Ofício de Notas e Registros da Comarca Vinculada de Altaneira/CE – Cartório Regis

**POLÍTICA DE PRIVACIDADE E DE PROTEÇÃO DE DADOS PESSOAIS**

ALTANEIRA/CE, 01/08/2022.

**MANUAL DE POLÍTICA E IMPLEMENTAÇÃO DA LGPD.**

**1) DISPOSIÇÕES PRELIMINARES**

Em respeito à Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/18) bem como às normas pertinentes à matéria (Provimento 50/CNJ; Provimento 74/CNJ; Provimento 88/CNJ; Instrução Normativa RFB nº 1111/2010; Lei nº 6.015/73), publica-se esta Política de Privacidade de Dados, que norteará todo tratamento que ocorrer nesta serventia.

As serventias extrajudiciais estão sujeitas a um regime híbrido de tratamento de dados pessoais, pois exercem privativamente uma função pública, em regime de delegação (art. 236 CF). Enquanto a atividade fim da serventia está sujeita ao regime público do art. 23, §4º da LGPD, o gerenciamento administrativo e financeiro da serventia é nitidamente privado.

Desse modo, o OFÍCIO DE NOTAS E REGISTROS DA COMARCA VINCULADA DE ALTANEIRA/CE – CARTÓRIO REGIS interage com diferentes tipos de usuários em diferentes circunstâncias, que podem implicar em tratamento de dados pessoais:

• **Atendimento presencial dos Usuários do Cartório** - Dados pessoais são fornecidos diretamente pelo usuário no atendimento em balcão para que sejam realizados diversos atos notariais ou para a realização de consulta de informações dos livros e arquivos da serventia.

• **Atendimento remoto dos Usuários pela Plataforma do E-Notariado** – Dados pessoais são fornecidos diretamente pelo usuário por intermédio da plataforma para a remissão de solicitações à serventia para que sejam realizados atos notariais, de maneira remota.

• **Funcionários, Candidatos e Prestadores de Serviços** - No contexto de relações de trabalho, prestação de serviços ou de atividades de recrutamento, quando atuar enquanto empregador ou potencial empregador ou contratante de serviços, dados pessoais poderão ser tratados para fins de comunicação, recrutamento, manutenção de banco de currículos e/ou cumprimento de obrigações trabalhistas e fiscais.

Em observância ao que determina a LGPD, o OFÍCIO DE NOTAS E REGISTROS DA COMARCA VINCULADA DE ALTANEIRA/CE – CARTÓRIO REGIS torna pública a identidade do seu encarregado, para envio de eventual comunicação, pedidos de esclarecimentos ou exercício de quaisquer dos direitos previstos nesta Política:

**Encarregado Interno (DPO): BRENDA LOPES DE LIMA REGIS**

E-mail do Encarregado: lgpdcartorioregisdealtaneira@gmail.com

**Funções do responsável pela proteção de dados da empresa (DPO) (Conforme art. 5º, VIII, art. 41, § 2º e 48 da LGPD):**

1) Prestar esclarecimentos e adotar providências das demandas dos titulares, no prazo de até 15 dias da solicitação (Art. 19, II);

2) Receber e responder as comunicações da Autoridade Nacional de Proteção de Dados (ANPD);

3) Orientar e capacitar funcionários e contratados quanto às boas práticas de proteção de dados;

4) Quando solicitado, emitir Relatório de Impacto para a ANPD, em nome do Controlador, que é responsável pelas decisões a respeito do tratamento de dados;

5) Emitir Notificação de Incidente para a ANPD e titulares dos dados afetados;

6) Executar as demais atribuições determinadas pelo controlador e as estabelecidas em normas complementares editadas pela ANPD.

**Obrigações:**

Existem algumas obrigações relacionadas a incidentes que podem causar risco ou dano relevante ao titular do dado:

Comunicação, dentro de um prazo razoável, à Autoridade de Proteção de Dados e ao titular do dado (descrição do dado afetado, informações sobre o titular do dado, indicação de medidas técnicas e seguranças para proteção dos dados pessoais, etc);

A Autoridade de Proteção de Dados verificará a seriedade do incidente e pode requerer obrigações adicionais;

É importante realizadas medidas adequadas e técnicas para impedir o acesso de terceiros ao dado;

Responsabilidade dos agentes de tratamento: LGPD criou uma isenção de responsabilidade aos agentes de tratamento quando provado que o dano foi exclusivamente causado pelo titular do dano ou algum terceiro.

LGPD diz que deve haver um Encarregado para agir como um canal de comunicação entre os titulares dos dados e a Autoridade de Proteção de Dados.

**Demais observações:**

Titulares de dados pessoais de outras operações de tratamento realizadas pela serventia que não estejam contempladas nesta Política também poderão entrar em contato com seu Encarregado de Proteção de Dados para vindicar maiores informações sobre os tratamentos realizados, em prestígio à autodeterminação informativa.

Este *cartorioregis.com.br* possui, a fim de trazer uma maior facilidade ao usuário, links para sites de serviços que não operados por esta serventia e, portanto, não se encontram sob a sua responsabilidade. O usuário reconhece estar ciente que não poderá haver eventual responsabilização desta serventia por questões ligadas a tais websites.

**LGPD: do que se trata?**

A lei nº 13.709/2018 entrará em vigor em agosto de 2020 e disciplina como os dados pessoais de pessoas físicas podem ser tratados fisicamente ou por meio digital por terceiros, fixando limites e procedimentos.

**Qual o objetivo da Lei?**

“*Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.*”

A Lei é aplicável a qualquer operação de tratamento realizada, independente do meio, do país de sua sede ou do país onde estejam localizados os dados.

**Propósito:**

a) Regulamenta - O uso, a proteção e a transferência de dados pessoais no Brasil;

b) Globalização - A lei está alinhada às regulamentações internacionais, como GDPR (em vigor desde mai/18);

c) Define Regras - Para a segurança, transparência, confidencialidade de dados, privacidade e proteção de informações pessoais na coleta, armazenamento e tratamento dos dados por empresas e órgãos públicos.

**Alguns dados importantes sobre a questão da segurança dos dados[[1]](#footnote-1):**

-> Como se gerencia uma violação de dados no Brasil?

- 43% É a chance de enfrentarmos uma violação. É a maior do mundo (~ 27%);

- 46% Das violações foram ataques maliciosos ou criminosos;

- 100 dias É o tempo necessário para conter cada violação;

- 240 dias É o tempo médio para identificar uma violação.

**O que muda com a LGPD?**

Os cidadãos poderão saber como os cartórios tratam os dados pessoais:

▪ como e por que coletam

▪ como armazenam

▪ por quanto tempo guardam

▪ com quem compartilham

Do lado do Cartório, o trabalho será fornecer essas informações de forma clara, inteligível e simples.

**Principais fundamentos**

1. Transparência: Os cartórios devem atuar de forma transparente permitindo que o titular de dados saiba exatamente o que será feito com seus dados pessoais.

2. Controle: O titular de dados tem o direito de decidir e entender todo o ciclo de vida de seus dados pessoais nos cartórios.

3. Ética: Os cartórios devem tratar os dados pessoais de forma não discriminatória e não abusiva, sempre respeitando a liberdade, a intimidade e a privacidade dos titulares de dados.

**Quais dados devem ser protegidos:**

- **Dados Pessoais**: Informação relacionada à pessoa natural identificada ou identificável, obtidos em qualquer tipo de suporte (papel, eletrônico, informático, som, imagem, etc.).

- **Dados Sensíveis**: Dados pessoais da origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

**Quem fiscalizará o cumprimento da lei?**

A chamada Autoridade Nacional de Proteção de Dados (ANPD) será a responsável por fiscalizar e aplicar as sanções a quem descumprir a lei. Por ora, enquanto a Autoridade Nacional não está atuando, o Ministério Público está, de forma proativa, responsável por zelar, implementar e fiscalizar o uso de dados.

**Quem pode ser responsabilizado?**

A Lei prevê duas figuras importantes, relacionadas aos responsáveis pelo tratamento de dados: o chamado “controlador” e o “operador”.

**Controlador** -> pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (TITULAR DO CARTÓRIO).

**Operador** -> pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. (ESCREVENTES)

O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, fica obrigado a repará-lo, solidariamente.

**Quais são as sanções previstas na lei?**

Sanções administrativas:

(i) Advertência

(ii) Obrigação de divulgação do incidente

(iii) Eliminação de dados pessoais

(iv) Bloqueio, suspensão e/ou proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados pessoais

(v) Multa de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil e no seu último exercício, limitada a R$ 50 milhões. \*\* Cartórios não estão incluídos nesta hipótese em razão do art. 23, paragrafo 4º e art. 52, II.

A Autoridade (ANPD) deve levar as seguintes questões em consideração:

(i) Reincidência

(ii) Boa-fé

(iii) Capacidade financeira

(iv) Proporcionalidade

(v) Adoção imediata de medidas corretivas

(vi) Procedimentos e ferramentas internas relativas proteção de dados

(vii) Políticas de boas práticas e governança

(viii) Cooperação

(ix) Grau de dano/seriedade

(x) Vantagem obtida ou intencionada

**Boas práticas da LGPD para implementar nos cartórios:**

• Possuir total transparência na sua atuação;

• Respeitar os interesses e direitos dos titulares de dados;

• Utilizar apenas os dados estritamente necessários para determinada finalidade;

• Adotar uma abordagem proativa e preventiva em relação à segurança de dados;

• Entender a privacidade como algo positivo para os negócios;

• Garantir a segurança do dado ao longo de todo seu ciclo de vida na serventia.

**2) DOS CONCEITOS LEGAIS:**

• **Titular (art. 5º, V)**: Conforme a Lei Geral de Proteção de Dados (LGPD), é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

**• Agentes de tratamento (art. 5º, IX):**

a) Controlador (art. 5º, VI): pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. (TITULAR DA SERVENTIA – TABELIÃO).

b) Operador (art. 5º, VII): pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

• **Consentimento**: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

• **Tratamento**: Toda operação realizada com dados pessoais, como 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**: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

• **Eliminação (art. 5º, XIV)**: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

• **Relatório de impacto à proteção de dados pessoais (art. 5º, XVII)**: documentação do controlador que deve conter 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 prevenção e mitigação de risco.

*\*\*É necessário prever o RISCO de vazarem informações por não descartar corretamente cópias de documentos ou então usa-los como rascunho... prever o descarte como forma de PREVENCAO ao risco.*

• **Dado Pessoal**: De acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD), toda informação relacionada à pessoa natural identificada ou identificável é considerada dado pessoal. Informações como RG, CPF, endereço, contatos de telefone e e-mail se enquadram nesse conceito, bem como aquelas que, quando combinadas, produzem como resultado a identificação de um indivíduo.

• **Dado Pessoal Sensível**: O dado pessoal sensível é aquele que trata sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual; e dado genético ou biométrico.

• **Dado Anonimizado**: Trata-se de informação que perde a possibilidade de vinculação com seu titular, a partir da utilização de meios técnicos razoáveis e disponíveis para impossibilitar a associação entre o dado e o seu proprietário, seja de forma direta ou indireta. Quando anonimizado, o dado não é considerado pessoal pela LGPD, salvo quando o processo de anonimização ao qual foi submetido puder ser revertido.

• **Dado Pseudoanonimizado**: O dado pseudoanonimizado é aquele que passou por processo com o fito de impossibilitar sua associação com o seu titular, sendo mantida pelo controlador separadamente, em ambiente controlado e seguro, a informação que, quando associada ao dado pseudoanonimizado, identificará o indivíduo.

• **Controlador**: Trata-se da pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

• **Co-controlador**: Haverá co-controladores, quando dois ou mais responsáveis pelo tratamento determinarem conjuntamente as finalidades e os meios do tratamento de dados pessoais

• **Operador**: É operador, a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

• **Autoridade Nacional de Proteção de Dados (ANPD)**: A ANPD é órgão da administração pública, atualmente integrante da Presidência da República, responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o país, com a prerrogativa de aplicar sanções em caso de descumprimento das disposições da norma.

• **Encarregado**: É a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados, a Autoridade Nacional de Proteção de Dados (ANPD) e outras entidades reguladoras.

**- O que são “dados pessoais”?**

São informações relacionadas à pessoa física identificada ou identificável. A lei traz um conceito amplo, já que qualquer dado isolado ou agregado a outro que possa identificar uma pessoa física é caracterizado como dado pessoal.

Trata-se de Qualquer informação que identifique o indivíduo em particular, obtidos em qualquer tipo de suporte (papel, eletrônico, informático, som, imagem, etc.). Ou seja, ajudam você a identificar direta ou indiretamente o indivíduo.

• Filiação de natureza política, filosófica ou religiosa

• Origem, étnica ou racial

• Filiação sindical

• Convicção religiosa

• Dado genético ou biométrico

• Dado sobre saúde ou vida sexual

• Opinião política

Exemplos: nome, data de nascimento, profissão, nacionalidade, hábitos de consumo, etc. Nesse sentido, vale dizer que o e-mail, o login ou o telefone corporativo que identifica a pessoa também são dados que devem ser tratados com a devida atenção! Caso um dado não seja apto de forma alguma a identificar um indivíduo, então seu tratamento não está sujeito à lei. É o chamado “dado anonimizado”.

Dados que versem sobre origem racial ou ética, convicção religiosa, dado genético ou biométrico, aqueles referentes à saúde ou à vida sexual e aqueles relacionados a filiação em sindicato ou a organização de caráter religioso, filosófico ou político são os chamados “dados pessoais sensíveis”, que recebem atenção especial da lei.

**- O que não é Dado Pessoal?**

Dados anonimizados ou que passam por processo de anonimização não são dados pessoais (art. 5º, III e XI): o dado anonimizado é relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Já a anonimização é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

O uso de dados anonimizados se mostra primordial para possibilitar o desenvolvimento e aprimoramento de novas tecnologias, como a Internet das Coisas e a Inteligência Artificial, porém a dificuldade é enorme de se comprovar que meios técnicos razoáveis e disponíveis na ocasião do tratamento não possam levar a identificação do titular.

A Lei também não atinge diretamente documentos confidenciais, segredos de negócios, fórmulas, algoritmos, direitos autorais ou propriedade industrial, que são protegidos por outras normas, mas somente eventuais dados pessoais que estejam dentro de tal tipo de conteúdo.

**- O que é “tratamento de dados”?**

Assim como o conceito amplo a respeito dos dados pessoais, a LGPD apresenta um conceito aberto e um rol exemplificativo das ações que são consideradas como tratamento de dados pessoais.

Tratamento (art. 5º, X): 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.

Para se tratar dados pessoais, o que inclui a prática da coleta e todas as demais citadas pelo dispositivo legal como a recepção, classificação, arquivamento e transferência, sempre é necessário ter um fundamental legal. Nesse ponto, mostra-se importante observar que o consentimento se torna uma das 10 (dez) hipóteses legais para o tratamento de dados, conforme veremos a seguir.

O escopo da lei é bem amplo, elencando VINTE AÇÕES! O “Tratamento de Dados” é considerado como toda operação realizada com dados pessoais, como as que se referem a:

(1) coleta, (2) produção, (3) recepção, (4) classificação, (5) utilização, (6) acesso, (7) reprodução, (8) transmissão, (9) distribuição, (10) processamento, (11) arquivamento, (12) armazenamento, (13) eliminação, (14) avaliação ou (15) controle da informação, (16) modificação, (17) comunicação, (18) transferência, (19) difusão ou (20) extração.

**Em quais situações não é aplicável a LGPD?**

Por pessoa física para fins particulares e não econômicos;

Para fins jornalísticos, artísticos e acadêmicos;

Para a segurança pública, defesa nacional, segurança do Estado ou atividades de investigação;

Quando os dados são provenientes de fora do Brasil e não são objeto de comunicação ou uso compartilhado com agentes de tratamento brasileiros.

**3) DO TRATAMENTO DE DADOS PESSOAIS E DOS PRINCÍPIOS LEGAIS:**

De acordo com a Lei Geral de Proteção de Dados Pessoais, tratamento é 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.

O tratamento de dados pessoais realizado por esta serventia observa os princípios contidos na LGPD, os quais seguem listados abaixo:

• **Finalidade**: O tratamento dos dados deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

• **Adequação**: Deve haver compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto da sua realização.

• **Necessidade**: O titular dos dados tem direito à 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.

• **Livre Acesso**: Deve ser garantida ao titular a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Dados dos atos praticados pelo Cartório, porém, sujeitam-se às disposições da legislação registral aplicável, que vinculam o direito de acesso às informações constantes nos livros e arquivos ao pagamento dos emolumentos devidos, nos termos do Art. 14 da Lei nº 6.015/93 (Lei de Registros Públicos) e Art 30, incisos VIII e X da Lei nº 8.935/94 (Lei dos Notários e Registradores).

• **Qualidade dos Dados**: O titular tem o direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento

• **Transparência**: O titular tem direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

• **Segurança**: Os agentes de tratamento devem prezar pela 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**: Deve-se prezar pela adoção de medidas para prevenção à ocorrência de danos em virtude do tratamento de dados pessoais.

• **Não discriminação**: É vedada a realização de tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos

• **Responsabilização e Prestação de Contas**: O agente de tratamento deve demonstrar a 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.

**4) DAS BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS**

A Lei Geral de Proteção de Dados Pessoais estabelece um rol taxativo de bases legais que legitimam o tratamento, dentre elas:

• Para o cumprimento de obrigação legal ou regulatória pelo controlador;

• Pela administração pública e **serventias extrajudiciais** (art. 23, §4º da LGPD), para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

• Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

• Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

• Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

• Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

• Mediante expresso, livre e inequívoco consentimento do titular

• Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

A atividade fim da serventia é a conferir publicidade aos atos praticados, por meio das informações tornadas manifestamente públicas pelo titular (Art. 7º, §4º da Lei 13.709). A base legal que ampara semelhante tratamento, portanto, é o cumprimento de obrigação legal (Art. 7º, II e Art. 23, caput e §4º da Lei 13.709).

Outras operações de tratamento de dados pessoais poderão ser fundamentadas em uma ou mais hipóteses dentre as elencadas acima e a finalidade de sua realização será explicitada de forma clara ao titular.

No tocante ao tratamento realizado com base no legítimo interesse, este poderá se dar sem o consentimento do titular para atendimento de finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: apoio e promoção de atividades do controlador e proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

Dentre os interesses legítimos desta serventia no tratamento de dados pessoais, encontram-se os de:

• Prestar, fornecer, manter, desenvolver, aprimorar, divulgar e ampliar a utilização dos nossos serviços;

• Personalizar a experiência e utilização dos nossos serviços pelo usuário, inclusive para o fornecimento de informações relativas à prestação destes serviços.

• Gerar análises e relatórios estatísticos sobre o funcionamento e operação dos nossos serviços;

• Possibilitar o contato com o usuário a respeito do andamento dos serviços que estão sendo prestados;

• Disponibilizar e melhorar mecanismos de segurança e monitoramento dos nossos serviços;

• Detectar e impedir a utilização dos nossos serviços para propósitos fraudulentos ou que visem alterar as funcionalidades dos nossos serviços ou a prática de abusos e atos ilegais contra o usuário;

**Quando os dados forem sensíveis, o tratamento somente poderá ocorrer nas seguintes hipóteses (art. 11):**

I – consentimento pelo titular, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

**5) DAS PRINCIPAIS CATEGORIAS DE DADOS PESSOAIS E SUAS FINALIDADES**

**Dados do Registro Público**: São as informações fornecidas pelo usuário à serventia extrajudicial territorialmente competente a fim de que seja realizado os atos de notas e registro, bem como as informações que já integram o registro das serventias extrajudiciais, de acesso público (Art. 7º, §4º LGPD c/c Art. 1º da Lei de Registros Públicos), tais como nome, endereço, data de nascimento, sexo, estado civil, direitos em relação à propriedade, requerimentos, instrumentos particulares registráveis, referência a documentos arquivados nas serventias, dados de transações imobiliárias, ônus e outras restrições sobre a propriedade, serventia territorialmente competente, etc. A base legal para o tratamento de tais dados é o cumprimento de obrigação legal.

**Dados de identificação e comunicação** (apresentante, interessado no registro, titular de dados pessoais): Nome completo, e-mail, telefone, celular, endereço, documento de identificação (RG, CPF, CNH, etc). A base legal para o tratamento de tais dados depende do tipo de atividade de tratamento pretendida (privacidade contextual), podendo ser cumprimento de obrigação legal, legítimo interesse, execução de contrato, etc.

**Dados financeiros e de pagamento**: São as informações pessoais necessárias para que possamos processar o pagamento dos serviços prestados, incluindo seu CPF, endereço, informações bancárias de cobrança e crédito (e.g. número da agência e da conta corrente), número do cartão de crédito, dentre outros. Os dados financeiros e de pagamento são tratados para o fornecimento de produtos e/ou serviços, manutenção de arquivos, cumprimento de obrigações fiscais. A base legal para o tratamento de tais dados é o cumprimento de obrigação legal, especialmente a legislação fiscal.

**Dados de funcionários**: Nome completo, inclusive o nome social; data de nascimento; número e imagem da Carteira de Identidade (RG); número do Cadastro de Pessoas Físicas (CPF); número e imagem da Carteira Nacional de Habilitação (CNH); fotografia 3x4; estado civil; idade; tipo sanguíneo e fator RH; nível de instrução ou de escolaridade; endereço completo; número de telefone e endereço de correio eletrônico (e-mail); filiação a sindicato; nome dos genitores; nome de usuário e senha específicos para uso dos serviços da Entidade Empregadora; comunicação mantida entre colaborador e serventia; atestados médicos.

A base legal para o tratamento de tais dados é a execução de contrato.

**Dados de identificação digital**: São informações geradas automaticamente, quais sejam, as características do dispositivo de acesso, as características do navegador, o Protocolo de Internet (IP, data e hora), as telas da Central acessadas, os registros de acesso à Central, os dados de geolocalização, histórico das solicitações realizadas Para tal coleta, a serventia fará uso de algumas tecnologias padrões, como cookies, que são pequenos arquivos de texto que um site, quando visitado, coloca no computador do usuário ou no seu dispositivo móvel, por navegador de internet (browser).

Todos os navegadores permitem ao utilizador aceitar, recusar ou apagar cookies, em sua aba de configurações. Ao desativar cookies, porém, o usuário pode impedir que alguns serviços da web funcionem corretamente, afetando, parcial ou totalmente, a navegação no website. Os dados técnicos sobre o computador/dispositivo móvel são tratados para identificação de usuários no meio digital e prevenção a fraudes. A base legal para o tratamento de tais dados é o cumprimento de obrigação legal, especificadamente as estipuladas no Marco Civil da Internet (Lei nº 12.965/2014).

**6) DAS ATIVIDADES DE TRATAMENTO DESENVOLVIDAS PELA SERVENTIA:**

|  |  |  |  |
| --- | --- | --- | --- |
| ATIVIDADE DE TRATAMENTO | DADOS COLETADOS | BASE LEGAL | DURAÇÃO DO TRATAMENTO |
| Atendimento presencial do Usuário do | Dados do Registro Público;  Dados de identificação e comunicação;  Dados financeiros | Cumprimento de obrigação legal (Lei de Registros Públicos) | A depender do ato, nos termos do Provimento  50/2015 do CNJ |
| Atendimento eletrônico do Usuário Remoto | Dados do Registro Público;  Dados de identificação e comunicação;  Dados financeiros | Cumprimento de obrigação legal (Provimentos 89, 100 e  109 do CNJ) | A depender do ato, nos termos do Provimento  50/2015 do CNJ |
| Comunicação à  COAF (Conselho de Controle de Atividades Financeiras - Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo | Dados do Registro Público; Dados de identificação e comunicação; Dados financeiros;  Outros dados do beneficiário final | Cumprimento de obrigação legal  (Provimento 88/2019 do CNJ) | 05 anos (nos termos do Provimento 88/2019 do CNJ) |
| Gestão de Relações  Laborais | Dados de funcionários; Dados financeiros e de pagamento | Execução de contrato; Cumprimento de obrigação legal (CLT) | Até 10 anos após extinção do contrato (em atendimento a prazos prescricionais) |
| Análise de currículos e recrutamentos | Dados de identificação e comunicação;  Currículos | Consentimento | 90 dias ou até a oposição do titular (sugestão) |
| Gestão de Prestadores de Serviços | Dados de identificação e comunicação; Dados financeiros e de pagamento | Execução de contrato; cumprimento de obrigação legal | Até 10 anos após extinção do contrato (em atendimento a prazos prescricionais) |
| Controle de Acesso às Instalações da Serventia | Dados biométricos | Execução de contrato  (funcionários); | Durante a vigência do contrato de trabalho |
| Sistema de  Videovigilância | Imagens de funcionários e visitantes | Legítimo Interesse  (segurança) | 6 dias |
| Atendimento de Solicitações dos Titulares de Dados Pessoais pelo Encarregado | Dados de identificação e comunicação; | Cumprimento de obrigação legal (Lei 13.709 – LGPD) | Enquanto perdurar responsabilidades de tratamentos conexos |
| Atendimento Geral (Sugestões/Reclamações) | Dados de identificação e comunicação; | Legítimo Interesse (melhoria dos serviços) | Enquanto perdurar responsabilidades de tratamentos conexos |
| Cookies do Website | Dados de identificação digital; | Cumprimento de obrigação legal (Lei nº 12.965 – Marco Civil da Internet) | Mínimo de 06 meses, na forma do art. 15 da Lei nº 12.965, e máximo de 01 ano |

**7) POLÍTICA DE COOKIES**

Cookies são pequenos arquivos de texto pequenos colocados no dispositivo do usuário, os quais podem ser coletados posteriormente por servidores Web no domínio que os colocou. É possível escolher quais cookies serão utilizados durante a navegação, sendo assim a base legal para o tratamento de dados pessoais, neste caso, é o consentimento do titular.

• **Cookies de sessão**: Cookies que são utilizados “na sessão”, a cada vez que o usuário visita o *website*, expirando em seguida, quando este o deixa. Esses cookies não são armazenados no dispositivo permanentemente e ajudam a minimizar a necessidade de transferir dados pessoais pela internet. Eles também podem ser excluídos ou ter a permissão de uso recusada pelo usuário, contudo, tais ações prejudicarão o desempenho e a sua experiência no uso do *website*. Os cookies também utilizam registros de hora de acesso e saída da página web.

• **Cookies de rastreamento**: Cookies que permitem o reconhecimento de visitantes que retornam à página do website da serventia. Ao combinar um identificador anônimo gerado aleatoriamente, o cookie de rastreamento mantém o controle sobre o local de onde veio o usuário do site, o mecanismo de busca que pode ter usado, o link em que clicou, a senha usada e sua localização geográfica ao acessar a página.

• **Cookies persistentes**: Cookie que é salvo no dispositivo do usuário por um período fixo (às vezes, por algumas horas, outras, por um ano ou mais) e não é excluído ao encerrar o navegador. Os cookies persistentes são utilizados quando o *website* precisa lembrar quem é o visitante por mais de uma sessão de navegação. Esse tipo de cookie pode ser usado para armazenar preferências, para que sejam lembradas em uma próxima visita ao site.

• **Cookies analíticos ou de desempenho**: Cookies de desempenho são utilizados para melhorar a sua experiência no uso do *website*. Esses cookies ajudam o cartório a adaptar o conteúdo do website para refletir o que os usuários consideram mais interessante e identificar quando surgem problemas técnicos com as páginas relacionadas aos serviços ofertados. Esses dados também podem ser utilizados para compilar relatórios que nos ajudam a analisar como as páginas são utilizadas, quais são os problemas mais comuns e como podemos melhorá-las.

Os dados e os registros de atividades coletados no website da serventia serão armazenados em ambiente seguro e controlado, pelo prazo mínimo de 6 (seis) meses, nos termos do Marco Civil da Internet (art. 15).

Desativar Cookies: É possível impedir a atuação de alguns cookies por meio das configurações do navegador (consulte a função “Ajuda” do seu navegador web para saber como). No entanto, esteja ciente que a eventual desativação de algum cookie poderá afetar a funcionalidade deste e de outros sites que você visita. A desativação de cookies possivelmente resultará em um mau funcionamento do website desta serventia.

**8) DO COMPROMETIMENTO COM A LGPD**

O OFÍCIO DE NOTAS E REGISTROS DA COMARCA VINCULADA DE ALTANEIRA/CE – CARTÓRIO REGIS declara seu integral comprometimento com a Lei Geral de Proteção de Dados, que dispõe sobre a proteção de dados pelas serventias extrajudiciais, tendo adotado as seguintes ações no âmbito do Compliance de Proteção de Dados em implementação na serventia:

• Todos os prepostos e prestadores terceirizados de serviços foram orientados sobre os deveres, requisitos e responsabilidades decorrentes da Lei nº 13.709/2018;

• Foram arquivados, em classificador próprio, os comprovantes e registros de participação em cursos, seminários, conferências, workshops e afins, proporcionados pelo Oficial ou um dos Encarregados, com a indicação do conteúdo das orientações, bem como da carga horária, transmitidas nesses eventos;

• Foi nomeado Encarregado de proteção de dados, que atuarão como canal de comunicação entre os titulares de dados pessoais e a ANPD. A nomeação ocorreu mediante portaria (divulgada a todos os funcionários) e contrato escrito arquivado em classificador próprio;

• Foi divulgada a Política de Privacidade da serventia e de Canal de Atendimento ao titular de dados pessoais, estando em processo de mapeamento dos dados pessoais para instituição do sistema de controle de fluxo;

• Funcionários foram instruídos para a expedição de certidão ou informação restrita ao que constar nos indicadores e índices pessoais, inclusive solicitações de certidões ou informações em bloco, ou agrupadas, ou segundo critérios não usuais de pesquisa.

**9) DOS DIREITOS DOS TITULARES DE DADOS PESSOAIS**

A Lei Geral de Proteção de Dados Pessoais tem a autodeterminação informativa como princípio basilar no tocante aos direitos dos titulares (art. 18). Entende-se por autodeterminação informativa a possibilidade do titular de compreender e influenciar, sujeito às determinadas restrições legais, os tratamentos que são realizados com os seus dados pessoais, conferindo transparência a estas operações.

Nem todos os direitos previstos no art. 18 da LGPD poderão ser exercidos perante o acervo público da serventia extrajudicial, em razão das peculiaridades desse acervo e da incidência das regras específicas do microssistema notarial e registral.

Esta serventia, no contexto de suas atividades legais de tratamento de dados pessoais, reforça o seu compromisso de respeito aos direitos dos titulares, sendo estes:

**• Confirmação da existência de tratamento (Art. 18, I, LGPD)**

O titular de dados pessoais poderá questionar, junto a esta serventia, se há realização de operações de tratamento relativas a dados pessoais seus, por meio do Canal de Atendimento com o Encarregado.

A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular, a qual deve ser formulada em formulário contido no *website* do Cartório, sendo garantida a gratuidade da solicitação.

Esta serventia responderá a requisição no prazo de até 15 (quinze) dias, contados da data do requerimento do titular com comprovação de autenticidade.

**• Acesso aos dados (Art. 18, II, LGPD)**

O titular de dados pessoais poderá solicitar e receber uma cópia de todos os eventuais dados pessoais coletados e armazenados;

Dados do Registro Público sujeitam-se às disposições da legislação registral aplicável, que vinculam o direito de acesso às informações constantes no fólio real ao pagamento dos emolumentos devidos, nos termos do Art. 14 da Lei nº 6.015/73 (Lei de Registros Públicos) e do Art. 30, Incisos VIII e X, da Lei nº 8.935/94 (Lei dos Notários e Registradores).

**• Correção de dados incompletos, inexatos ou desatualizados (Art. 18, III, LGPD):**

O titular de dados pessoais poderá requisitar a correção de dados que estejam incompletos, inexatos ou desatualizados.

Dados dos tabelionatos de notas e protestos sujeitam-se às disposições da legislação registral aplicável, que estabelece procedimento específico para a retificação do registro, averbação ou anotação, não sendo devido o pagamento de selos e taxas apenas nos casos em que a retificação decorra de erro imputável ao oficial.

**• Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou desconformes com a LGPD (Art. 18, IV, LGPD):**

Dados do Registro Público, por seu interesse público, não poderão ser anonimizados, bloqueados ou eliminados, sob pena de comprometer o arquivo público destinado a conferir cognoscibilidade aos direitos.

Ressalta-se, no entanto, que sempre que possível, os dados utilizados em pesquisas jornalísticas, científicas ou afins, serão anonimizados.

**• Portabilidade dos dados a outro fornecedor de serviço ou produto**

O titular de dados pessoais poderá requisitar que seus dados pessoais sejam disponibilizados a outro fornecedor de serviço ou produto, respeitados o segredo comercial e industrial da instituição, bem como os limites técnicos de sua infraestrutura.

Baseando-se nas diretrizes do Art. 20 do Regulamento Geral Europeu de Proteção de Dados (GDPR), que inspirou a edição da LGPD, o titular somente poderá exercer o direito de portabilidade de dados em operações de tratamento cuja base legal seja o consentimento ou a execução de contrato. Dados do Cartório não são coletados mediante consentimento ou assinatura de contrato (Art. 7º, §4º da LGPD c/c Art. 1º da Lei de Registros Públicos).

Enquanto não há regulação pelo CNJ ou pela CGJ/CE, para fins de orientação mais específica, tomamos como sugestão de orientação a adotada pela Corregedoria Geral de Justiça do Estado de São Paulo, no sentido de aduzir que “*os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro não se equiparam a fornecedores de serviços ou produtos para efeito de portabilidade de dados pessoais*” (item 147 do Provimento nº 23 CGJ-SP).

Regulamentações sobre o direito de portabilidade de dados poderão ser proferidas pela Autoridade Nacional de Proteção de Dados (arts 17, V e 40 da LGPD).

**• Eliminação dos dados pessoais tratados com o consentimento do titular (Art. 18, VI, LGPD)**

O titular de dados pessoais poderá requisitar a exclusão de dados pessoais tratados nesta serventia, que não procederá com a eliminação apenas se houver um motivo legítimo para a sua manutenção (Art. 16 LGPD), como eventual obrigação legal de retenção de dados.

Na hipótese de eliminação, a serventia se reserva o direito de escolher o procedimento de eliminação empregado, comprometendo-se a utilizar mecanismo que evite a recuperação dos dados.

Dados do Registro Público não poderão ser eliminados, por constituírem dados tornados manifestamente públicos pelo titular, considerando a própria publicidade que se espera dos serviços notariais e registrais para a constituição de direitos, aos quais se dispensa a coleta de consentimento (art. 7º, §4º da Lei Geral de Proteção de Dados c/c art. 1º da Lei de Registros Públicos). Nos termos do art. 7º, §1º da Lei nº 8.159/1991 (Lei da Política Nacional de Arquivos Públicos e Privados), são públicos os conjuntos de documentos produzidos e recebidos por entidades privadas encarregadas da gestão de serviços públicos, a exemplo dos serviços notariais e registrais, em consonância com o art. 236 da Constituição Federal.

**• Informação das entidades públicas e privadas com as quais esta serventia realizou o Uso Compartilhado de dados (Art. 18 VII, LGPD).**

O titular de dados pessoais possui o direito de saber com quais entidades públicas e privadas esta serventia pode realizar o compartilhamento de dados, o que é informado por meio desta Política de Privacidade e Proteção de Dados.

**• Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (Art. 18, VIII, LGPD);**

Sempre que a coleta de dados de determinado serviço esteja amparada no consentimento, o titular de dados pessoais será informado sobre a possibilidade de não fornecer consentimento. Em determinados casos, a negativa do consentimento poderá implicar na impossibilidade de prestação de determinados serviços, e a serventia indicará tais casos e suas consequências.

**• Revogação do consentimento (Art. 18, IX, LGPD)**

Dados do Registro Público são dados tornados manifestamente públicos pelo titular, considerando a própria publicidade que se espera dos serviços notariais e registrais para a constituição de direitos, aos quais se dispensa a coleta de consentimento (art. 7º, §4º da Lei Geral de Proteção de Dados c/c art. 1º da Lei de Registros Públicos).

O titular de dados pessoais poderá revogar o consentimento concedido a determinadas operações de tratamento, hipótese que não afetará a legalidade de qualquer tratamento realizado antes da revogação do consentimento. Em determinados casos, a revogação poderá implicar na impossibilidade de prestação de determinados serviços, esta serventia indicará quais serviços podem ser descontinuados.

**Resumindo os Conceitos da Lei:**

|  |  |  |  |
| --- | --- | --- | --- |
| Direitos do Titular  • Acesso às informações;  • Correção dos dados;  • Anonimização, bloqueio ou eliminação de dados • Portabilidade dos dados pessoais  • Revisões de decisões tomadas em tratamento dos dados pessoais (perfil pessoal, profissional, de consumo, de crédito ou personalidade). | Controlador  • Deve garantir a segurança dos dados, respondendo pelos danos decorrentes da violação da segurança de dados  • Devem emitir um relatório de impacto à proteção dos dados (riscos, metodologia, análise das medidas, salvaguardas e mecanismos de mitigação dos riscos) • Transferência internacional somente para países ou órgãos internacionais que proporcionem grau de proteção adequado; | Consentimento  • Obrigatório, salvo as situações explicitas na Lei;  • Dados estritamente necessários para a finalidade de tratamento  • Pode ser revogado a qualquer momento pelo Titular  • Deve ser expressa claramente em clausulas destacadas, contendo as finalidades e os Agentes de Tratamento, não podendo ocorrer vício de consentimento  • O Titular deve ser avisado em caso de alteração | Sanções  • Advertência, com indicação de medidas corretivas  • Multa (simples ou diárias) de até 2% do faturamento do último exercício, limitado a 50 milhões por infração.  • Publicitação da infração;  • Bloqueio / eliminação dos dados pessoais a que se refere a infração |

**10) DA ELIMINAÇÃO DE DADOS PESSOAIS**

O pedido de exclusão dos dados e interrupção do tratamento será acatado na medida do possível legal. A LGPD, a Lei de Registros Públicos e o Provimento CNJ 50/2015 impõem que algumas informações permaneçam sempre públicas, de modo que haverá, tão-somente, a exclusão das informações tratadas para algumas das finalidades expressas nesta Política.

Os dados coletados por esta serventia serão excluídos nas seguintes situações:

• Quando a finalidade para a qual a informação foi coletada tenha sido alcançada ou quando o dado deixar de ser necessário ou pertinente para o alcance desta finalidade, conforme descrito nesta Política;

• Quando da revogação do consentimento por parte do Titular, nos casos em que este se faça necessário;

• Mediante determinação da autoridade competente para tanto.

Os dados pessoais poderão ser conservados por esta serventia, contudo:

• Para cumprimento de obrigação legal ou regulatória;

• Para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

• Para transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGDP;

**11) DO COMPARTILHAMENTO DOS DADOS PESSOAIS**

O compartilhamento de dados pessoais com órgãos da Administração Pública deverá atender a uma finalidade específica, seja para a execução de uma política pública, seja para o cumprimento de uma atribuição legal, respeitando os princípios de proteção de dados pessoais, conforme o artigo 26 da Lei Geral de Proteção de Dados.

Dados dos registros públicos, portanto, apenas serão compartilhados em cumprimento a obrigações legais e/ou normativas ou, quando forem adotados mecanismos de anonimização que não permitam a identificação do titular do dado pessoal.

Na execução de sua atividade fim, a serventia possui a obrigação de avaliar a existência de suspeição nas operações ou propostas de operações dos usuários e comunicar suspeitas de lavagem de dinheiro ou financiamento de terrorismo ao Conselho de Controle de Atividades Financeiras (Provimento 88 do CNJ).

Também possui a obrigação de encaminhar a Declaração de Operações Imobiliárias (DOI) à Receita Federal (IN RFB nº 1112/2010). Ademais, caso não adote mecanismo de comunicação sincronizada (Webservice), deve diariamente atualizar o Banco de Dados Light (BDL), para fim de viabilização do registro eletrônico.

No que tange às demais atividades de tratamento, esta serventia apenas compartilhará dados tratados com terceiros os dados pessoais tratados nas seguintes hipóteses:

• Para o cumprimento de obrigação legal e regulatória;

• Com a Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos;

• Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados;

• Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

• Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

• Para a proteção da sua vida ou da incolumidade física, bem como a de terceiros;

• Para a tutela da saúde, em procedimento realizado por profissional da área ou entidade sanitária;

• Quando necessário para atender aos interesses legítimos desta serventia ou de terceiros, exceto nos casos que prevalecem os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

• Caso o titular dos dados consinta;

• Para proteção de crédito, inclusive quanto ao disposto na legislação pertinente.

**12)TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS**

Segundo a LGPD, a transferência internacional de dados pessoais somente será permitida nos seguintes casos:

• Para países ou organismos internacionais com grau de proteção de dados pessoais adequado;

• Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, na forma de: cláusulas contratuais específicas para determinada transferência, cláusulas-padrão contratuais, normas corporativas globais, selos, certificados e códigos de conduta regularmente emitidos;

• Quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

• Quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

• Quando a autoridade nacional autorizar a transferência;

• Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

• Quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público;

• Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades;

• Para o cumprimento de obrigação legal ou regulatória pelo controlado;

• Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

• Para exercício regular de direitos em processo judicial, administrativo ou arbitral.

A transferência internacional de dados pessoais será realizada por esta serventia com fundamento nas bases indicadas nesta Política e nos termos da legislação vigente.

**13) INCIDENTE DE SEGURANÇA**

Em caso de incidente de segurança que envolva vazamento dados pessoais, a ocorrênciaserá comunicada, pelo Encarregado, à Autoridade Nacional de Proteção de Dados e ao respectivo titular, quando o incidente possa acarretar risco ou dano relevante (art. 48 da LGPD).

A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

• a descrição da natureza dos dados pessoais afetados;

• as informações sobre os titulares envolvidos;

• a indicação das medidas técnicas e de segurança utilizadas para a proteção

• dos dados, observados os segredos comercial e industrial;

• os riscos relacionados ao incidente;

• os motivos da demora, no caso de a comunicação não ter sido imediata;

• as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo

Em que pese ainda inexistir regulamentação específica para o incidente, o relatório produzido dentro de uma política de controle de incidentes de segurança atende os requisitos legais e previne responsabilidades

**14) DAS BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO**

Em conformidade com os princípios da Lei Geral de Proteção de Dados, e com as boas práticas de segurança da informação e de proteção de dados pessoais, esta serventia garante que os dados pessoais coletados são tratados de forma íntegra e segura, de acordo com padrões de segurança da informação, confidencialidade e integridade pelo tempo for necessário para realizar as finalidades para as quais foram coletados ou para cumprir com os requerimentos legais aplicáveis.

Dados do Tabelionato de Notas sujeitam-se ainda às disposições do Provimento no 74/2018 do CNJ, que versa sobre os requisitos de tecnologia da informação das serventias extrajudiciais.

Por isso, a serventia adota sistemas informatizados de vigilância, controles de acesso em suas instalações, unidade de alimentação ininterrupta (nobreak), refrigeração compatível com os equipamentos de hardware, serviços de backup, softwares antivírus e antissequestro, softwares licenciados para uso comercial, firewall, proxy, dentre outros controles preventivos, detectivos e corretivos de segurança da informação. Para facilitar a governança desses ativos, esta serventia também possui inventário de ativos de hardware e software arquivados em sua sede.

Os dados pessoais tratados somente serão acessados por pessoas autorizadas, à luz do que dispõe a legislação vigente, e capacitadas para lhes conferir o tratamento adequado, conforme medidas de segurança adequadas para a proteção contra acesso não autorizado, alteração, divulgação ou destruição de dados pessoais coletados e armazenados.

**15) INSTRUÇÕES DE SEGURANÇA WEB**

O Controlador responsável por ditar as diretrizes de tratamento é o delegatário desta serventia. Todos os colaboradores são treinados para compreender a importância da privacidade e proteção. Tem-se o compromisso de cumprir a legislação de proteção de Dados, por meio da adoção de medidas de segurança da informação.

Esta serventia, visando garantir uma maior segurança quando no acesso do seu Website, sugere ao usuário que siga as seguintes precauções:

• Não responder nem clicar em links provenientes de e-mails desconhecidos;

• Não acessar sites suspeitos;

• Manter mecanismos de proteção ativos e atualizados, como antivírus e antimalware;

• Não instalar programas ou aplicativos de fontes estranhas ou ilegais

Independente das outras isenções e declarações elencadas na presente Política, o usuário, ao utilizar os serviços ofertados por esta serventia, declara-se ciente e concorda com as seguintes disposições:

• Esta serventia, bem como os seus parceiros, colaboradores e afins não poderão ser responsabilizados por fatos oriundos de atividades criminosas (e.g. ataque hacker), caso fortuito ou força maior.

• Esta serventia, bem como os seus parceiros, colaboradores e afins não poderão ser responsabilizados por quaisquer erros e/ou inconsistências na transmissão dos dados, bem como relacionados à qualidade ou disponibilidade da conexão de internet, capazes de obstar o adequado recebimento de informações;

• Esta serventia, bem como seus colaboradores e parceiros, não serão responsabilizados pelo uso do domínio eletrônico em discordância com as disposições elencadas nesta Política (e.g. imputação de dados, por parte de algum usuário, desatualizados, incompletos ou inverídicos);

• O usuário reconhece que incapacidade técnica e econômica de prevenção absoluta contra ataques, invasões, vírus, vazamento e perda de dados ou outros atos ilícitos que porventura aconteçam no domínio eletrônico, isentando, assim, esta serventia e seus colaboradores, bem como os operadores e encarregados de qualquer dano, indireto ou direto, advindos desses infelizes eventos.

**16) DA ATUALIZAÇÃO DESTA POLÍTICA DE PRIVACIDADE**

Esta Política de Privacidade e Proteção de Dados Pessoais poderá ser alterada a qualquer tempo caso haja necessidade. Por isso, recomenda-se que seja consultada com regularidade e verificada a data de modificação.

Se após a leitura desta Política de Privacidade e Proteção de Dados Pessoais restar qualquer dúvida ao usuário, ou por qualquer razão precisar se comunicar para assuntos envolvendo os seus dados pessoais, o contato poderá ser realizado por um dos e-mails dos encarregados:

**Encarregado Interno (DPO): Brenda Lopes de Lima Regis**

**E-mail:lgpdcartorioregisdealtaneira@gmail.com**

1. Dados fornecidos por Cost of data Breach. Ponemon Institute, 2018. [↑](#footnote-ref-1)