade)	Há canais específicos para recepcionar requisições relacionadas a proteção de dados?
O programa de governança está em monitoramento contínuo e passa por avaliações periódicas?	Há plano de comunicação para treinamentos internos e KPI's para monitorar tais treinamentos?	Houve adequação de contratos firmados com terceiros?

Estamos prontos?

Abordados os principais pontos disciplinados pela LGPD e as medidas necessárias à adequação do tratamento de dados pessoais à referida Lei, é importante que tenhamos em mente que, mais que uma nova norma repleta de imposição de obrigações a quem ela se submete, a LGPD traz a oportunidade de tornar relações mais francas, transparentes e éticas entre sócios, empregados, prepostos, prestadores de serviços e, principalmente, entre o escritório de Advocacia e seus clientes.

Cumpre lembrar por fim, que a LGPD não está isolada em um cenário global, portanto, ao acompanhar a tendência mundial iniciada com maior força pelos países europeus, a LGPD coloca o Brasil em um cenário de viabilidade competitiva, elevando sua confiabilidade em relação à proteção de dados pessoais. Portanto, ganhamos todos com sua implementação e correta fiscalização do seu cumprimento.

Créditos

Opice Blum
Bruno e Vainzof Advogados

Sócios

Renato Opice Blum
Danielle Serafino

Revisão

Ana Rita Bibá Gomes de Almeida
Gabriela Silveira Bueno dos Santos
Tiago Neves Furtado

Elaboração

Helena Rodrigues Vaz Pedrosa
Maria Beatriz Previtali
Rodrigo Toller

Apoio

OAB SÃO PAULO
Comissão de Privacidade
e Proteção de Dados