LEI GERAL DE PROTEÇÃO DE DADOS
2º TABELIONATO DE ALEGRETE

Controlador: Jonatas Rolla Espindola

CPF: 004.217.330-20

E-mail: tabelionatoespindola@gmail.com

Celular: 51 99208-0844

Encarregado: Leonardo da Mota Paim

(i) E-mail: segundotabelionatto@hotmail.com

(ii) Telefones: (55) 34223300 ou (55) 99727-4939.

A forma de comunicação com a autoridade Nacional de Proteção de Dados (ANPD), quando necessária será feita através de peticionamento eletrônico à Secretaria Geral.

Operadores funcionários, estagiários, escritório de contabilidade, Loebler, Empresa Sky Informática, Tribunal de Justiça- TJ/RS; Conselho Nacional de Justiça- CNJ, Colégio Notarial do Brasil – CNB/RS,

1) INVENTÁRIO DE DADOS PESSOAIS.

O Inventário de Dados Pessoais – IDP consiste no registro das operações de tratamento dos dados pessoais realizados pelo 2º Tabelionato de Alegrete/RS - Tabelionato Espindola (LGPD. Art. 37).

Este registro descreve informações em relação ao tratamento de dados pessoais realizados pelo Tabelionato, para exercício de suas atividades e prestação de serviços, e ficará arquivado em planilha e será atualizado periodicamente:

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

b) categorias de dados pessoais, e descrição dos dados utilizados nas respectivas atividades:

(1) dados comuns:

- Nome Completo
- Carteira de Identidade (RG - Registro Geral)
- CPF (Cadastro de Pessoa Física)
- Certidões pessoais das esferas Federal, Estadual e Municipal
- Cópia de matrícula de imóvel
- Endereço
- Profissão
- E-mail
- Telefone de contato
- Contas bancárias
- Outras informações relevantes;

(2) dados sensíveis:

- Imagens
- Biométricos

- Atas com informações sobre dados sindicais
- Partidos políticos
- Interditos
- Procurações de menores
- Declaratórias de União Homoafetiva);

c) a identificação das formas de obtenção/coleta dos dados pessoais:

Podemos coletar dados pessoais durante o cadastro tais como: nome completo; número do CPF; número do RG ou documento equivalente; gênero; e-mail; número do telefone fixo ou celular; endereço residencial ou profissional; data do nascimento; idade; nome de usuário; profissão; estado civil; nacionalidade; local de nascimento; nome dos pais; nome do cônjuge; número do CPF do cônjuge;

Também coletamos, armazenamos e usamos determinadas categorias especiais de informações pessoais mais sensíveis, como: condição de exposição política (pessoa politicamente exposta), portador de necessidade especial, imagens e biometria.

d) base legal:

(i) Para cumprimento de algumas obrigações legal específica (em conformidade com o Artigo 7º, II e III- LGPD)

(ii) Para atender os interesses legítimos do controlador de dados nos termos do inciso IX do Artigo 7º, inciso II - LGPD

(iii) com o consentimento do usuário inciso IX do Artigo 7° inciso II da LGPD

e) descrição da categoria dos titulares:

Funcionários do cartório- CLT, estagiários, prestador de serviço externo (pessoa natural), clientes e pessoas que tem dados armazenados no acervo do cartório.

f) se há compartilhamento de dados com terceiros, identificando eventual transferência internacional:

O 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola; não compartilha informações com terceiros particulares, a não ser através de fornecimento de certidões de instrumentos públicos lavrados ou registrados no tabelionato, cuja publicidade é prevista em lei.

Porém, por força de lei, compartilha dados com o Conselho Nacional de Justiça- CNJ, Tribunal de Justiça do Estado- TJ/RS; Prefeitura Municipal; Secretaria da Fazenda Estadual, para o envio de DITS de inventário e doação; com a Receita Federal, para o envio das Declarações Sobre Operações Imobiliárias- DOI, com a CENSEC, para enviar informações de escrituras e testamentos lavrados; como o IBGE, para enviar dados sobre divórcios realizados, CNB/RS, Sky Informática (NOTAR), Sistema de Controle de Atividades Financeiras – SISCOAF, Central Eletrônica de Publicações e de Interdições e Tutelas - CEPIT.

Poderá, a qualquer tempo, mediante requisição ou mandado, fornecer dados ou informações relativas aos usuários a outros serviços públicos digitais cuja finalidade seja a efetiva prestação de serviço público pelo compartilhamento de dados ou informações ou atender demanda judicial ou policial ou por requisição do Ministério Público, conforme o artigo 7º, incisos III e VI, e o artigo 26, § 1º, I, III, IV e V, e § 2º da Lei 13.709/18.

Não há transferência internacional.

g) categorias de destinatários, se houver:

Fornecedores; prestadores de serviços; Entidades; Autoridades públicas, usuários, funcionários e estagiários.

h) prazo de conservação dos dados:

Os Dados são armazenados em ambiente seguro e controlado (Sky Remote Backup), por prazo estabelecido legal e/ou reguladoramente, sendo que para fins de auditoria, preservação de direitos, ou se tivermos alguma outra razão legítima para mantê-los, podemos armazenar os dados pelo período mínimo de

10 (dez) anos contados a partir do momento que os dados são armazenados conforme artigo 848 caput da Consolidação Normativa Notarial e Registral, podendo ser estendido por prazo maior nas hipóteses em que a lei e/ou norma regulatória assim estabelecerem ou para preservação de direitos. Contudo, podemos excluí-lo definitivamente segundo a nossa exclusiva conveniência em prazo menor. Os Dados podem ser armazenados em nossos servidores próprios ou de terceiro contratado para esse fim (Sky Remote Backup), de acordo com os critérios da legislação aplicável, podendo ainda serem armazenados por meios de tecnologia de cloud computing e/ou outras tecnologias que surjam futuramente, visando sempre a melhoria e aperfeiçoamento de nossos serviços.

i) medidas de segurança organizacionais e técnicas adotadas:

Treinamento do pessoal que opera os dados, sala do acervo e dos servidores com acesso restrito a pessoas autorizadas, mantidas chaveadas; senha individual para cada funcionário e estagiário, com a delimitação do que podem acessar e modificar no banco de dados; documentos de encaminhamento de escrituras e escrituras lavradas, guardados em armário fechados, sem acesso visual pelos usuários do serviço do tabelionato. Computadores posicionados de modo que não sejam visualizados pelo público externo. Agenda e livro de registro de assinaturas mantidos em uma prateleira de armário, longe do alcance do público. Sala reservada para a leitura e entrega de escrituras e testamentos. Câmeras posicionadas em locais estratégicos. Alarme com monitoramento por empresa de segurança.

PLANO DE AÇÃO PARA IMPLEMENTAÇÃO DE NOVOS PROCESSOS

O plano de ação para a implementação dos novos processos, procedimentos, controles e demais medidas internas, incluindo a revisão e criação de documentos envolve:

- revisar a prática de lavratura de todos os atos do cartório, estabelecendo um liame entre as leis setoriais e a LGPD, estabelecendo diretrizes uniformes sobre o conteúdo mínimo necessário em diferentes contextos possíveis para produzir o efeito de segurança dos documentos produzidos e ao mesmo tempo assegurar a proteção de dados pessoais dos titulares dos dados envolvidos;

- respeitar o princípio da necessidade (artigo 7º, III, LGPD), utilizar o mínimo suficiente de dados pessoais suficientes para praticar o ato;

- indicar para quais finalidades os dados são coletados;

- revisar e elaborar contratos de funcionários, fornecedores, clientes e prestadores de serviços, visando a adequação da LGPD bem como considerando os 3 pilares de segurança: confidencialidade, integridade e disponibilidade, em conformidade com a ISSO 27001, 27002 e a extensão ISSO 27701.

As formas de comunicação com o tabelião do 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola que é considerado o "Controlador" dos seus Dados, conforme o artigo 5º, inciso VI da Lei 13.709/18 e o seu Encarregado de Dados se dará pelos canais abaixo:

(i) E-mail: segundotabelionatto@hotmail.com, tabelionatoespindola@gmail.com

(ii) Telefones: (55) 34223300 ou (55) 997274939.

A forma de comunicação com a autoridade Nacional de Proteção de Dados (ANPD), quando necessária será feita através de peticionamento eletrônico à Secretaria Geral.

AVALIAÇÃO DAS VULNERABILIDADES (GAP ASSESSMENT)

A avaliação das vulnerabilidades (gap assessment) para análise de lacunas em relação à proteção de dados pessoais no que se refere às atividades desenvolvidas na serventia será realizada ao correr do tempo e com base no que for constatado será elaborado e serão tomadas decisões diante das vulnerabilidades encontradas e implementadas as adequações necessárias e compatíveis com a tomada de decisões;

Será atualizado, sempre que necessário, não podendo ultrapassar um ano, o inventário de dados, que será arquivado e disponibilizado em caso de solicitação da Corregedoria Geral da Justiça, da Autoridade Nacional de Proteção de Dados Pessoais ou de outro órgão de controle.

REVISÃO DOS CONTRATOS

- Foram revisados os contratos de trabalho dos funcionários e estagiários, com a inclusão da cláusula de obrigatoriedade a respeito das normas de privacidade e proteção de dados nos contratos e regulamentos internos.

- Foram revisados os modelos e minutas das escrituras lavradas no Tabelionato, incluindo a observação sobre o cumprimento da LGPD e com quem são compartilhados os dados dos titulares.

- Foi elaborado e assinado Termos de Tratamento de Dados Pessoais pelos operadores, que ficou arquivado em pasta própria na Serventia.

- Foram elaboradas orientações e procedimentos para as contratações futuras, estabelecendo a forma de coleta de informações sobre os futuros candidatos a emprego pela CLT ou estágio, cujos deverão ser treinados dentro da legislação vigente, antes de serem efetivados e realizarem o tratamento de dados.

- O compartilhamento de dados é feita com o Tribunal de Justiça do RS, com o Conselho Nacional de Justiça, com as Centrais por força de obrigatoriedade, com a contadora e com o IBGE. Eventuais compartilhamentos de dados com terceiros serão pontuais e serão submetidos a auditorias regulares, para realizar a gestão de terceiros.

- São fornecedores de tecnologia, automação e armazenamento, as empresas: SKY INFORMÁTICA LTDA, REDE CONESUL DE TELECOMUNICAÇÕES e SOLUÇÃO INFORMÁTICA LTDA e estão adequadas às exigências da LGPD quanto aos sistemas e programas de gestão de dados internos utilizados.

ENCARREGADO DO TRATAMENTO DE DADOS

O **Encarregado do Tratamento de dados é o Tabelião Substituto Leonardo da Mota Paim,** que poderá ser contatado através do e-mail segundotabelionatto@hotmail.com, tabelionatoespindola@gmail.com ou dos telefones (55) 34223300 ou (55) 997274939.

Segundo define a LGPD (Art. 5º, VIII), o encarregado é pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)

RELATÓRIO DE IMPACTO

Foi elaborado o Relatório de impacto à proteção de dados pessoais, referente aos atos em que o tratamento de dados possa gerar risco às liberdades civis e aos direitos fundamentais do titular.

Este relatório ficará arquivado juntamente com os demais documentos relativos à proteção de dados.

- Descrição dos tipos de dados coletados

Para elaborar o cadastro e atualização dos dados do usuário:

Nome completo;

Data de Nascimento;

Nome dos pais;

Foto;

Número de CPF;

Endereço de e-mail;

Número de celular;

Data de nascimento;

Estado civil;

Profissão

Biometria

Dados referentes aos seus endereços.

- Para lavratura de atas notariais, escrituras e procurações:

Nome completo;

Data de Nascimento;

Nome dos pais;

Foto;

Número de CPF;

Endereço de e-mail;

Número de celular;

Data de nascimento;

Estado civil;

profissão

Biometria;

Dados referentes aos seus endereços físico e virtual;

Acesso a redes sociais para elaboração da ata;

Acesso a conversas de WhatsApp;

Vídeo;

Áudio.

Demais Documentos necessários para a elaboração dos documentos

Também foram estabelecidos procedimentos visando informar:

- Metodologia utilizada para coleta

- Metodologia de garantia da segurança da informação

- Análise do controlador com relação à medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

DAS MEDIDAS DE SEGURANÇA, TÉCNICAS E ADMINISTRATIVAS

Para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito- Artigo 46 e seguintes LGPD.

Para isto, foi elaborada a Política de segurança da Informação, com medidas de segurança técnica e 0rganizacional, com previsão de mecanismos de segurança e plano de resposta a incidentes.

Foi realizada avaliação do sistema do banco de dados onde há tratamento de dados pessoais e sensíveis, com ciência e acompanhamento do encarregado de dados, bem como avaliação da segurança de integração de sistemas, análise da segurança das hipóteses de compartilhamento de dados com terceiros e a realização de treinamento com os funcionários e estagiários, que são os operadores.

Foi elaborado o Plano de resposta a incidentes, nos termos do art. 48 da LGP, em documento separado, que ficará arquivado na pasta corresponde à implantação da segurança de dados.

Foi feita a avaliação do banco de dados em que há tratamento de dados pessoais e sensíveis, bem como das câmeras de segurança, e os resultados foram submetidos à ciência do encarregado pelo tratamento dos dados pessoais da serventia.

Além disto, foi realizada a avaliação de segurança de integrações de sistemas, através das redes internas e análise de segurança das hipóteses de compartilhamento de dados pessoais com terceiros, que são realizados por imposições legais, tais como Tribunal de Justiça do RS, Conselho Nacional de Justiça- CNJ, Corregedoria Geral de Justiça e seus departamentos, IBGE, Receita Federal, Receita Estadual, Prefeitura Municipal, CENSEC, CEPIT, SISCOAF.

Foi realizado treinamento dos operadores que trabalham no Tabelionato, como funcionários ou estagiários e este treinamento é realizado sempre que há a verificação de alguma circunstância que o exija ou quando há novas orientações a serem dadas.

Será realizada a inutilização e eliminação de documentos, de acordo com a Tabela de Temporalidade de Documentos, prevista no Provimento 50/2015 da Corregedoria Nacional da Justiça, de forma a impedir a identificação dos dados neles contidos.

Os dados que remanescerem nos índices, classificadores, indicadores, banco de dados, arquivos de segurança ou qualquer outro modo de conservação serão tratados de acordo com o que determina a LGPD.

Os documentos físicos também são digitalizados e guardados em nuvem.

Os documentos físicos que tem dados pessoais e dados pessoais sensíveis são guardados junto ao acervo do tabelionato, em salas fechadas e com controle de acesso.

TREINAMENTO

São realizados treinamentos para implementação da cultura de privacidade e proteção de dados pessoais, bem como para a capacitação de todos os envolvidos no tratamento dos dados pessoais sobre os novos controles, processos e procedimentos, observando o seguinte:

I – capacitar todos os trabalhadores da serventia a respeito dos procedimentos de tratamento de dados pessoais;

II – realizar treinamentos com todos os novos trabalhadores;

III – manter treinamentos regulares, de forma a reciclar o conhecimento sobre o assunto e atualizar os procedimentos adotados, sempre que necessário;

IV – organizar, por meio do Encarregado e eventual equipe de apoio, programa de conscientização a respeito dos procedimentos de tratamento de dados, que deverá atingir todos os trabalhadores; e

V – manter os comprovantes da participação em cursos, conferências, seminários ou qualquer modo de treinamento proporcionado pelo controlador aos operadores e Encarregado, com indicação do conteúdo das orientações transmitidas.

O treinamento é feito constantemente, especialmente para que a cultura da privacidade seja agregada ao dia-a-dia do tabelionato, mantendo os documentos fora do alcance de vista dos usuários, as telas de computadores voltadas somente para o operador, o livro de registro de assinatura guardado em armário, escrituras, documentos de encaminhamentos e fichas em local seguro.

DAS MEDIDAS DE TRANSPARÊNCIA E ATENDIMENTO A DIREITOS DE TITULARES

Como medida de transparência e prezando pelos Direitos dos Titulares dos dados, a responsável pela serventia elaborou:

I – canal eletrônico específico para atendimento das requisições e/ou reclamações apresentadas pelos titulares dos dados pessoais; e

II – fluxo para atendimento aos direitos dos titulares de dados pessoais, requisições e/ou reclamações apresentadas, desde o seu ingresso até o fornecimento da resposta.

São divulgadas em local de fácil visualização e consulta pelo público as informações básicas a respeito dos dados pessoais e procedimentos de tratamento, os direitos dos titulares dos dados, o canal de atendimento disponibilizado aos titulares de dados para que exerçam seus direitos e os dados de qualificação do encarregado, com nome, endereço, e meios de contato. Estas informações constam de quadros expostos em lugar visível, junto ao atendimento ao público.

MEDIDAS DE TRANSPARÊNCIA AO USUÁRIO

Esta serventia reconhece importância da privacidade e da segurança dos dados pessoais de nossos clientes, empregados, fornecedores, prestadores de serviço e demais parceiros, motivo pelo qual respeita a Lei 13.709 de 14/08/2018 – Lei Geral de Proteção de Dados – LGPD.

Para expressar nosso respeito ao princípio da defesa da privacidade e à Lei de Proteção de Dados, estabelecemos uma Política de Proteção a Dados Pessoais e Privacidade.

Nossa política tem por objetivo traçar diretrizes e orientações para o tratamento de dados pessoais, protegendo a privacidade dos nossos clientes e parceiros, visando à gestão de dados pessoais e à gestão de incidentes de segurança da informação no ambiente convencional ou de tecnologia de nossas atividades.

Um dos aspectos mais importantes da nossa política é o compromisso de que os processos que envolvam a coleta de dados pessoais deverão seguir rigorosamente as determinações dos órgãos fiscalizadores, em especial o Conselho Nacional de Justiça e a Corregedoria Geral de Justiça.

Nossos colaboradores têm conhecimento da nossa Política de Proteção a Dados Pessoais e à Privacidade e a violação das normas previstas pode acarretar sanção disciplinar. Todos os nossos empregados e estagiários assinam um termo de confidencialidade e são orientados a atuarem apenas dentro dos fins e limites especificados na legislação que regula a atividade registral. Informamos aos nossos usuários que realizamos tratamento de dados pessoais para cumprimento de dever legal, motivo pelo qual não é necessário o fornecimento de consentimento do titular dos dados, uma vez que o tratamento de dados pessoais é realizado para o atendimento da finalidade pública da nossa atividade, com o objetivo de executar as competências legais e cumprir as atribuições legais do serviço público registral, conforme expressamente previsto no inciso II do art. 7º da referida Lei, exceto no caso de dados sensíveis.

Salientamos que os serviços Notariais e de Registro foram equiparados às Pessoas Jurídicas de Direito Público pelo § 4º do artigo 23 da Lei.

Seus dados podem ser transmitidos, via centrais como CENSEC e para diversos órgãos públicos, para cumprimento de obrigações legais/normativas, sempre tomando as devidas precauções para garantir a segurança e confidencialidade dos dados pessoais.

A inutilização e/ou eliminação de dados deve observar o previsto no Provimento nº 50/2015 do CNJ – Conselho Nacional de Justiça.

Nossos serviços utilizam as seguintes informações pessoais do seu cadastro:

- Nome
- RG
- CPF
- Data de Nascimento
- Endereço
- Filiação
- Nacionalidade
- Profissão
- Estado civil e qualificação do cônjuge
- Endereço residencial e profissional completo, inclusive e-mail
- Telefones, inclusive celular
- Se se trata de pessoa exposta politicamente

Para solucionar qualquer dúvida sobre o nosso compromisso com a privacidade de dados ou para exercer algum direito enquanto titular, faça contato com o nosso encarregado pelo tratamento de dados pessoais, Leonardo da Mota Paim, através do E-mail: segundotabelionatto@hotmail.com, ou tabelionatoespindola@gmail.com

Telefones: (55) 34223300 ou (55) 997274939.

PROCEDIMENTOS INTERNOS PARA ACESSO AOS DIREITOS DOS TITULARES (QR CODE- CARTAZ, NOME DO ENCARREGADO)

ADOÇÃO DE CARTAZES E DIVULGAÇÃO NAS REDES SOCIAIS

POLÍTICA INTERNA DE PRIVACIDADE E PROTEÇÃO DE DADOS (PRIVACIDAE INTERNA)

Foi elaborada a Política Interna de Privacidade e Proteção de Dados, em documento separado, que ficará arquivado com os demais documentos da LGPD

POLÍTICA INTERNA DE PRIVACIDADE E PROTEÇÃO DE DADOS 2º TABELIONATO DE ALEGRETE- TABELIONATO ESPINDOLA

ORIENTAÇÕES E RESPONSABILIDADES SOBRE O TRATAMENTO DE DADOS – LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 - LGPD.

Essas orientações gerais são destinadas a todos os colaboradores da serventia e tratam das formas de coleta, tratamento e compartilhamento de dados pessoais a que tiverem acesso, em decorrência de suas funções, bem como sobre as respectivas responsabilidades.

A LGPD estabelece, em seu art. 6º, que o tratamento de dados pessoais deve observar a boa-fé e dez princípios fundamentais específicos. São eles:

• finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

• adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

• necessidade: 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;

• livre acesso: 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;

• qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

• 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;

• 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;

• prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

• não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e

• responsabilização e prestação de contas: demonstração, pelo agente, 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.

No caso deste 2º Tabelionato de Alegrete/RS a despeito da autorização legislativa para o tratamento de dados pessoais (artigo 7º, incisos II e X da LGPD), é fundamental garantir que os princípios listados acima sejam respeitados.

Passo 1 - Identificação das hipóteses de tratamento aplicáveis

Como determinar a hipótese legal que autoriza o tratamento de dados pessoais? Isso depende das finalidades e contextos específicos de cada situação.

É natural imaginar que, para os atos notariais seriam sempre aplicáveis as hipóteses II e X do artigo 7º da LGPD, quais sejam: “para o cumprimento de obrigação legal ou regulatória pelo controlador”.

No entanto, não existe uma regra geral que se adeque a todas as situações, mesmo considerando se tratar da prestação de serviços de registro e notariais. Poderá haver, inclusive, situações em que o cartório não seja adequado para a prestação dos serviços pretendidos e — nessa última hipótese — os dados eventualmente coletados devem ser eliminados (p.ex. cópias de documentos pessoais, dados de identificação, etc.)

O importante é avaliar caso a caso e documentar a hipótese aplicável, uma vez que o titular deverá conhecer a hipótese legal autorizadora do processamento de seus dados pessoais.

Além disso, o princípio da responsabilização e prestação de contas requer que aquele que realiza o tratamento de dados pessoais possa demonstrar que está plenamente aderente à LGPD, comprovando a observância e o cumprimento das normas de proteção de dados pessoais estabelecidas, inclusive quanto a sua eficácia.

Por essa razão, cabe a cada um dos operadores (colaboradores da serventia) avaliar bem a hipótese de tratamento aplicável, em atenção aos requisitos de transparência, responsabilização e prestação de contas.

Seguem algumas orientações, na forma de perguntas, que objetivam facilitar a identificação da hipótese mais apropriada para o tratamento dos dados a serem fornecidos.

Tratamento para o cumprimento de obrigação legal ou regulatória - essa hipótese é aplicável quando é necessário processar dados pessoais para o cumprimento de obrigações legais ou regulatórias específicas. Exemplo: reconhecimento de firmas, cadastro de ficha padrão, lavratura de escrituras

Para enquadramento nessa hipótese, deve-se avaliar:

1. É possível identificar a obrigação legal ou regulatória específica que requer o processamento do dado?

2. O titular do dado será informado sobre a norma que determina a obrigação legal ou regulatória que exige o tratamento do dado?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

Passo 2 - Verificação de conformidade do tratamento de dados quanto aos princípios da LGPD

Uma vez identificada a hipótese de tratamento aplicável às situações específicas de processamento de dados pela serventia, deve-se partir para outras questões importantes para a verificação da conformidade quanto aos princípios da LGPD.

Para tanto, o operador (colaborador da serventia) deverá observar os seguintes tópicos:

Identificar a finalidade para a qual o tratamento de dado é necessário. Os propósitos devem ser legítimos, específicos e explícitos (princípio da finalidade)

– p. ex.: registro de certidão, lavratura de escritura, procuração, abertura de cartão, etc.

Definir como a finalidade do tratamento será informada ao titular, o que deve ser feito antes do início do tratamento do dado (princípio da finalidade) – isso consiste em explicar para o cliente por qual razão são necessários os dados solicitados (leis, normas, provimentos, etc.)

Garantir que o tratamento do dado será apenas para a finalidade informada ao titular (princípio da adequação) – explicar que todos os colaboradores têm o dever de sigilo imposto por lei e que o compartilhamento se dá apenas em decorrência de obrigação normativa. Importante esclarecer que os dados pessoais coletados pela serventia passam a constituir o que se denomina arquivo público, passível de conhecimento por meio de certidão, hipótese na qual o solicitante da certidão se responsabiliza por eventual uso indevido da informação.

Ao executar a coleta e tratamento de dados, atentar para limitar a utilização ao mínimo de informações necessárias, garantindo abrangência pertinente e proporcional à consecução das finalidades necessárias à realização do ato (princípio da necessidade) – p.ex. desnecessidade de indagar religião, orientação sexual, etc.

Proceder à verificação contínua quanto à exatidão, à clareza, à relevância e à atualização dos dados do titular. O objetivo é manter-se fiel à finalidade de tratamento informada (princípio da qualidade do dado) – p. ex. atualização do cartão de firmas.

Passo 3 – Coleta dos dados

A coleta é uma das operações de tratamento referenciadas pelo art. 5º, inciso X da LGDP. Essa operação representa a etapa inicial do ciclo de vida do tratamento de dados, na qual serão obtidos todos os dados pessoais do cidadão

(titular dos dados), necessários à realização do ato notarial pretendido. Tendo em vista que a coleta é a operação inicial de tratamento dos dados pessoais, a realização de tal operação somente deve ser realizada mediante o atendimento das hipóteses de tratamento, das medidas de segurança, dos princípios, dos diretos do titular e demais regras dispostas pela LGPD a serem rigorosamente observadas por cada colaborador da serventia.

Passo 4 – Segurança no tratamento dos dados

Os agentes de tratamento (colaboradores da serventia) devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46).

Neste ponto, observar alguns cuidados básicos de acesso aos sistemas, tais como:

- Acessar os sistemas sempre por meio de login e senha pessoais;
- Jamais compartilhar login e senha com outros colaboradores;
- Criar senhas de acesso hierarquizadas, limitando o acesso de todos os colaboradores a dados desnecessários ao exercício das suas atividades;
- Não clicar ou abrir anexos de fontes não confiáveis;
- Não permitir a utilização dos equipamentos da serventia por pessoas não autorizadas ou estranhas ao quadro funcional;
- Não utilizar pen drives ou outros dispositivos nos equipamentos da serventia;
- Não compartilhar a senha de wifi, etc.

Observar rigorosamente todos os deveres constantes do Provimento 74 do CNJ.

Quanto aos documentos físicos, cada colaborador deve manter a atenção e o cuidado necessários para a preservação dos dados em tratamento, tais como:

- Manter os documentos organizados em pastas;
- Sempre que se afastar do posto de trabalho por períodos curtos, virar os documentos em tratamento com a face para baixo;
- Se o afastamento do posto de trabalho for mais longo, arquivar o documento nas caixas e armários disponibilizados para esse fim;
- Manter os documentos sigilosos em salas onde não houver acesso ao público;
- Manusear os documentos das partes com cuidado e discrição, sem prejuízo de outros cuidados.

Passo 5 – Término do tratamento dos dados

Nos termos da LGPD, o término do tratamento de dados pessoais ocorre em quatro hipóteses:

(I) exaurimento da finalidade para os quais os dados foram coletados ou quando estes deixam de ser necessários ou pertinentes para o alcance desta finalidade;

(II) fim do período de tratamento;

(III) revogação do consentimento ou a pedido do titular, quando for o caso, resguardado o interesse público;

(IV) determinação da autoridade nacional em face de violação do disposto na Lei.

Na incidência de qualquer uma das hipóteses acima, a Lei determina que os dados sejam eliminados. Contudo, no caso das serventias extrajudiciais, remanesce a obrigação legal de manutenção desses dados, por tempo indeterminado.

No caso de eliminação de dados sempre observar a tabela de temporariedade contida no Provimento 50 do CNJ.

No âmbito dos serviços extrajudiciais é importante que este dispositivo seja harmonizado com a legislação especial, uma vez que os dados pessoais coletados pela serventia passam a constituir o que se denomina arquivo público de forma que, mesmo exaurida a finalidade precípua da coleta (o dado pessoal passará a compor documento de valor permanente (quer por sua natureza histórica, probatória ou informativa), o qual tem natureza inalienável e imprescritível.

PRIVACIDADE DESDE A CONCEPÇÃO E POR PADRÃO

Privacidade desde a concepção

Os agentes de tratamento ou qualquer outro colaborador que participe da coleta ou tratamento de dados pessoais são obrigados a garantir a segurança da informação para proteção dos dados pessoais.

Segundo o previsto pelo caput do art. 46 da LGPD, a proteção dos dados pessoais é alcançada por meio de medidas de segurança, técnicas e administrativas.

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.
>
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados: a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
>
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. O art. 46, § 2º menciona que as medidas de

> segurança, técnicas e administrativas para proteção de dados pessoais deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Isso apresenta um conceito fundamental para a proteção da privacidade dos dados pessoais denominado Privacidade desde a Concepção.

O conceito de Privacidade desde a Concepção significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do tratamento de dados.

Tal privacidade pode ser alcançada por meio da aplicação dos 7 Princípios Fundamentais (Cavoukian, 2009) destacados a seguir:

1 - Proativo, e não reativo; preventivo, e não corretivo

A abordagem de Privacidade desde a Concepção (PdC) é caracterizada por medidas proativas e não reativas. Ou seja, essa abordagem antecipa e evita eventos invasivos de privacidade antes que eles aconteçam.

Desse modo, não espera que riscos de privacidade se materializem e antecipam soluções para as infrações de privacidade antes de sua ocorrência, de modo a impedir o evento danoso.

Em resumo, a Privacidade desde a Concepção vem antes do fato, não depois. Se aplicada a tecnologias da informação, práticas organizacionais, projeto físico ou em rede de ecossistemas de informação, a PdC começa com um reconhecimento explícito do valor e dos benefícios de adoção de práticas de privacidade fortes, de forma precoce e consistente.

2 - Privacidade deve ser o padrão dos sistemas de TI ou fluxos de serviços

A privacidade por padrão procura oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou fluxo de serviços. É uma forma de evitar que qualquer ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão.

Nesse passo, ressaltamos a importância do conhecimento e estreita aplicação do Provimento 74 do CNJ.

3 - Privacidade incorporada ao projeto (design)

A privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de TI e práticas de negócios. Isto significa que não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade.

Para alcançar esse objetivo, cada colaborador deve observar rigorosamente os fluxos de procedimentos desenvolvidos e, sempre que possível, devem propor revisões que possibilitem o constante aprimoramento do sistema como um todo.

4 - Funcionalidade total

A PdC não envolve simplesmente a formalização de declarações e compromissos de privacidade por parte dos colaboradores. Refere-se a satisfazer todos os objetivos da qualidade, não apenas os objetivos de privacidade. A PdC permite uma funcionalidade total, com resultados reais e práticos.

Ao incorporar privacidade em todas as etapas dos procedimentos internos da serventia, garantimos a proteção dos usuários dos serviços e uma maior qualidade nos nossos serviços. A questão da privacidade é frequentemente vista como de nenhuma ou baixa relevância. Essa visão é equivocada, pois a PdC visa justamente satisfazer todos os objetivos da serventia, tais como: qualidade, rapidez, eficiência, segurança jurídica e não apenas a garantia de privacidade para os titulares dos dados.

5 - Segurança e proteção de ponta a ponta

Por ser incorporada ao sistema antes do primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos na prestação dos serviços desta serventia.

Devem ser adotadas fortes medidas de segurança nos sistemas operacionais, tais como: firewall para a rede de computadores, login controlado por senha para acesso de qualquer colaborador, dentre outros. A privacidade deve ser protegida continuamente ao longo do ciclo de vida do tratamento dos dados em questão.

O princípio “Segurança” tem relevância especial nos serviços de registro e notariais porque, em sua essência, trabalhamos com cidadania e a segurança jurídica das partes.

Cada colaborador deve assumir a sua parcela de responsabilidade pela segurança dos dados pessoais dos usuários, durante todo o ciclo de tratamento, de modo consistente com os padrões que foram definidos nos organogramas padronizados para cada setor ou serviço. Os padrões de segurança aplicados devem garantir a confidencialidade, integridade e disponibilidade dos dados pessoais durante todo o seu ciclo de tratamento, incluindo, entre outros, métodos de destruição segura, criptografia apropriada, e métodos fortes de controle de acesso e registro.

Na LGPD, a segurança é um princípio a ser observado no tratamento de dados pessoais, destacado pelo art. 6º, inciso VII.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> VII - 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;

6 - Visibilidade e Transparência

A PdC objetiva garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente.

Importante que cada colaborador atente para a sua responsabilidade na coleta de dados pessoais, o que implica um dever de cuidado e de proteção.

7 - Respeito pela privacidade do usuário

Acima de tudo, a privacidade desde a concepção exige que cada um de nós respeite os direitos dos titulares dos dados pessoais.

De acordo com a LGPD o respeito à privacidade do titular dos dados pessoais é orientado pelos seguintes aspectos:

- Consentimento ou hipótese de tratamento prevista em lei - é necessário o consentimento livre e específico do titular dos dados para a coleta, uso ou divulgação de dados pessoais, exceto onde permitido por lei.

- Precisão - os dados pessoais devem ser precisos, completos e atualizados, conforme necessário para cumprir finalidades especificadas (constante atualização).
- Acesso - os titulares devem ter acesso aos seus dados pessoais e ser informados do uso e divulgação de tais dados. Para essa finalidade divulgamos na rede social Facebook e através de avisos afixados na serventia, a forma de uso e divulgação de dados.

PRIVACIDADE POR PADRÃO

Os agentes de tratamento (colaboradores da serventia) devem implementar medidas adequadas para garantir que, por padrão, apenas serão processados os dados pessoais necessários para cumprimento da(s) finalidade(s) específica(s) legalmente definida(s).

Essa obrigação de implementação significa que cada operador deve limitar a quantidade de dados pessoais coletados, a extensão do tratamento e acessibilidade ao mínimo necessário para a concretização da finalidade do tratamento dos dados pessoais. Essa medida deve garantir, por exemplo, que nem todos os usuários tenham acesso ilimitado e por tempo indeterminado aos dados pessoais tratados pelo cartório.

Na LGPD, a Privacidade por Padrão está diretamente relacionada ao princípio da necessidade, expresso pelo art. 6º, inciso III.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> III - necessidade: 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;

A privacidade por padrão é obtida por meio da adoção das seguintes práticas:

- Especificação da finalidade - os objetivos para os quais os dados pessoais são coletados, usados, retidos e divulgados devem ser comunicados ao titular dos dados no momento em que as informações são coletadas. As finalidades especificadas devem ser claras, limitadas e relevantes em relação ao que se pretende ao tratar os dados pessoais.
- Limitação da coleta - a coleta de dados pessoais deve ser legal e limitada ao necessário para os fins especificados.
- Minimização dos dados - a coleta dos dados pessoais que possa identificar individualmente o titular de dados deve obter o mínimo necessário de informações pessoais, de acordo com as exigências legais para a prática do ato pretendido.
- Limitação de uso, retenção e divulgação - o uso, retenção e divulgação de dados pessoais devem limitar-se às finalidades relevantes identificadas para o titular de dados, conforme exigência legal (p.ex. – fornecimento de certidão). Os dados pessoais serão retidos apenas pelo tempo necessário para cumprir as finalidades declaradas e depois eliminados com segurança, que deve ser triturado.

O presente documento é de conhecimento obrigatório para todos os colaboradores da serventia e complementa, no que couber, as demais informações/treinamentos já disponibilizados para todos os funcionários e estagiários.

POLITICA INTERNA DE SEGURANÇA DA INFORMAÇÃO

Conforme Art. 6º da LGPD, é recomendada a coleta de dados limitada para a realização dos atos.

- Conforme o Art. 7º da LGPD, o compartilhamento de dados com as centrais e outras entidades é definido por regulamentação própria. Nessa hipótese, o tratamento não precisa necessariamente ser baseado no consentimento, mas sim no cumprimento de obrigação legal ou regulatória.

○ Em última instância, utilizar outros embasamentos legais da LGPD, como o Consentimento.

○ Verifique se as empresas que prestam serviços de TI e ou backup em nuvem estão em conformidade com a LGPD e

○ Não utilizar usuários genéricos, como "usuário Balcão". Foram criados usuários pra acesso individualizado ao sistema, cada um com limitação aos dados que serão tratados.

○ Usuários e senhas são pessoais e intransferíveis.

○ Não deixar seu login aberto ao deixar a estação de trabalho. Os funcionários e estagiários que realizam o tratamento de dados são orientados e treinados para fechar sua tela, quando se ausentam da área de trabalho.

○ Os backups externos são feitos em dispositivos criptografados, executados e transportados pelo controlador, e ciente de suas responsabilidades perante a LGPD e Provimento nº 74 do CNJ.

○ Utilização de senhas fortes, não compartilhamento de usuário e senha com colegas.

● TI geral:

○ Conforme o Provimento nº 74 do CNJ, há um responsável técnico pela TI da serventia, que é a Empresa Solução Informática Ltda.

○ Os sistemas da Sky Informática possuem auditorias internas conforme o Provimento nº 74 do CNJ exige.

○ Ao receber mídias/arquivos externos por meio físico ou eletrônico, certificamo-nos de que estes não causem efeitos nocivos aos sistemas de computação. É realizada uma triagem em máquina com antivírus atualizado.

○ Conforme a própria LGPD, há um Encarregado (DPO).

○ A rede de computadores do cartório é servida por uma rede cabeada, exclusiva para os equipamentos. Há outra rede, com wifi disponibilizado ao público

○ Foi feito, juntamente com a TI um mapeamento de dados e processos para saber exatamente onde estão os dados, onde e

stão os riscos, e o que pode ser feito para mitigar incidentes.

○ Foram estabelecidos processos seguros, inclusive para as rotinas de manutenção de documentos impressos. Não são deixados fichas, livros, certidões e quaisquer documentos impressos em locais onde o público possa ter acesso.

○ Foi estabelecida segurança por camadas. No ambiente físico, como por exemplo acesso a sala de servidor, arquivos e gavetas com documentos importantes estão em salas e arquivos chaveados, ambiente da rede, nos sowares, etc.

○ Os provedores de serviços na nuvem estão em conformidade com a LGPD.

○ São utilizados hardwares e softwares com gestão centralizada.

Nos impressos da serventia:

○ São fragmentados os rascunhos com dados pessoais ou relevantes.

○ Os livros, certidões, fichas, tem acesso restrito.

○ Não são deixadas informações importantes em post-its ou expostos.

○ As segundas vias de recibo em local seguro e com acesso restrito.

○ É realizado o descarte correto de material impresso, de forma que inviabiliza a recuperação de dados, feita por máquina fragmentadora.

As informações das câmeras são mantidas no dispositivo que a acompanha, sobrepondo-se a cada quinze dias. O acesso às câmeras é restrito ao controlador e encarregado, pelo monitor e no celular.

Foram elaborados os procedimentos internos de Acesso aos Direitos dos Titulares

PROCEDIMENTOS INTERNOS DE ACESSO AOS DIREITOS DOS TITULARES

As ações adotadas para adaptação ao regime da Lei nº 13.709, de 2018, referente aos procedimentos internos de acesso aos direitos dos titulares que ficará arquivado neste Cartório para fins de fiscalização pelo juiz diretor do foro ou pela Corregedoria-Geral de Justiça.

As ações adotadas foram as seguintes:

- Foi nomeado ENCARREGADO para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), Leonardo da Mota Paim, sendo seu nome e contato devidamente divulgado no site do Cartório e em cartazes internos e externos;

- Foram orientados os prepostos, os prestadores de serviços terceirizados e o encarregado do Cartório sobre as formas de coleta, de tratamento e de compartilhamento de dados pessoais a que tiverem acesso, bem como sobre as respectivas responsabilidades, bem como sobre as práticas adotadas em relação à proteção de dados pessoais;

A orientação oferecida aos prepostos, aos prestadores de serviços terceirizados e ao encarregado do Cartório incluiu:

I – as medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito;

II – a informação de que a responsabilidade dos operadores prepostos, ou terceirizados, e de qualquer outra pessoa que intervenha em uma das fases abrangida pelo fluxo dos dados pessoais, subsiste mesmo após o término do tratamento;

III – a forma de comunicação com aqueles que forneçam os seus dados pessoais e com terceiros;

IV – o atendimento de eventuais solicitações dos direitos do titular de dados contido no art. 18 da Lei nº 13.709, de 2018, em prazo razoável.

Foram elaborados e estão sendo mantidos no Cartório:

I – sistema de controle do fluxo abrangendo a coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais, até a restrição de acesso futuro;

II – política de privacidade que descreva os direitos dos titulares de dados pessoais, de modo claro e acessível, os tratamentos realizados e a sua finalidade;

III – canal de atendimento adequado para informações, reclamações e sugestões ligadas ao tratamento de dados pessoais, com formulários específicos e fluxo de atendimento das requisições e/ou reclamações apresentadas, desde o seu ingresso até o fornecimento da resposta.

Foram, ainda, tomadas as seguintes medidas:

I – mapeamento das atividades de tratamento de dados pessoais por meio de formulário e questionário sobre os aspectos gerais da Lei nº 13.709, de 2018, que está devidamente arquivado na serventia;

II – condução da avaliação das vulnerabilidades e lacunas em relação à proteção de dados pessoais no que se refere às atividades desenvolvidas na serventia;

III – revisão e adequação dos contratos e convênios, internos e externos que tratam de compartilhamento de dados pessoais;

IV – realização de relatórios de impacto à proteção de dados pessoais referentes aos atos em que o tratamento desses dados gera risco a direitos e liberdades fundamentais;

V – adoção de medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito;

VI – implementação de sistemas de controle de fluxo, abrangendo coleta, tratamento, armazenamento e compartilhamento de dados pessoais, com o foco de proteger contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, prevendo a vedação do compartilhamento dos dados pessoais sem autorização específica, legal ou normativa e permissão, quando necessário, da elaboração dos relatórios de impacto previstos nos arts. 32 e 38 da Lei n. 13.709, de 2018;

VII - orientação a todos os prepostos e prestadores de serviços terceirizados sobre a necessidade de comunicação dos incidentes de segurança com dados pessoais imediatamente à Corregedoria Geral de Justiça e ao juiz diretor do foro da comarca, com esclarecimentos da natureza do incidente e das medidas adotadas, para a apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados;

VIII – exigência das empresas de automação de adequação às exigências da Lei nº 13.709, de 2018, quanto aos sistemas e programas de gestão de dados internos utilizados;

IX – orientação aos prepostos e divulgação nas redes sociais do cartório sobre o livre acesso dos titulares sobre o tratamento de seus dados pessoais, por intermédio de consulta facilitada e gratuita, que poderá abranger a exatidão, a clareza, a relevância, a atualização, a forma, a duração do tratamento e a integralidade dos dados; sendo que tal gratuidade não alcança a prática dos atos inerentes à prestação dos serviços notariais e de registros, e não abrangerá a emissão de certidões sobre as quais incidam emolumentos ou isenções na forma da lei específica;

X – orientação aos prepostos sobre a necessidade de exigir o fornecimento, por escrito, da identificação do solicitante e da finalidade da solicitação para a

expedição de certidão em inteiro teor ou quando forem solicitadas certidões ou informações em bloco, ou agrupadas, ou segundo critérios não usuais de pesquisa, ainda que relativas a registros e atos notariais envolvendo titulares distintos de dados pessoais;

XI- orientação aos prepostos sobre a expedição de nota de devolução quando houver solicitação de certidões e informações formuladas em bloco, relativas a registros e atos notariais do mesmo titular de dados pessoais ou de titulares distintos, quando as circunstâncias da solicitação indicarem a finalidade de tratamento de dados pessoais, pelo solicitante ou outrem, de forma contrária aos objetivos, fundamentos e princípios da Lei nº 13.709, de 2018;

XII – orientação aos prepostos sobre a exigência de identificação do solicitante para as informações que abranjam dados pessoais, quando se tratar de requerimento eletrônico, salvo se a solicitação for realizada por responsável ou preposto da serventia extrajudicial, na prestação do serviço público delegado;

XIII - orientação aos prepostos sobre necessidade de armazenamento em local com acesso controlado dos documentos físicos que contenham dados pessoais e dados pessoais sensíveis em salas ou compartimentos com controle de acesso;

XIV – orientação aos prepostos sobre a digitalização dos documentos físicos, respeitados disposições e prazos definidos no Provimento da Corregedoria Nacional de Justiça nº 50, de 28 de setembro de 2015, que “dispõe sobre a conservação de documentos nos cartórios extrajudiciais”;

XV – orientação aos prepostos sobre os deveres previstos na Lei nº 13.709, de 2018, em relação aos dados pessoais que remanescerem em índices, classificadores, indicadores, banco de dados, arquivos de segurança ou qualquer outro modo de conservação adotado na serventia extrajudicial, mesmo após a inutilização e eliminação de documentos físicos.

O Termo de Uso foi elaborado conforme os preceitos da LGPD – Ficam ambos arquivados na pasta própria no Tabelionato.

TERMO DA POLÍTICA DE PRIVACIDADE

Esta é a política de privacidade do **Segundo Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola**. Nesta Política, explicamos como tratamos os dados pessoais dos usuários, inseridos e fornecidos por quem utiliza dos serviços deste cartório.

A Lei nº 13.709/18, Lei Geral de Proteção de Dados ("LGPD"), é o primeiro marco regulatório abrangente sobre o tema de proteção de dados pessoais no Brasil e dispõe sobre o tratamento de dados pessoais, inclusive em meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A LGPD define como "dado pessoal" toda informação relacionada a uma pessoa natural identificada ou identificável, que doravante será chamado de "Dados". Tratamento de Dados significa quaisquer operações realizadas com Dados. Tais operações de tratamento incluem coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, armazenamento, arquivamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de Dados ("Tratamento"). A LGPD estabelece como fundamentos da proteção de Dados, além do respeito à privacidade e à inviolabilidade da intimidade, a liberdade de expressão, de informação, de comunicação e de opinião, assim como o desenvolvimento econômico e tecnológico, a inovação, a livre concorrência e a livre iniciativa.

Essa Política fala sobre o Tratamento de Dados pessoais e/ou outras informações fornecidas por você ao utilizar os serviços prestados por este Tabelionato e regula a forma como coletamos e usamos os seus dados, em obediência ao artigo 7º, § 3º da Lei 13.709/18.

1. **Comprometimento com a segurança dos seus Dados:** O 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola está comprometido com a segurança dos seus Dados Pessoais, assim sendo, os seus Dados serão

mantidos em sigilo e não serão compartilhados ou divulgados a terceiros, salvo nas hipóteses expressamente estabelecidas nesta Política e em aderência à legislação e/ou regulamentação vigente.

2. **Responsabilidade pela Qualidade e Transparência dos Dados que coletamos:** Você, ao utilizar os serviços, concorda expressamente em fornecer apenas Dados verdadeiros, atuais, completos e precisos e em não declarar dados falsos na utilização dos Serviços. Você será o único responsável pelas informações falsas, excessivas, incorretas, incompletas, ou imprecisas que nos forneceu e pelos danos, diretos ou indiretos, que isso cause ao 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola.

3. **Os Dados são coletados nas seguintes hipóteses:** (i) para o encaminhamento de escrituras (ii) para o encaminhamento de atos notariais (iii) quando fornecidos por outros titulares sobre você ou por você sobre outros titulares; obedecendo aos princípios norteadores da Lei 13.709/18, em especial ao da necessidade presente no inciso III do artigo 6º.

4. O 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola somente recebe ou coleta os seguintes tipos de informações relacionadas a você:

(1) **dados comuns:** (RG, CPF, Certidões, Certidões de estado civil, Cópia de matrícula de imóvel, Endereço, Profissão, e-mail, telefone, contas bancárias, dentre outros; (2) **dados sensíveis:** (imagens, biométricos; atas com informações sobre dados sindicais, partidos políticos, interditos, procurações de menores, declaratórias de União Homoafetiva).

5. **Dados que coletamos:** Podemos coletar dados pessoais durante o cadastro tais como: nome; número do CPF; número do RG ou documento equivalente; gênero; e-mail; número do telefone fixo ou celular; endereço residencial ou profissional; data do nascimento; idade; nome de usuário; profissão; estado civil; nacionalidade; local de nascimento; nome dos pais; nome do cônjuge; número

do CPF do cônjuge; código postal; país. Também coletamos, armazenamos e usamos determinadas categorias especiais de informações pessoais mais sensíveis, como: condição de exposição política (pessoa politicamente exposta), portador de necessidade especial, imagens e biometria.

6. **Utilizamos os seus Dados, para as seguintes finalidades**: agendar Atendimento no 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola, para o encaminhamento e lavratura de escrituras e atos notariais; de acordo com o artigo 7º, inciso III e o artigo 23, §§ 4º e 5º da Lei 13.709/18.

7. **Compartilhamento e divulgação dos Dados:** O 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola; não compartilha informações com terceiros particulares, exceto com as Centrais previstas em lei, Receita Federal, para encaminhamento da Declaração Sobre Operações Imobiliárias-DOI, CENSEC, TJ/RS para informações previstas em lei, Corregedoria Geral d Justiça do RS- CGJ/RS, Conselho Nacional de Justiça- CNJ, IBGE, COAF, Prefeitura Municipal para a informação das guias de ITBI e Fazenda Estadual, para encaminhar as guias de ITCD. Porém poderá, a qualquer tempo, fornecer dados ou informações relativas aos usuários a outros serviços públicos digitais cuja finalidade seja a efetiva prestação de serviço público pelo compartilhamento de dados ou informações ou atender demanda judicial ou policial ou por requisição do Ministério Público, conforme o artigo 7º, incisos III e VI, e o artigo 26, § 1º, I, III, IV e V, e § 2º da Lei 13.709/18.

8. **Nossas bases legais para uso dos Dados**: O 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola; realiza o tratamento de seus Dados de acordo com as bases legais previstas no artigo 7º, inciso III da LGPD.

9. **Armazenamento e exclusão dos Dados**: Os Dados são armazenados em ambiente seguro e controlado (Sky Remote Backup), por prazo estabelecido legal e/ou reguladoramente, sendo que para fins de auditoria, preservação de

direitos, ou se tivermos alguma outra razão legítima para mantê-los, podemos armazenar os Dados pelo período mínimo de 10 (dez) anos contados a partir do momento que os dados são armazenados conforme artigo 848 caput da Consolidação Normativa Notarial e Registral, e Provimento 50/2015- CNJ, podendo ser estendido por prazo maior nas hipóteses em que a lei e/ou norma regulatória assim estabelecerem ou para preservação de direitos. Contudo, podemos excluí-lo definitivamente segundo a nossa exclusiva conveniência em prazo menor. Os Dados podem ser armazenados em nossos servidores próprios ou de terceiro contratado para esse fim (Sky Remote Backup), de acordo com os critérios da legislação aplicável, podendo ainda serem armazenados por meios de tecnologia de cloud computing e/ou outras tecnologias que surjam futuramente, visando sempre a melhoria e aperfeiçoamento de nossos serviços.

10. **Seus direitos, opções e controles**: Nos termos das leis e regulamentos relativos à proteção de dados pessoais, incluindo, mas não se limitando a LGPD, você possui direitos e garantias em relação aos seus Dados.

Confirme e acesse seus Dados: você poderá requisitar detalhes e/ou cópia dos Dados a seu respeito guardados por nós, pelo endereço eletrônico: segundotabelionatto@hotmail.com, tabelionatoespindola@gmail.com ou através de requerimento expresso do titular ou de representante legalmente constituído, diretamente no endereço do Tabelionato, a saber: Rua Nossa Senhora do Carmo, 130, Sala 103, Centro, Alegrete-RS.

11. **Altere ou corrija seus Dados**: Caso deseje, você pode revogar consentimentos, eliminar, bloquear, pedir a anonimização ou a portabilidade de seus Dados: você poderá revogar o seu consentimento, sempre que o tratamento de Dados se basear em consentimento, nos termos da LGPD ou solicitar a exclusão de seus Dados, a qualquer momento, nos termos legais. Armazenamos o seu histórico: você poderá entrar em contato com o 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola; assim como nós estamos autorizados a entrar em contato com você, para que você possa acessar certas funcionalidades de nossos Serviços, tirar dúvidas, fazer reclamações ou sugestões, por meio do e-mail segundotabelionatto@hotmail.com, tabelionatoespindola@gmail.com ou dos

telefones (55) 34223300 ou (55) 997274939. As conversas serão armazenadas por nós e poderemos utilizar seu conteúdo como meio de prova em juízo, para prestação de nossos Serviços, ou nas demais hipóteses previstas em lei.

12. **Segurança da Internet:** Destacamos que a transmissão de Dados pela internet não é completamente segura por diversos fatores, incluindo fatores de rede e de operação, e o 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola; não tem como garantir a completa segurança dos dados transmitidos por esta via, uma vez que o compartilhamento de dados se dá com o Poder Público e há situações em que, por exemplo, o Tribunal de Justiça do Estado, que é uma das instituições a quem enviamos dados, teve, recentemente, seus dados hackeados.

O Controlador responsabiliza-se pela manutenção de medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

Em conformidade ao art. 48 da Lei nº 13.709, o Controlador comunicará ao Titular e à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao Titular.

13. **Alterações a essa Política:** O 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola poderá alterar o conteúdo desta Política a seu exclusivo critério e a qualquer tempo, sendo certo que a versão atualizada estará disponível nas plataformas.

14. **Cookies:** Não utilizamos cookies na coleta de dados, nosso provedor é apenas de acesso à internet, o que pode ser comprovado diretamente com a empresa RCT – Rede Conesul Telecom.

15. **Canais de Relacionamento**: Segundo a LGPD, o 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola tem o titular considerado

como "Controlador" dos seus Dados, conforme o artigo 5º, inciso VI da Lei 13.709/18.

E o seu Encarregado de Dados é o Tabelião Substituto Leonardo da Mota Paim.

Se após a leitura desta Política você ainda tiver qualquer dúvida, sobre assuntos envolvendo os seus Dados, você pode falar com a gente pelos canais abaixo:
(i) E-mail : segundotabelionatto@hotmail.com, tabelionatoespindola@gmail.com
(ii) Telefones: (55) 34223300 ou (55) 997274939.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

1) DESCRIÇÃO DOS TIPOS DE DADOS COLETADOS E TRATADOS:

1.1) Para elaborar o cadastro e atualização dos dados do usuário:

Nome completo;

Data de Nascimento;

Nome dos pais;

Foto;

Número de CPF;

Endereço de e-mail;

Número de celular;

Data de nascimento;

Estado civil;

Profissão

Biometria

Dados referentes aos seus endereços.

1.2) Para lavratura de atas notariais, escrituras e procurações:

Nome completo;

Data de Nascimento;

Nome dos pais;

Foto;

Número de CPF;

Endereço de e-mail;

Número de celular;

Data de nascimento;

Estado civil;

profissão

Biometria;

Dados referentes aos seus endereços físico e virtual;

Acesso a redes sociais para elaboração da ata notarial

Acesso a conversas de WhatsApp;

Vídeo;

Áudio.

Demais documentos necessários para a elaboração dos instrumentos

2) METODOLOGIA UTILIZADA PARA COLETA

Todos os dados solicitados através do atendimento ao cliente, salvo especificado de outra forma, são obrigatórios, e o não fornecimento desses dados poderá impossibilitar o fornecimento dos serviços por parte do Tabelionato.

Os dados serão coletados através da apresentação de documentos, que serão digitalizados no sistema NOTAR, da empresa SKY INFORMÁTICA LTDA.

Os documentos podem ser apresentados fisicamente ou ser enviados através do email do Tabelionato ou pelo WhatsApp, mantidos exclusivamente para a utilização pela Serventia. Estes dados são coletados pelos atendentes ou pela escrevente e pelo substituto.

Ao solicitar e fornecer os dados durante a realização de algum serviço, o cliente dará o seu consentimento para coleta dos dados de número de telefone e endereço de e-mail, para que possam ser usados para comunicações ou notificações por e-mail ou mensagem, em relação aos serviços vinculados a sua pessoa. Estes dados serão solicitados no protocolo de atendimento do serviço e inseridos no sistema do Tabelionato, em observância aos requisitos legais relacionados a comunicação do cliente e cumprimento do Provimento nº 74/2018/CNJ, Provimento 88/2019/CNJ e a Lei nº 13.709/2018.

A comunicação será realizada quando for necessário comunicar ao usuário de algum fato relevante sobre a movimentação dos serviços solicitados;

O usuário que não consentir com a disponibilização das informações dos dados deverá entrar em contato com o Tabelionato para ter conhecimento do andamento dos serviços solicitados ou vinculados a sua pessoa, através dos canais de atendimento disponíveis.

3) METODOLOGIA DE GESTÃO DE RISCOS E SEGURANÇA A INFORMAÇÃO

3.1. - Controle de acesso às instalações do cartório, com restrição de acesso a terceiros estranhos ao quadro funcional nas áreas de tratamento de dados.

3.2. - Separação física do setor de arquivo, com limitação de acesso e restrição de autorização para manipulação dos documentos arquivados.

3.3. - Controle de acesso à rede de informática do cartório, mediante identificação de usuário e senha.

3.4. - Controle de acesso ao sistema de gestão da informação do cartório, mediante classificação de perfis de acesso, com categorias de autorização de funções.

3.5. - Restrição de acesso aos servidores e banco de dados, com identificação do usuário e limitação amplitude de acesso.

3.6. - Identificação do interessado quando da entrega de documentos lavrados, registrados ou cópias de documentos arquivados, garantindo que a pessoa seja a titular da informação.

3.7. - Utilização de dados pessoais mínimos conforme exigências e requisitos das leis e regulamentos que normatizam a atividade registral.

3.8. - Espelhamento local dos dados e realização de backups locais e remotos para garantia da integridade do banco de dados.

3.9. - Limitação do acesso remoto ao banco de dados.

3.10. - Utilização de sistemas de firewall e anti-vírus robustos e adequados ao nível de segurança da rede e dos sistemas.

3.11. - Monitoramento constante da rede, sistemas e programas instalados, bem como tentativas de invasão e identificação de falhas ou defesas frágeis.

3.12. - Treinamento, conscientização e comprometimento de todos os colaboradores na gestão da segurança das informações.

3.13. - Contratação de empresa especializada para implementação, monitoramento e auditoria dos sistemas de controle e segurança da informação.

4) ANÁLISE DO CONTROLADOR COM RELAÇÃO À MEDIDAS, SALVAGUARDAS E MECANISMOS DE MITIGAÇÃO DE RISCOS ADOTADOS. (FAZER PLANILHA)

4.1. - Como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados:

Os dados serão coletados através da apresentação de documentos, que serão digitalizados no sistema NOTAR, da empresa SKY INFORMÁTICA LTDA. Os documentos podem ser apresentados fisicamente ou ser enviados através

do e-mail do Tabelionato ou pelo WhatsApp, mantidos exclusivamente para a utilização pela Serventia. Estes dados são coletados pelos atendentes ou pela escrevente e pelo substituto.

São armazenados no banco de dados através do Sistema Notar, com impressão da ficha padrão e coleta de assinatura que é digitalizada no sistema e arquivada. As cópias de documentos apresentados são arquivados em livros próprios, bem como digitalizados no sistema do cartório.

Estes dados são armazenados em nuvem do Sky Remote, da empresa Sky Informática Ltda e em HD externo, que fica em mãos do controlador.

Além destes dados, são coletadas imagens pela câmera de segurança, que fica armazenada internamente durante 15 dias, sendo descartadas as imagens automaticamente após este tempo.

O acesso às câmeras é limitado ao controlador, ao encarregado de dados, através de monitor interno e no celular.

4.2. - Fonte de dados utilizada para coleta dos dados pessoais:

Os dados serão coletados através da apresentação de documentos, que serão digitalizados no sistema NOTAR, da empresa SKY INFORMÁTICA LTDA. Os documentos podem ser apresentados fisicamente ou ser enviados através do e-mail do Tabelionato ou pelo WhatsApp, mantidos exclusivamente para a utilização pela Serventia. Estes dados são coletados pelos atendentes ou pela escrevente e pelo substituto.

4.3. Com quais órgãos, entidades ou empresas dados pessoais são compartilhados e quais são esses dados:

Tribunal de Justiça do Estado do RS- TJ/RS- envio de arquivos de selos digitais, com valores, recibos, extratos de receita e despesa, CENSEC- Envio de relatórios de escrituras lavradas, testamentos com nome, CPF, data, livro e folha lavrados.

IBGE

4.4. Quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam:

- Funcionários e estagiários:
- Coleta, retenção, processamento, compartilhamento e eliminação: Caroline Cassol Marques e Leonardo da Mota Paim
- Coleta: Ernesto Rodrigues Custódio, Gabrielly Guterres Alves e estagiários.
- Dados dos funcionários: Escritório de Contabilidade Loebler

4.5. Se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais:

A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso.

A tecnologia adotada diz respeito ao que determina o Provimento 74/2018 e às medidas de segurança já mantidas no Tabelionato.

4.6. Medidas de segurança atualmente adotadas:

- Backup em nuvem no Sistema Sky Remote.

- Eliminação de documentos, informações e material não utilizado, quando em papel, através de fragmentação.

- Treinamento dos funcionários e estagiários para adequação a políticas de manuseio de documentos, descarte adequado, tratamento dos dados de forma sigilosa.

- Mudança na disposição das mesas e equipamentos do salão de atendimento, para que os clientes e usuários não tenham a visão das telas dos computadores.

- Salas dos arquivos do acervo e do servidor e replicador mantidas fechadas à chave.

- Acesso limitado aos funcionários e estagiários das dependências do tabelionato onde se lavram os atos.

- Sala de leitura e entrega de documentos públicos privativa.

- Acesso das câmeras limitado ao tabelião e ao encarregado.

TERMO DE TRATAMENTO DE DADOS PESSOAIS

O 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola está comprometido com a segurança dos Dados Pessoais dos usuários, colaboradores e terceiros, assim sendo, os Dados deverão ser mantidos em sigilo e não serão compartilhados ou divulgados a terceiros, salvo nas hipóteses expressamente estabelecidas em Lei e em aderência à legislação e/ou regulamentação vigente.

Os Dados são coletados nas seguintes hipóteses**:** (i) para o encaminhamento de escrituras (ii) para o encaminhamento de atos notariais (iii) quando fornecidos por outros titulares sobre você ou por você sobre outros titulares; obedecendo aos princípios norteadores da Lei 13.709/18, em especial ao da necessidade presente no inciso III do artigo 6º.

O 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola somente recebe ou coleta os seguintes tipos de informações relacionadas ao titular:

(1) **dados comuns:** (RG, CPF, Certidões, Cópia de matrícula de imóvel, Endereço, Profissão, e-mail, telefone, contas bancárias, estado civil;

(2) **dados sensíveis:** (imagens, biométricos; atas com informações sobre dados

sindicais, partidos políticos, interditos, procurações de menores, declaratórias de União Homoafetiva).

Podem ser coletados dados pessoais durante o cadastro tais como: nome; número do CPF; número do RG ou documento equivalente; gênero; e-mail; número do telefone fixo ou celular; endereço residencial ou profissional; data do nascimento; idade; nome de usuário; profissão; estado civil; nacionalidade; local de nascimento; nome dos pais; nome do cônjuge; número do CPF do cônjuge; código postal; país; idiomas; curso; paga pensão; valor da pensão.

Também coletamos, armazenamos e usamos determinadas categorias especiais de informações pessoais mais sensíveis, como: condição de exposição política (pessoa politicamente exposta), portador de necessidade especial, imagens e biometria.

Utilizamos os Dados Pessoais, para as seguintes finalidades: agendar Atendimento no 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola, para o encaminhamento de escrituras e atos notariais, para reconhecimento de assinaturas, sendo determinado por lei que o tabelião deve identificar a parte e atestar sua capacidade, de acordo com o artigo 7º, inciso III e o artigo 23, §§ 4º e 5º da Lei 13.709/18.

TERMOS DE USO

ACEITAÇÃO DOS TERMOS E POLÍTICAS DE PRIVACIDADE DA PÁGINA DO FACEBOOK E DOS SERVIÇOS CARTORIAIS DO 2º TABELIONATO ESPINDOLA DA COMARCA DE ALEGRETE-RS

Ao utilizar os serviços, o usuário confirma que leu e compreendeu os Termos e Políticas aplicáveis a ele e concorda em ficar vinculado a eles.

DEFINIÇÕES

Para os fins destes Termos de Uso e Política de Privacidade, consideram-se:

Agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública, direta e indireta;

Agentes de Estado: inclui órgãos e entidades da Administração pública além dos seus agentes públicos;

Códigos maliciosos: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

Sítios e aplicativos: sítios e aplicativos por meio dos quais o usuário acessa os serviços e conteúdos disponibilizados;

Terceiro: pessoa ou entidade que não participa diretamente em um contrato, em um ato jurídico ou em um negócio, ou que, para além das partes envolvidas, pode ter interesse num processo jurídico;

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;

Usuários (ou "Usuário", quando individualmente considerado): todas as pessoas naturais que utilizarem o serviço (citar o serviço);

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

ARCABOUÇO LEGAL

O Arcabouço legal aplicável ao serviço notarial, do 2º Tabelionato de Alegrete compreende:

1. Lei Geral de Proteção de Dados Pessoais (LGPD) - LEI 13.709, DE 14 DE AGOSTO DE 2018;

2. Marco civil da internet — LEI Nº 12.965, DE 23 DE ABRIL DE 2014;

3. Decreto da Governança no Compartilhamento de Dados - DECRETO Nº 10.046, DE 9 DE OUTUBRO DE 2019;

4. Normas complementares do Gabinete de Segurança da Informação da Presidência (GSI/PR);

5. Decreto que institui a Estratégia de Governo Digital - DECRETO Nº 10.332, DE 28 DE ABRIL DE 2020;

6. Lei nº 13.460, de 26 de junho de 2017 Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública;

7. Decreto nº 7.724, de 16 de maio de 2012 Regulamenta a Lei no 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), que dispõe sobre o acesso a informações previsto na Constituição;

8. Provimento nº 74 da Corregedoria Nacional da Justiça - CNJ de 31 de julho de 2018;

9. Provimento 134 da Corregedoria Nacional de Justiça- CNJ de 24 de agosto de 2022;

DESCRIÇÃO DO SERVIÇO

Dados que coletamos: Podemos coletar dados pessoais durante o cadastro tais como: nome; número do CPF; número do RG ou documento equivalente; gênero; e-mail; número do telefone fixo ou celular; endereço residencial ou profissional; data do nascimento; idade; nome de usuário; profissão; estado civil; nacionalidade; local de nascimento; nome dos pais; nome do cônjuge; número do CPF do cônjuge; código postal; país.

Também coletamos, armazenamos e usamos determinadas categorias especiais de informações pessoais mais sensíveis, como: condição de exposição política (pessoa politicamente exposta), portador de necessidade especial, imagens e biometria.

Utilizamos os seus Dados para as seguintes finalidades: agendar Atendimento no 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola, para o encaminhamento de escrituras e atos notariais, de acordo com o artigo 7º, inciso III e o artigo 23, §§ 4º e 5º da Lei 13.709/18.

Para a lavratura dos atos também são utilizados os dados coletados, que fazem parte do instrumento público.

Compartilhamento e divulgação dos Dados: O 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola, não compartilha informações com terceiros particulares. Porém poderá, a qualquer tempo, fornecer dados ou informações relativas aos usuários a outros serviços públicos digitais cuja finalidade seja a efetiva prestação de serviço público pelo compartilhamento de

dados ou informações, como as Centrais Registrais e Notariais (CENSEC, TJ/RS, CNJ, ANOREG, CENTRAL DE TESTAMENTOS, COLÉGIO NOTARIAL, IBGE E COAF) ou atender demanda judicial ou policial ou por requisição do Ministério Público, conforme o artigo 7º, incisos III e VI, e o artigo 26, § 1º, I, III, IV e V, e § 2º da Lei 13.709/18.

Nossas bases legais para uso dos Dados: O 2° Tabelionato de Notas da Comarca de Alegrete-RS – Tabelionato Espindola, realiza o tratamento de seus Dados de acordo com as bases legais previstas no artigo 7º, inciso III da LGPD.

Armazenamento e exclusão dos Dados: Os Dados são armazenados em ambiente seguro e controlado (Sky Remote Backup), por prazo estabelecido legal e/ou reguladoramente, sendo que para fins de auditoria, preservação de direitos, ou se tivermos alguma outra razão legítima para mantê-los, podemos armazenar os Dados pelo período mínimo de 10 (dez) anos contados a partir do momento que os dados são armazenados conforme artigo 848 caput da Consolidação Normativa Notarial e Registral, podendo ser estendido por prazo maior nas hipóteses em que a lei e/ou norma regulatória assim estabelecerem ou para preservação de direitos. Contudo, podemos excluí-lo definitivamente segundo a nossa exclusiva conveniência em prazo menor. Os Dados podem ser armazenados em nossos servidores próprios ou de terceiro contratado para esse fim (Sky Remote Backup), de acordo com os critérios da legislação aplicável, podendo ainda serem armazenados por meios de tecnologia de cloud computing e/ou outras tecnologias que surjam futuramente, visando sempre a melhoria e aperfeiçoamento de nossos serviços.

DIREITOS DO USUÁRIO

Seus direitos e preferências:

Garantimos opções de escolha e controle, o Regulamento Geral sobre Proteção de Dados ou "RGPD" confere certos direitos às pessoas físicas no que

diz respeito aos seus dados pessoais. Dessa forma, buscamos garantir transparência e controles de acesso a fim de permitir aos usuários se beneficiar dos direitos mencionados. Os direitos conferidos às pessoas físicas, sem prejuízo das limitações previstas na legislação aplicável, são os seguintes:

Direito de acesso - o direito de ser informado e solicitar acesso aos dados pessoais processados por nós;

Direito de retificação - o direito de solicitar que alteremos ou atualizemos os seus dados pessoais quando os mesmos estiverem incorretos ou incompletos;

Direito de remoção - o direito de solicitar a remoção de seus dados pessoais; Neste caso, os atos cartorários não poderão ser lavrados;

Direito de restrição - o direito de solicitar que deixemos, temporária ou permanentemente, de processar todos ou alguns dos seus dados pessoais;

Direito de oposição - o direito, a qualquer momento, de se opor ao processamento dos seus dados pessoais por motivos relacionados à sua situação particular; o direito de se opor à manipulação dos seus dados pessoais para fins de marketing direto;

Direito à portabilidade de dados - o direito de solicitar uma cópia dos seus dados pessoais em formato eletrônico e o direito de transmitir os referidos dados pessoais para utilização no serviço de terceiros. Esta solicitação somente poderá ser atendida mediante autorização judicial.

Direitos do Titular

O Titular tem direito a obter do Controlador, em relação aos dados por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei nº 13.709;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador e expressa autorização judicial;

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei nº 13.709;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º da Lei nº 13.709. Direito de Revogação do Consentimento. Este consentimento poderá ser revogado pelo Titular, a qualquer momento, mediante solicitação via e-mail ou correspondência ao Controlador. A consequência será a impossibilidade de prestar o serviço cartorário ao usuário.

RESPONSABILIDADES DO USUÁRIO E DA ADMINISTRAÇÃO PÚBLICA

USUÁRIO

O Usuário se responsabiliza pela precisão e veracidade dos dados informados no cadastro e reconhece que a inconsistência destes poderá implicar a impossibilidade de utilizar serviços públicos do Governo Federal. O login e senha só poderão ser utilizados pelo usuário cadastrado. Este deve manter o sigilo da senha, que é pessoal e intransferível, não sendo possível, em qualquer hipótese, a alegação de uso indevido, após o ato de compartilhamento.

O usuário da Plataforma é responsável pela atualização das suas informações pessoais e consequências na omissão ou erros nas informações pessoais cadastradas. O Usuário é responsável pela reparação de todos e quaisquer danos, diretos ou indiretos (inclusive decorrentes de violação de quaisquer direitos de outros usuários, de terceiros, inclusive direitos de

propriedade intelectual, de sigilo e de personalidade), que sejam causados à Administração Pública Federal (APF), a qualquer outro Usuário, ou, ainda, a qualquer terceiro, inclusive em virtude do descumprimento do disposto nestes Termos de Uso e Política de Privacidade ou de qualquer ato praticado a partir de seu acesso à Internet, ao sítio e/ou Aplicativo. O Órgão não poderá ser responsabilizado pelos seguintes fatos:

a. Equipamento infectado ou invadido por atacantes;

b. Equipamento avariado no momento do consumo de serviços;

c. Proteção do computador;

d. Proteção das informações baseadas nos computadores dos usuários;

e. Abuso de uso dos computadores dos usuários;

f. Monitoração clandestina do computador dos usuários;

g. Vulnerabilidades ou instabilidades existentes nos sistemas dos usuários;

h. Perímetro inseguro;

ADMINISTRAÇÃO PÚBLICA

A Administração Pública, no papel de custodiante das informações pessoais dos Usuários, deve cumprir todas as legislações inerentes ao uso correto dos dados pessoais do cidadão de forma a preservar a privacidade dos dados utilizados na plataforma.

Publicar e informar ao Usuário as futuras alterações a estes Termos de Uso e Política de Privacidade por meio da página do Facebook (tabelionatoespindola), instagran (@tabelionatoespindola) conforme o princípio da publicidade estabelecido no artigo 37, caput, da Constituição Federal. Em nenhuma hipótese, a Administração Pública Federal será responsável pela instalação no equipamento do Usuário ou de terceiros, de códigos maliciosos (vírus, trojans, malware, worm, bot, backdoor, spyware, rootkit, ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo Usuário.

MUDANÇAS NOS TERMOS DE USO

RESPONSABILIDADES:

ADMINISTRAÇÃO PÚBLICA FEDERAL

Publicar e informar ao Usuário as futuras alterações a estes Termos de Uso e Política de Privacidade por meio da página do Facebook (tabelionatoespindola), Instagran (@tabelionatoespindola) conforme o princípio da publicidade estabelecido no artigo 37, caput, da Constituição Federal.

DAS ALTERAÇÕES E ATUALIZAÇÃO DESTES TERMOS DE USO

Esta política tem validade indeterminada, podendo ser alterada em seus termos, a qualquer tempo, e a versão deste termo de uso será vinculada no ato da aceitação do usuário.

INFORMAÇÕES PARA CONTATO

Se após a leitura destes Termos você ainda tiver qualquer dúvida, sobre assuntos envolvendo os seus Dados, você pode falar com a gente pelos canais abaixo:

(i)E-mail: segundotabelionatto@hotmail.com, tabelionatoespindola@gmail.com

(ii) Telefones: (55) 34223300 ou (55) 997274939.

FORO

Quaisquer disputas ou controvérsias oriundas de quaisquer atos praticados no âmbito da utilização dos sítios e/ou aplicativos pelos usuários, inclusive com relação ao descumprimento dos Termos de Uso e Política de Privacidade ou pela violação dos direitos da Administração Pública Federal, de outros Usuários e/ou de terceiros, inclusive direitos de propriedade intelectual, de sigilo e de personalidade, serão processadas na Comarca de Alegrete-RS.

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

Sumário:

1. OBJETIVO
2. ABRANGÊNCIA
3. DIRETRIZES DE GOVERNANÇA
4. PAPÉIS E RESPONSABILIDADES DO ENCARREGADO A INCIDENTES DE SEGURANÇA
5. INCIDENTES QUE SERÃO CONSIDERADOS
6. RECUPERAÇÃO
7. DISPOSIÇÕES FINAIS

1. OBJETIVO

Definir o plano de resposta a incidente de segurança do 2º Tabelionato de Alegrete.

Atender à Lei de Registros Públicos, Lei n. 8935/1994, Lei 13.709/2018 LGPD e Provimento 134/2022- CNJ

2. ABRANGÊNCIA

Esta Norma é um documento interno, com valor jurídico e aplicabilidade imediata, plena e indistinta. Ela deve ser de conhecimento e aplicação exclusiva ao encarregado nomeado pelo Tabelião.

3. DIRETRIZES DE GOVERNANÇA

O Encarregado de LGPD deve dispor de uma estrutura formalmente constituída de governança.

O Encarregado tem o papel fundamental de estipular e garantir a aderência às diretrizes da segurança da informação e privacidade de dados, além de auxiliar no estabelecimento de controles de segurança adequados para cada área.

4. PAPÉIS E RESPONSABILIDADES DO ENCARREGADO A INCIDENTES DE SEGURANÇA

O plano de resposta a incidentes de segurança com dados pessoais prevê a comunicação ao Juiz Diretor do Foro, a Corregedoria Geral da Justiça/RS, e à Autoridade Nacional de Proteção de Dados, no prazo máximo de 48 horas, nos termos do artigo 13 do Provimento 134, do CNJ, com esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados.

Os incidentes de segurança com dados pessoais serão imediatamente comunicados pelos operadores ao controlador.

5. INCIDENTES QUE SERÃO CONSIDERADOS (ROL MERAMENTE EXEMPLICATIVO)

O encarregado deverá levantar o máximo de informação possível a respeito do incidente, identificando, por exemplo:

-Qual foi a causa do incidente;

-Quais foram as vulnerabilidades exploradas ou que levaram ao incidente;

-Se houve o uso de credenciais comprometidas e quais são essas credenciais;

-Quais sistemas, equipamentos e redes foram comprometidos;

-Quais setores do tabelionato foram afetados;

-Se houve exposição, transferência ou sequestro de dados;

-Quais dados e quais titulares, exatamente, foram afetados; etc.

Será documentado o incidente ainda que seja feita a opção pela não comunicação, como forma de demonstrar a conformidade com a lei, exibindo-se as razões pelas quais foi feita esta opção.

5.1. Contenção e erradicação

Essa é a fase de conter e erradicar o incidente, limitando os danos. A ação depende do incidente específico, mas o objetivo é evitar que ele cause mais prejuízos do que já causou.

Isso implica atuar na raiz do incidente e estabelecer formas de contenção (podendo até mesmo ser necessário desabilitar sistemas inteiros). Será importante, nesta etapa, procurar preservar as evidências que possam ajudar a identificar melhor o que ocorreu e os eventuais responsáveis.

6. RECUPERAÇÃO

Depois que o incidente estiver contido e erradicado, serão restaurados dados e serviços.

Essa etapa pode incluir a restauração de backups, clonagem de máquinas virtuais e reinstalação de sistemas, dentre outras medidas.

7. DISPOSIÇÕES FINAIS

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com a Política e outras Normas e Procedimentos aplicáveis e relevantes adotados pela serventia.