SANTA CATARINA

POLÍTICA DE PRIVACIDADE PROTEÇÃO DE DADOS

Classificação: Restrito

1. Propósito, Escopo e Usuários

A **ORDEM DOS ADVOGADOS DO BRASIL, SEÇÃO DE SANTA CATARINA - OAB/SC**, tem como compromisso defender a Constituição, respeitando assim a privacidade e proteção dos dados pessoais dos advogados e terceiros que se relacionam, em observância à legislação vigente.

Esta Política estabelece os princípios básicos pelos quais a Instituição trata os dados pessoais dos advogados, dependentes, colaboradores e todo e qualquer titular que eventualmente tenha acesso aos dados, e indica as responsabilidades de seus departamentos de negócios e colaboradores durante o tratamento dos dados pessoais.

Os usuários deste documento são os colaboradores, permanentes ou temporários, prestadores de serviços, com contratos habituais ou pontuais, bem como membros eleitos e/ou voluntários que atuam em nome da **OAB/SC**.

2. Legislações de Referência

- Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)
- Constituição Federal de 1988
- Estatuto da Advocacia e a Ordem dos Advogados do Brasil - Lei 8906/94
- Regulamento Geral do EAOAB
- Provimentos do CFOAB
- Regimento Interno da OAB/SC
- Resoluções do Conselho Pleno da OAB/SC
- Normativas da diretoria da OAB/SC
- Código Civil
- Código de Defesa do Consumidor
- Marco Civil da Internet

3. Documentos de referência

A Política de Privacidade e Proteção de Dados está pautada em documentos, que precisam estar adequados às atividades da instituição, efetivando a estratégia de proteção de dados e privacidade. Documentos que envolvem a estratégia e estão listados no decorrer desta Política, demonstrando como o procedimento indicado apresentará a devida eficácia.

Documentos para aplicação da estratégia:

- Código de Conduta
- Política de Retenção de dados (Tabela de Temporalidade)
- Atribuições do Encarregado de Proteção de Dados (DPO)
- Procedimento de Requisição de Acesso aos Dados do Titular - DSAR
- *Política de Segurança da Informação*
- *Rotina de treinamentos*
- *Diretrizes para criação de Inventário de Dados*
- *Política de Controle de Acessos*
- *Relatório de Impacto*
- *Consentimento Válido, com informação de que pode ser revogado*
- *Procedimento de descarte de dados*
- *Procedimento de senhas fortes*
- *Acordo ou Termo de Confidencialidade*
- *Procedimento de Retenção e Dados*
- *Adequação Contratual*

4. Definições

As seguintes definições dos termos utilizados neste documento são extraídas do artigo 5.º da Lei Geral de Proteção de Dados:

Dados pessoais: quaisquer informações relativas a uma pessoa singular identificada ou identificável ("**titular dos dados**"); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.

Dados pessoais sensíveis: dados pessoais que são, por sua natureza, particularmente sensíveis em relação aos direitos e liberdades fundamentais e que, por isso, merecem proteção específica, pois o contexto de seu tratamento pode criar riscos significativos aos direitos e liberdades fundamentais. Esses dados pessoais incluem dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados de saúde, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual.

Tratamento: uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, sendo o principal responsável pelo tratamento de dados.

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais conforme as diretrizes do controlador.

Agentes de Tratamento: o controlador e o operador.

Tratamento: Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Transferência internacional de dados pessoais: Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Relatório de Impacto: documento do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Encarregado de Dados Pessoais: Profissional que exerce a comunicação entre o titular de dados e o controlador, bem como a ANPD e o controlador.

ANPD (Autoridade Nacional de Proteção de Dados Pessoais): Órgão que possui responsabilidade em relação à privacidade e proteção de dados, bem como fiscalizar as empresas em relação à matéria.

5. Princípios básicos relativos ao tratamento de dados pessoais

Os princípios de proteção de dados descrevem as responsabilidades básicas para as organizações que tratam dados pessoais. O artigo 6.º do LGPD estipula que "*As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios*".

5.1. Finalidade

Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

5.2. Adequação

Deve haver a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

5.3. Necessidade

Deve haver limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

5.4. Livre Acesso

Como forma de segurança ao titular de dados pessoais, é uma garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

5.5. Qualidade dos dados

Para garantir, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

5.6. Transparência

Garantia aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

5.7. Segurança

Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

5.8. Prevenção

A adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

5.9. Não descriminação

Impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.

5.10. Responsabilização e prestação de contas:

Demonstração, pelo Controlador ou Operador, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

6. A proteção de dados nas atividades internas da OAB/SC:

Para demonstrar o cumprimento dos princípios da proteção de dados, a instituição deve concretizar a proteção de dados em todas as suas atividades que envolvam dados pessoais.

6.1. Coleta de dados pessoais

A **OAB/SC** coleta os dados exigidos pela legislação para o cadastro de advogados e de estagiários quando os mesmos ingressam na Ordem dos Advogados do Brasil Seção de Santa Catarina.

Coleta dados de titulares advogados inscritos em Santa Catarina e noutras Seccionais, bem como de titulares que não são advogados e que participam de eventos ou ações realizadas pela OAB/SC.

Coleta de dados de titulares que integram os processos administrativos em tramitação perante os órgãos da OAB/SC.

O **Encarregado de Dados** irá trabalhar e conscientizar a instituição para garantir que a **OAB/SC** não colete informações que não sejam estritamente necessárias para a finalidade para a qual foram obtidas.

Os dados pessoais devem ser adequados, relevantes e limitados ao que é necessário para o processamento.

6.1.2. Das obrigações legais que devem ser cumpridas pela OAB/SC

Lei 8.906/94: Art. 58. Compete privativamente ao Conselho Seccional: VIII - manter cadastro de seus inscritos;

Regulamento Geral: Art. 24. Aos Conselhos Seccionais da OAB incumbe alimentar, automaticamente, por via eletrônica, o Cadastro Nacional dos Advogados – CNA, mantendo as informações correspondentes constantemente atualizadas. § 1º O CNA deve conter o nome completo de cada advogado, o nome social, o número da inscrição, o Conselho Seccional e a Subseção a que está vinculado, o número de inscrição no CPF, a filiação, o sexo, a autodeclaração de cor ou raça, a data de inscrição na OAB e sua modalidade, a existência de penalidades eventualmente aplicadas, estas em campo reservado, a fotografia, o endereço completo e o número de telefone profissional, o endereço do correio eletrônico e o nome da sociedade de advogados de que eventualmente faça parte, ou esteja associado, e, opcionalmente, o nome profissional, a existência de deficiência de que seja portador, opção para doação de órgãos, Registro Geral, data e órgão emissor, número do título de eleitor, zona, seção, UF eleitoral, certificado militar e passaporte.

Regulamento Geral: art. 137-D A notificação inicial para a apresentação de defesa prévia ou manifestação em processo administrativo perante a OAB deverá ser feita através de correspondência, com aviso de recebimento, enviada para o endereço profissional ou residencial constante do cadastro do Conselho Seccional. § 1º Incumbe ao advogado manter sempre atualizado o seu endereço residencial e profissional no cadastro do Conselho Seccional, presumindo-se recebida a correspondência enviada para o endereço nele constante.

6.2. Uso e Retenção

As finalidades, métodos, limitação de armazenamento e período de retenção de dados pessoais devem ser consistentes com as informações contidas na *Política de Privacidade,* disponibilizado ao titular de dados pessoais.

Mecanismos de segurança, com a utilização de uma *Política de Segurança da Informação*, adequados projetados para proteger dados pessoais devem ser usados para evitar que dados pessoais sejam roubados, mal utilizados ou utilizados de maneira desconforme à finalidade, além de serem evitadas violações de dados pessoais. O **Encarregado de Dados**, com o auxílio do Comitê de Privacidade, é responsável pelo cumprimento dos requisitos listados nesta seção.

Os dados armazenados pelo controlador de dados devem ser revisados e atualizados conforme necessário, para que dentro do banco de dados não possuam dados sem finalidade.

O **Encarregado de Dados**, com o auxílio do Comitê de Privacidade, é responsável por garantir que todos os funcionários sejam treinados para entender a importância de coletar dados precisos e mantê-los.

O **Encarregado de Dados**, com o auxílio do Comitê de Privacidade, é responsável por garantir que os procedimentos e políticas adequados estejam em vigor para manter os dados pessoais precisos e atualizados, levando em consideração o volume de dados coletados, a velocidade com que podem mudar e qualquer outros fatores relevantes.

O **Encarregado de Dados**, com o auxílio do Comitê de Privacidade, revisará as datas de retenção de todos os dados pessoais processados pela **OAB/SC**, por referência ao *Inventário de Dados*, identificando quaisquer dados que não sejam mais necessários no contexto da finalidade registrada. Esses dados serão excluídos / destruídos com segurança de acordo com um procedimento de descarte de dados.

Os dados pessoais devem ser mantidos de forma que o titular dos dados possa ser identificado apenas durante o tempo necessário para o processamento.

Os dados pessoais serão retidos de acordo com o *Procedimento de Retenção de Dados* (tabela de temporalidade) e, uma vez que sua data de retenção tenha passado, eles devem ser destruídos com segurança conforme estabelecido neste procedimento.

Quando os dados pessoais forem retidos além da data de processamento, eles serão minimizados / criptografados / pseudonimizados para proteger a identidade do titular dos dados no caso de violação de dados, estará estabelecido no *Procedimento de Retenção de Dados.*

Nas hipóteses descritas no artigo 16º da Lei Geral de Proteção Dados, os dados serão mantidos, de acordo com cada operação de tratamento de dados, nas seguintes situações: *Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.*

6.3. Divulgação para Terceiros

Sempre que um fornecedor, prestador de serviços ou membro eleito ou nomeado tratar dados pessoais em nome da **OAB/SC**, o **Encarregado de Dados** deve tomar as providências para que este Operador forneça medidas de segurança para proteger dados pessoais apropriados aos riscos associados. Para isso deve ser utilizada a *Política de Due Diligence,* no momento da contratação deste Operador, ou a qualquer tempo, garantindo que as medidas de segurança sejam seguidas.

A **OAB/SC** deve exigir contratualmente que o fornecedor ou parceiro de negócios forneça o mesmo nível de proteção de dados.

O tratamento de dados pelos Operadores de dados, em nome da **OAB/SC**, deve estar limitado ao tratamento descrito nas obrigações contratuais, ou sob as instruções da **OAB/SC** e não para quaisquer outros fins.

No caso das relações contratuais que originam um grande fluxo de tratamento de dados, as medidas de seguranças devem estar especificadas e explícitas, deixando claras

as respectivas responsabilidades e as do Operador, em contrato relevante ou em qualquer outro documento juridicamente vinculante, como um *Acordo de Tratamento de Dados*.

O **Encarregado de Dados** é responsável por tomar as providências adequadas para que, nos casos em que organizações terceirizadas possam ter transmitido dados pessoais imprecisos ou desatualizados, informá-los de que as informações são imprecisas e/ou desatualizadas e não devem ser usadas para informar decisões sobre os indivíduos em questão, e para passar qualquer correção aos dados pessoais para terceiros, quando necessário.

A **OAB/SC** deve garantir que os dados pessoais não sejam divulgados a terceiros não autorizados, incluindo familiares, amigos, órgãos governamentais e, em certas circunstâncias, a Polícia. Todos os colaboradores devem ter cautela quando solicitados a divulgar dados pessoais mantidos sobre outro indivíduo a um terceiro. É importante ter em mente se a divulgação das informações é ou não relevante e necessária**.**

Todas as solicitações de fornecimento de dados por um desses motivos devem ser apoiadas por documentos apropriados e todas as divulgações devem ser autorizadas previamente por procedimento interno ratificado pelo **Encarregado de Dados e Comitê de Privacidade da OAB/SC.**

6.4. Transferência internacional de dados pessoais

Os dados pessoais coletados pela OAB/SC são mantidos em servidor próprio, no entanto, a OAB/SC utiliza alguns serviços que possuem o armazenamento dos dados fora do país, motivo pelo qual serão descritos os cuidados necessários.

Antes de transferir dados pessoais para fora do Brasil, é importante uma avaliação de adequação pelo controlador de dados, levando em consideração os seguintes aspectos:

● A natureza das informações que estão sendo transferidas;

● O país ou território de origem e destino final das informações;

● Como as informações serão utilizadas e por quanto tempo;

● As leis e práticas do país do cessionário, incluindo códigos de prática relevantes e obrigações internacionais; e

- As medidas de segurança que devem ser tomadas em relação aos dados no exterior.

Seguindo essas diretrizes, e observados tais aspectos, a transferência internacional de dados ocorrerá, de maneira transparente com o titular, informando inclusive a localidade da transferência internacional na *Política de Privacidade*.

Quando necessário, para que possa identificar os riscos da operação de transferência internacional de dados, será realizado um Relatório de Impacto de Dados Pessoais, com o intuito de conhecer os riscos, mitigar e/ou eliminá-los.

6.5. Direitos de Acesso por Titulares de Dados

Quando a **OAB/SC** atuar como uma Controladora de dados pessoais, o **Encarregado de Dados**, com o auxílio do Comitê de Privacidade, é responsável por fornecer aos titulares de dados um mecanismo de acesso razoável para permitir que eles acessem seus dados pessoais, e deve permitir que eles atualizem, retifiquem, seus Dados Pessoais, se apropriado ou exigido por lei.

A **OAB/SC** garante que os titulares dos dados possam exercer estes direitos:

- Os titulares dos dados podem fazer solicitações de acesso aos dados conforme descrito no Procedimento de solicitação de acesso do titular;
- Esse procedimento também descreve como a **OAB/SC** garantirá que sua resposta à solicitação de acesso a dados esteja em conformidade com os requisitos do LGPD.

Os titulares dos dados têm o direito de reclamar a **OAB/SC** em relação ao processamento dos seus dados pessoais, ao tratamento de um pedido de um titular dos dados e aos recursos de um titular dos dados sobre a forma como as reclamações foram tratadas de acordo com o *Procedimento de Solicitação de Acesso ao Titular de Dados - DSAR*.

O canal unificado da solicitação dos titulares consta na *Política de Privacidade*, com o contato do Encarregado. Ocorrendo solicitações por outros canais da **OAB/SC**, o titular deve ser encaminhado para o canal unificado, para que não ocorra desvio de solicitações.

O **Encarregado de Dados**, com o auxílio do Comitê de Privacidade, é responsável por responder às solicitações de retificação dos titulares dos dados no prazo de 15 (quinze) dias. Se a **OAB/SC** decidir não atender à solicitação, o **Encarregado de Dados** deve

responder ao titular dos dados, com os fundamentos legais para o não atendimento da solicitação e informá-lo de seu direito de reclamar à autoridade nacional.

6.6. Portabilidade de dados

Os titulares de dados têm o direito de receber, mediante solicitação, uma cópia dos dados que forneceram em formato estruturado e transmitir esses dados para outro controlador, gratuitamente. O **Encarregado de Dados** é responsável por garantir que tais solicitações sejam tratadas dentro de 15 (quinze) dias contados a partir do recebimento do pedido do titular e a sua devida confirmação de autenticidade, não sejam excessivas e não afetem os direitos aos dados pessoais de outros titulares.

6.7. Direito ao apagamento

Um dos direitos dos titulares elencados na Lei Geral de Proteção de Dados é o direito que ele tem de solicitar o apagamento de seus dados da base de dados da instituição.

O **Encarregado de Dados** precisa fazer uma análise detalhada para responder ao titular, se este tem ou não este direito. Em análise não somente a Lei Geral de Proteção de Dados, mas também na legislação que a **OAB/SC** está submetida.

O **Encarregado de Dados** deve tomar as medidas necessárias (incluindo medidas técnicas) para informar os terceiros que tratam esses dados para atender à solicitação no prazo de 15 (quinze) dias contados a partir do recebimento do pedido do titular e a sua devida confirmação de autenticidade.

Nos raros casos em que a **OAB/SC** atua como Operadora de dados, irá auxiliar no que for preciso o Controlador dos dados, e seguir as diretrizes enviados por este, inclusive exercer o apagamento, caso fique comprovado sua possibilidade.

6.8. Segurança

Ao avaliar as medidas técnicas adequadas, o **Encarregado de Dados** considerará o seguinte:

● Proteção por senha, já utilizado no BR Conselhos, e deverá ser também aplicada para a Rede Interna, através de uma Política de Senhas;

● Bloqueio automático de terminais ociosos, caso não exista será validado internamente uma política para aplicação;

● Remoção de direitos de acesso para USB e outras mídias de memória;

● Software de verificação de vírus e firewalls;

● Direitos de acesso com base na função, onde cada um acessa o que lhe cabe dentro da sua função;

● Criptografia de dispositivos que saem das instalações da organização, como laptops, que pode ser estabelecida na *Política de Teletrabalho e BYOD;*

● Segurança de redes locais e de longa distância, que pode ser estabelecida na *Política de Controle de Acesso;*

● Tecnologias que aumentam a privacidade, como pseudonimização e anonimização;

● Identificar padrões de segurança internacionais apropriados relevantes para a **OAB/SC.**

Ao avaliar as medidas organizacionais adequadas, o **Encarregado de Dados** considerará o seguinte:

● Os níveis de treinamento apropriados para colaboradores da **OAB/SC**;

● Medidas que consideram a confiabilidade dos colaboradores, estabelecido no Termo de Responsabilidade*;*

● Identificação de medidas disciplinares para violações de dados;

● Monitoramento da equipe quanto ao cumprimento dos padrões de segurança relevantes;

● Controles de acesso físico a registros eletrônicos e em papel;

● Adoção de uma política de mesa limpa;

● Armazenamento de dados em papel em gabinetes à prova de fogo com fechadura;

● A imposição de obrigações contratuais às organizações importadoras para tomar as medidas de segurança adequadas ao transferir dados para fora do Brasil.

● Restringir o uso de dispositivos pessoais do próprio funcionário no local de trabalho, e adotar a *Política de BYOD (Bring Your Device);*

● Adotando regras claras sobre senhas;

● Fazer backups regulares de dados pessoais e armazenar, que são salvos na rede interna da instituição.

A avaliação e cumprimento dos requisitos mencionados acima ocorrerá de maneira periódica, visando a governança da privacidade e proteção dos dados pessoais.

7. Organização e Responsabilidades:

A responsabilidade de garantir o tratamento adequado de dados pessoais é de todos que trabalham para ou com a **OAB/SC** e que possuem acesso aos dados pessoais tratados pela **OAB/SC**.

As principais áreas de responsabilidades em relação ao tratamento de dados pessoais estão nas seguintes funções organizacionais:

A Presidência e a Diretoria, tomam decisões sobre e aprovam as estratégias gerais da OAB/SC no que tange a proteção de dados pessoais, com base nas medidas apresentadas pelo Comitê de Privacidade da OAB/SC.

O Encarregado é responsável pelo gerenciamento do programa de proteção de dados pessoais e é responsável pelo desenvolvimento e promoção de políticas de proteção de dados pessoais de ponta a ponta, conforme definido na *Descrição do Trabalho do Encarregado*.

A Procuradoria, juntamente com o Encarregado de Dados, monitora e analisa as leis de dados pessoais e alterações nas regulamentações, desenvolve requisitos de conformidade e auxilia a todos no cumprimento de suas obrigações de proteção de dados pessoais.

O gerente de TI é responsável por:

Garantir que todos os sistemas, serviços e equipamentos utilizados para armazenar dados pessoais atendam aos padrões de segurança aceitáveis.

Realizar verificações e varreduras regulares para garantir que o hardware e o software de segurança estão funcionando corretamente com vistas à garantia da confidencialidade, da integridade e da disponibilidade dos dados pessoais.

O gerente de comunicação e marketing é responsável por:

Aprovar quaisquer declarações de proteção de dados anexadas à comunicação, como e-mails e cartas.

Abordar quaisquer consultas de proteção de dados feitas por jornalistas ou meios de comunicação, como jornais.

Quando necessário, trabalhar com o Encarregado de Dados para garantir que as iniciativas de marketing da instituição cumpram os princípios de proteção de dados.

O Gestor de Pessoas é responsável por:

Melhorar a conscientização de todos os colaboradores a respeito da proteção de dados pessoais dos titulares de dados pessoais, internos e externos.

Organizar treinamentos para melhorar os conhecimentos técnicos e aumentar a conscientização dos colaboradores que trabalham com dados pessoais.

Proteger dados pessoais de colaboradores de ponta a ponta. Ele deve garantir que os dados pessoais dos colaboradores sejam tratados com base em finalidades comerciais legítimas e na necessidade do empregador.

Secretaria

Garantir que todos os sistemas, serviços e equipamentos utilizados para armazenar dados pessoais atendam aos padrões de segurança aceitáveis, tanto em relação ao cadastro dos inscritos, bem como aos procedimentos administrativos respectivos.

Tesouraria

São responsáveis por zelar pelas informações cadastrais e financeiras dos advogados.

Tribunal de Ética e Disciplina

Garantir que todos os sistemas, serviços e equipamentos utilizados para tratar dados pessoais atendam aos padrões de segurança aceitáveis considerando, especialmente, a sigilosidade dos processos disciplinares.

Secretaria do Conselho Pleno

Garantir que o tratamento dos dados pessoais, diante de suas atribuições primárias e secundárias, sejam feitos com observação das melhores práticas e aplicação de medidas de segurança, em conformidade com a Lei Geral de Proteção de Dados.

Central de Atendimento

Garantir o atendimento aos advogados, estagiários e terceiros, com atenção especial na proteção dos dados pessoais, priorizando segurança e privacidade em relação aos dados pessoais dos advogados, visando proteger a confidencialidade, integridade e disponibilidade dos dados pessoais.

8. Diretrizes de Tratamento Justo

8.1. Política de privacidade aos Titulares de Dados

No momento da coleta ou antes de coletar dados pessoais em qualquer tipo de atividade de tratamento, o **Encarregado de Dados** é responsável por informar adequadamente os titulares de dados dos seguintes: os tipos de dados pessoais coletados, as finalidades do tratamento, os métodos de tratamento, os direitos dos titulares de dados em relação aos seus dados pessoais, o período de retenção, possíveis transferências internacionais de dados, se os dados serão compartilhados com terceiros e as medidas de segurança da OAB/SC para proteger dados pessoais. Essas informações são fornecidas por meio de uma *Política de Privacidade*.

A Política de Privacidade da **OAB/SC** está no site, e o titular de dados deve ser encaminhado para este canal sempre que tiver seus dados coletados no ambiente virtual ou fora dele.

Áreas específicas da **OAB/SC** que façam a coleta de dados por outros meios, podem encaminhar o titular de dados para o site, ou ainda, em contato via e-mail, enviando o link da Política de Privacidade.

Quando os dados pessoais estão sendo compartilhados com terceiros, o **Encarregado de Dados** deve garantir que os titulares de dados tenham sido notificados sobre isso pela Política de Privacidade.

Quando dados pessoais sensíveis estiverem sendo coletados, o **Encarregado de Dados** deve certificar-se de que a Política de Privacidade indique explicitamente a finalidade para a qual esses dados pessoais sensíveis estão sendo coletados.

8.2. Obtenção de Consentimento quando necessário

O tratamento de dados pessoais pela **OAB/SC** é realizado com base na obrigação legal do controlador, na execução do contrato com os titulares (clientes e colaboradores), pelo legítimo interesse, ainda pela proteção ao crédito ou casos de exceção e para operações específicas, o consentimento.

Quando o tratamento de dados pessoais for baseado no consentimento do titular dos dados, o **Encarregado de Dados** é responsável por manter um registro de tal

consentimento. O **Encarregado de Dados** é responsável por fornecer aos titulares de dados opções para fornecer o consentimento e deve informar e garantir que seu

consentimento (sempre que o consentimento for usado como base legal para o tratamento) pode ser revogado a qualquer momento.

Os dados pessoais só devem ser tratados para a finalidade para a qual foram originalmente coletados. Caso a **OAB/SC** queira tratar dados pessoais coletados para outra finalidade, deve buscar o consentimento dos titulares de dados em redação específica e inequívoca. Qualquer solicitação desse tipo deve incluir a finalidade original para a qual os dados foram coletados e a(s) finalidade(s) nova(s) ou adicional(is). A solicitação também deve incluir o motivo da mudança de propósito. O **Encarregado de Dados** é responsável pelo cumprimento das regras deste parágrafo.

Agora e no futuro, o **Encarregado de Dados** deve garantir que os métodos de coleta de dados pessoais estejam em conformidade com a lei relevante, as boas práticas e os padrões do setor.

9. Segurança, Organização e Responsabilidades dos Dados

Todos os Colaboradores são responsáveis por garantir que quaisquer dados pessoais que a **OAB/SC** detém e pelos quais é responsável, sejam mantidos em segurança e não sejam, sob quaisquer condições, divulgados a terceiros, a menos que esse terceiro tenha sido especificamente autorizado para receber essas informações, através de um contrato celebrado entre as partes, ou celebrar um *Acordo de Confidencialidade*.

Todos os dados pessoais devem ser acessíveis apenas para aqueles que precisam usá-los, e o acesso só pode ser concedido em consonância com a *Política de Controle de Acesso*. Todos os dados pessoais devem ser tratados com a maior segurança e devem ser mantidos:

● Em uma sala fechada com acesso controlado; e / ou

● Em uma gaveta trancada ou arquivo; e / ou

● Se informatizado, protegido por senha de acordo com os requisitos corporativos da *Política de Controle de Acesso;* e / ou

● armazenados em mídia de computador (removível) que são criptografados;

Deve-se ter cuidado para garantir que as telas e terminais do PC não fiquem visíveis, exceto para colaboradores autorizados.

Os registros manuais não podem ser deixados onde possam ser acessados por pessoas não autorizadas e não podem ser removidos das instalações comerciais sem autorização explícita, devidamente registrada. Assim que os registros manuais não forem mais necessários para o suporte diário, eles devem ser removidos de maneira segura, se necessário a utilização de picotadora de papel.

Os dados pessoais só podem ser excluídos ou descartados de acordo com a sua finalidade, caso não tenha legislação que indique o armazenamento. Os registros manuais que atingiram sua data de retenção devem ser triturados e descartados como "lixo confidencial". Os discos rígidos de PCs redundantes devem ser removidos e imediatamente destruídos.

O processamento de dados pessoais "fora do local" apresenta um risco potencialmente maior de perda, roubo ou danos aos dados pessoais. A equipe deve ser especificamente autorizada a processar dados fora do local.

No caso de utilização de dispositivo móvel, celular ou notebook, ao acessar sistemas da instituição, o usuário deve tomar todas as medidas de segurança necessárias, para proteger os dados pessoais constantes nos dispositivos.

A responsabilidade de garantir o tratamento adequado de dados pessoais é de todos que trabalham para ou com a OAB/SC e que possuem acesso a dados pessoais que são tratados pela mesma

10. **Resposta a incidentes de violação de dados pessoais**

Quando a **OAB/SC** tiver conhecimento de um incidente de segurança ou de uma violação concreta de dados pessoais, o **Encarregado de Dados** irá realizar uma investigação interna e tomar as medidas corretivas apropriadas em tempo hábil, de acordo com uma *Política de Identificação e Resposta de Incidentes*.

Quando houver qualquer risco para os direitos e liberdades dos titulares de dados, a **OAB/SC** deve notificar as Autoridades de Proteção de Dados em prazo razoável, quando possível, no prazo de 48 horas.

O *tamplate* oferecido pela ANPD (Autoridade Nacional de Proteção de Dados) deve ser utilizado para que seja feita a notificação do incidente de maneira completa, conforme link: *https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca*.

11. Auditoria e Prestação de Contas

O **Encarregado de Dados** e/ou o Comitê de Privacidade da Instituição é responsável por auditar o quão bem os departamentos de negócios implementam esta Política.

Qualquer colaborador que viole esta Política estará sujeito a uma ação disciplinar. O colaborador também poderá estar sujeito a responsabilidades civis ou criminais se sua conduta violar leis ou regulamentos.

12. Conflitos de Direito

Esta Política destina-se a cumprir a Lei Geral de Proteção de Dados. No caso de qualquer conflito entre esta Política e as leis e as aplicáveis, estas últimas prevalecerão sobre esta Política.

13. Gerenciamento de registros mantidos com base neste documento

13.1. A **OAB/SC** irá estabelecer um inventário de dados e um processo de fluxo de dados como parte de sua abordagem para lidar com riscos e oportunidades em todo o projeto de conformidade com o LGPD. A partir de questionários respondidos pelos setores, e validado pelo Encarregado de Dados, e aqui seguem As *Diretrizes para Criação de Inventário* da OAB/SC e o fluxo de dados determinam:

- Processos internos que usam dados pessoais;
- Fonte de dados pessoais;
- Volume de titulares de dados;
- Descrição de cada item de dados pessoais;
- Atividade de processamento;
- Mantém o inventário das categorias de dados dos dados pessoais processados;
- Documenta a (s) finalidade (ões) para a (s) qual (is) cada categoria de dados pessoais é usada;
- Destinatários e potenciais destinatários dos dados pessoais;
- A função da OAB/SC em todo o fluxo de dados;
- Principais sistemas e repositórios;

- Quaisquer transferências de dados; e
- Todos os requisitos de retenção e descarte.

A **OAB/SC** está ciente de todos os riscos associados ao processamento de tipos específicos de dados pessoais.

A **OAB/SC** irá gerenciar quaisquer riscos identificados pela avaliação de riscos, a fim de reduzir a probabilidade de uma não conformidade com esta política.

Quando um tipo de processamento, em particular usando novas tecnologias e levando em consideração a natureza, escopo, contexto e finalidades do processamento é susceptível de resultar em um alto risco para os direitos e liberdades das pessoas naturais, a **OAB/SC** irá, antes do processamento, efetuar um *Relatório de Impacto das Operações de tratamento* previstas na proteção dos dados pessoais. Um único Relatório de Impacto pode abordar um conjunto de operações de processamento semelhantes que apresentam altos riscos semelhantes.

Quando, como resultado de um *Relatório de Impacto*, for claro que a **OAB/SC** está prestes a iniciar o processamento de dados pessoais que podem causar danos aos titulares dos dados, a decisão sobre se a **OAB/SC** pode ou não prosseguir deve ser encaminhado para revisão ao responsável pelo **Encarregado de Dados.**

Controles apropriados serão selecionados, as medidas de seguranças exigidas pela Lei Geral de Proteção de Dados com o apoio das ISO's 27701 e 29151, e aplicados para reduzir o nível de risco associado ao processamento de dados individuais a um nível aceitável, e quando possível será feita a devida eliminação do risco.

14. Validade e gerenciamento de documentos

Este documento é válido a partir de 01/04/2024.

O proprietário deste documento é o Encarregado de Dados, que deve verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.