POLÍTICA GERAL DE PRIVACIDADE E PROTEÇÃO DE DADOS

SÃO PAULO/SP, 10 DE SETEMBRO DE 2025.

SUMÁRIO

1. DO OBJETIVO DA POLÍTICA GERAL

Como sabido, a Lei Geral de Proteção de Dados (LGPD) representa um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil e trouxe significativas mudanças para o mundo corporativo. A partir da vigência da Lei, instituições públicas e privadas passaram a adotar medidas para assegurar o correto tratamento de dados, de modo a minimizar eventuais riscos.

Dentre essas medidas de adequações estão as políticas internas, que além de reger a forma adequada de realizar o tratamento de dados pessoais, conscientiza todo o corpo funcional da organização sobre os direitos, obrigações e sanções impostas pela LGPD.

Inclusive, o Provimento CNJ nº 134/2022 – criado para auxiliar os titulares responsáveis pelas serventias extrajudiciais no processo de adequação à LGPD –, determinou em seu artigo 6º, inciso VI a necessidade de definir e implementar Política Interna de Privacidade e Proteção de Dados.

Assim, o objetivo da presente política interna é:

- **Adequar a entidade às leis e regulamentações aplicáveis de proteção de Dados Pessoais e seguir as melhores práticas;**
- **Ser transparente em relação aos procedimentos internos de Tratamento de Dados Pessoais e proteger os direitos dos Colaboradores, Clientes, fornecedores e parceiros contra os riscos de vazamentos ou má utilização de Dados Pessoais;**
- **Estabelecer regras de tratamento de Dados Pessoais;**
- **Promover a conscientização de todo corpo funcional da serventia extrajudicial sobre a proteção de Dados Pessoais e da privacidade.**

Para isso, a presente Política apresenta princípios gerais de conduta, bem como obrigações a serem seguidas por todos do **REGISTRADOR E TABELIÃO DINAMARCO**, a fim de mitigar eventuais riscos relacionados a ameaças externas ou internas, deliberadas ou acidentais, que possam impactar na confidencialidade, integridade e disponibilidade das

informações do **REGISTRADOR E TABELIÃO DINAMARCO**, objetivando garantir a preservação dessas informações.

Esta Política se aplica a todos os Colaboradores do **REGISTRADOR E TABELIÃO DINAMARCO**, inclusive o Titular, e a parceiros, fornecedores e prestadores de serviços terceirizados. A violação desta Política estará sujeita a penalidades na esfera trabalhista, cível e criminal.

2. ABRANGÊNCIA DESTA POLÍTICA

Para que as orientações sobre o Tratamento de Dados Pessoais constantes nesta política possam ser aplicadas de modo adequado e eficaz, nos ditames da Lei Geral de Proteção de Dados e do Provimento CNJ nº 134/2022, é necessário que todo corpo institucional do **REGISTRADOR E TABELIÃO DINAMARCO** atue de forma contínua e permanente para cumprir as exigências da legislação.

Cada setor e/ou Colaborador do **REGISTRADOR E TABELIÃO DINAMARCO** tem um papel fundamental na aplicabilidade do quanto aqui disposto.

Todos os Colaboradores, no ato de sua contratação, receberão uma cópia desta Política vigente, bem como eventual documentação suporte aplicável (por exemplo, Termo de Confidencialidade).

3. DAS DEFINIÇÕES

Seguem abaixo as definições dos termos utilizados nesta Política.

- **LGPD:** Legislação brasileira nº 13.709/2018, comumente conhecida como Lei Geral de Proteção de Dados Pessoais, que regula as atividades de Tratamento de Dados Pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.
- **Legislação ou Legislação Aplicável:** Toda e qualquer legislação em vigor no Brasil em matérias de proteção de Dados incluindo, mas não se limitando, à Constituição Federal, ao Marco Civil da Internet, à Lei 13.709 – Lei Geral de Proteção de Dados

LGPD, seus decretos regulamentadores, bem como o Provimento CNJ nº 134/2022 e Seção VIII do Capítulo XIII das Normas de Serviço Extrajudicial editas pela E. Corregedoria Geral da Justiça de São Paulo.

- **Agentes de Tratamento:** Pode ser o Controlador ou o Operador de Dados Pessoais.
- **Controlador:** No cartório, o controlador é o Registrador e Tabelião, Rodrigo Valverde Dinamarco, de acordo com o Provimento CNJ nº 134/2022.
- **Operador:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o Tratamento de Dados Pessoais em nome do Controlador. Por exemplo: prestador de serviço de armazenamento de Dados Pessoais (Operador) é contratado e autorizado pelo **REGISTRADOR E TABELIÃO DINAMARCO** (Controlador) para tratar os Dados Pessoais estritamente de acordo com o que foi previsto no contrato.
- **Titular(es) de Dados:** Pessoa natural singular identificada ou identificável a quem se refere um Dado Pessoal específico.
- **Dados Pessoais:** Qualquer informação relativa a uma pessoa singular identificada ou identificável, que pode ser identificada, direta ou indiretamente, por referência a um identificador como nome, número de identificação, Dados de localização, identificador on-line ou a um ou mais fatores específicos a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural tais como nome completo; RG; CPF; data de nascimento; estado civil; profissão; endereço residencial e/ou comercial; Dados Pessoais de terceiros relacionados ao Titular de Dados (marido/esposa, filhos, funcionários).
- **Dados Pessoais Sensíveis:** Todo Dado Pessoal que pode gerar qualquer tipo de discriminação, como por exemplo os Dados 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, dado genético ou biométrico.
- **Tratamento de Dados Pessoais ou Tratamento:** Qualquer operação ou conjunto de operações efetuadas sobre Dados Pessoais ou sobre conjuntos de Dados Pessoais, por meios automatizados ou não automatizados, tais como a coleta, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a

consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

- **Encarregado pelo Tratamento de Dados Pessoais ou Data Protection Officer:** Também conhecido como ENCARREGADO ou DPO, é o responsável pela proteção de Dados Pessoais na instituição e pela interface de comunicação do Instituto com a ANPD e com os Titulares. Atualmente é exercido nesta instituição pelo Registrador e Tabelião Substituto, Afonso Pereira Oliveira Neto.
- **Comitê de Segurança da Informação ou CSI:** Grupo de Direção da instituição que tem a função de discutir e deliberar assuntos relacionados à segurança da informação.
- **Autoridade Nacional de Proteção de Dados ou ANPD:** Órgão pertencente à administração pública federal, responsável pela fiscalização do cumprimento das disposições da Lei Geral de Proteção de Dados Pessoais ("LGPD").
- **Anonimização:** Processo e técnica por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Dado anonimizado não é considerado Dado Pessoal.
- **Consentimento:** Manifestação livre, informada e inequívoca pela qual o Titular concorda com o Tratamento de seus Dados Pessoais para uma finalidade determinada.
- **Política de Privacidade:** Definição dos Conceitos e Medidas Organizacionais para cumprimento da legislação aplicável à Proteção dos Dados;
- **Política de Segurança da Informação:** Política do **REGISTRADOR E TABELIÃO DINAMARCO** sobre Segurança da Informação: [***PQ TIN 01*** - Política de Segurança da Informação].
- **Política de Gestão de Incidentes de Segurança e de Dados Pessoais:** Política do **REGISTRADOR E TABELIÃO DINAMARCO** sobre Incidentes de Segurança: [***PQ TIN 03*** - Política de Gestão de Incidentes de Segurança e de Dados Pessoais].
- **Segurança da Informação ou SI:** Sistema responsável por proteger a integridade, disponibilidade e confidencialidade dos sistemas de TI e pela implementação das medidas adequadas para alcançar este objetivo, sendo o apoio técnico do Encarregado e base para as questões relacionadas às medidas técnicas e administrativas.

- **Incidente de segurança:** É o acontecimento indesejado ou inesperado que possa comprometer a segurança dos Dados Pessoais, de modo a expô-los a acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de Tratamento inadequado de dados. Além dos danos aos Titulares, o Incidente pode causar danos ao patrimônio material e imaterial, instalações, sistemas, clientes e colaboradores do **REGISTRADOR E TABELIÃO DINAMARCO**, podendo gerar uma perda financeira, de informações e ser prejudicial à reputação da instituição, podendo levar a uma crise. Por exemplo: vazamento de Dados Pessoais por falha interna ou perda do acesso à base de dados de Colaboradores em razão de conduta maliciosa (hacker).
- **Informações Protegidas:** Todo e qualquer dado ou informação que o Colaborador desenvolva ou venha a ter acesso, direta ou indiretamente, em qualquer formato (oral ou escrito, seja em suporte físico ou digital), em virtude do seu vínculo com o **REGISTRADOR E TABELIÃO DINAMARCO** ou do desempenho de suas atividades contratadas pelo cartório.
- **Terceiro(s) ou Parceiro(s):** Qualquer pessoa, física ou jurídica, que atue em nome, no interesse ou para o benefício do **REGISTRADOR E TABELIÃO DINAMARCO**, preste serviços ou forneça outros bens.
- **Cliente:** Pessoa física ou jurídica (usuário) que utilize dos serviços oferecidos pelo **REGISTRADOR E TABELIÃO DINAMARCO**.
- **Coordenador(es):** Todo Colaborador que lidera uma equipe;

4. DAS REGRAS GERAIS SOBRE TRATAMENTO DE DADOS PESSOAIS

O inciso X do artigo 5º da LGPD estabelece que 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"*.

Observa-se que a definição de tratamento pela legislação é bem ampla. Por essa razão, a LGPD também determinou que os dados pessoais só poderão ser tratados se os princípios definidos em lei forem respeitados e se houver fundamento em alguma das hipóteses previstas na legislação, que são as chamadas “bases legais” de tratamento.

Esses dois pontos de extrema importância para o tratamento de dados serão abordados a seguir:

4.1. Dos Princípios da LGPD

A Lei Geral de Proteção de Dados, por meio de seus **princípios** elencados no artigo 6º, impõem diretrizes e limitações sobre como os Dados Pessoais poderão ser tratados.

Vejamos:

- **Finalidade:** Tratar os Dados Pessoais para objetivos legítimos, específicos, explícitos e informados ao Titular.

- **Adequação:** Tratar os Dados Pessoais de forma compatível com as finalidades informadas ao Titular dos Dados.

- **Necessidade:** Tratar somente os Dados necessários, tanto em questão de categorias de Dados, como em proporção. O mínimo possível para atingir as finalidades.

- **Livre acesso:** Garantir ao Titular de Dados a consulta gratuita e facilitada aos seus Dados Pessoais tratados, bem como à forma e duração do Tratamento.

- **Não discriminação:** Não utilizar o Tratamento para fins discriminatórios ilícitos ou abusivos.

- **Qualidade de Dados:** Garantir aos Titulares que seus Dados sejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu Tratamento.

- **Segurança:** Utilizar 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.

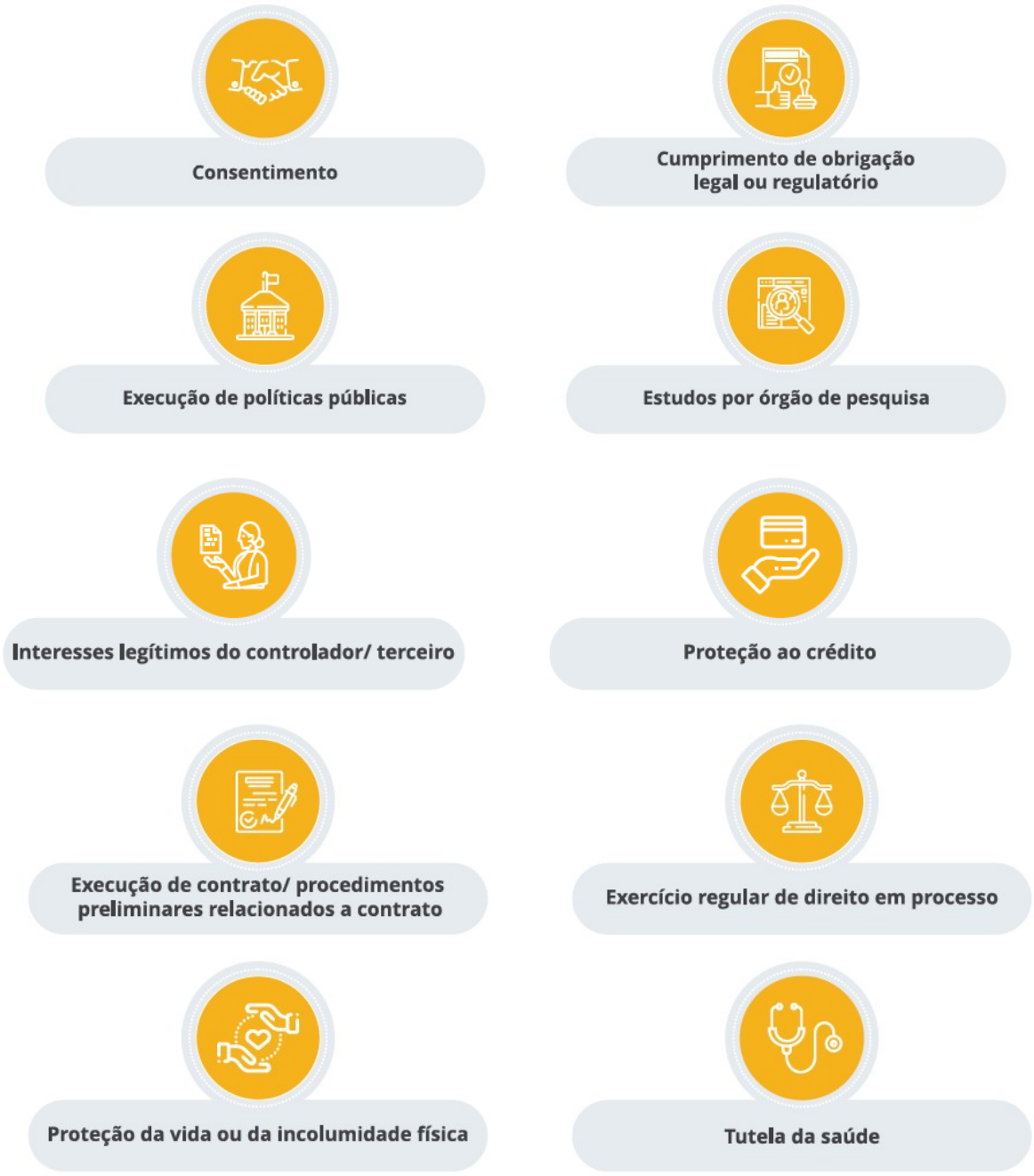
- **Prevenção:** Adotar todas as medidas possíveis para evitar danos ao (ou em decorrência do) Tratamento de Dados Pessoais.

- **Transparência:** Dar acesso aos Titulares a informações claras, precisas e facilmente acessíveis sobre o Tratamento de seus Dados Pessoais, resguardados os segredos comercial e industrial.

- **Responsabilização e prestação de contas:** Demonstrar a adoção de medidas eficazes para comprovar a observância e o cumprimento das normas de proteção de Dados.

4.2. Das Hipóteses de Tratamento de Dados

A LGPD determinou que o tratamento de dados só será realizado se puder ser fundamentado em uma das 10 (dez) bases legais:



Não existe um caso geral que se adeque a todas as situações. Poderá haver inclusive situações em que mais de uma hipótese legal seja cabível, se houver múltiplos propósitos para o tratamento do dado.

O importante é avaliar caso a caso e documentar as hipóteses aplicáveis, uma vez que o titular deverá conhecer a hipótese legal que autoriza o processamento de seus dados pessoais.

Além disso, o princípio da responsabilização e prestação de contas requer que o órgão ou entidade 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.

Para facilitar ainda mais o entendimento das bases legais, vejamos o conceito de cada uma:

a) Consentimento

Consentimento é a manifestação livre, informada, expressa e inequívoca que autoriza o tratamento de dados pessoais para uma finalidade determinada. Autorizações genéricas, isto é, autorizações que não têm como escopo uma finalidade específica, explícita e informada serão nulas.

O consentimento deverá ser fornecido por escrito em cláusula destacada ou por qualquer outra ação afirmativa que demonstre a vontade do titular dos dados. Não se admite em hipótese alguma o consentimento implícito.

Será sempre considerado uma autorização temporária porque pode ser revogado a qualquer momento pelo titular dos dados pessoais, por procedimento gratuito e facilitado.

Caso haja mudança na finalidade para o tratamento de dados pessoais para a qual o consentimento do titular foi obtido e desde que essa mudança não seja compatível com o consentimento originalmente dado, o controlador deverá informar previamente o titular sobre tal mudança.

Em caso de dados tornados manifestamente públicos pelo próprio titular dos dados, o agente fica desobrigado de obter o consentimento para tratamento de dados, observada a finalidade originária do tratamento, de modo que permanecem vigentes os demais direitos do titular e princípios estabelecidos na LGPD.

b) Cumprimento de obrigação legal ou regulatória

Essa é uma das bases legais que se aplicará senão à todas, à maior parte das atividades do cartório, uma vez que nossa atuação é regulamentada por leis específicas, que atribuem aos notários e registradores diversas obrigações legais.

Um exemplo do tratamento de dados com fundamento nessa base legal é o caso da obrigação de emitir certidões dos registros, efetuadas pelo cartório sempre que for solicitado por qualquer pessoa, sem necessidade de esta informar o motivo ou interesse do seu pedido, conforme dispõem os artigos 16 e 17 da lei nº 6.015/73, ressalvadas as hipóteses legais da exigência de motivação e dos legitimados a requerer.

Outro exemplo é a contratação de um colaborador, que obriga seu empregador a compartilhar dados pessoais com órgãos públicos, como Receita Federal do Brasil, E-social etc.

c) Execução de políticas públicas

Esta é uma base legal muito específica da LGPD, pois se aplica somente à administração pública, e não a empresas ou entidades privadas.

Ela garante que o poder público poderá tratar e fazer uso compartilhado de dados pessoais se eles forem necessários para colocar em prática políticas públicas previstas em leis e regulamentos ou respaldadas em contratos e convênios.

É o caso de dados necessários para implementar programas de assistência social e de transferência de renda, dentre muitos outros exemplos possíveis.

Vale ressaltar ainda que o Art. 4º da lei deixa bem claro que ela não se aplica ao tratamento de dados realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

d) Estudos por órgãos de pesquisa

A realização de estudos por órgãos de pesquisa, como IBGE e IPEA, também está prevista como base legal na LGPD.

O detalhe é que a lei coloca que, sempre que possível, deve ser feita a anonimização dos dados. Ou seja, preferencialmente deve-se adotar procedimentos que impossibilitem a associação direta ou indireta entre um dado e um indivíduo.

Além disso, a lei aborda especificamente a realização de estudos em saúde pública, deixando claro que, nestes casos, os dados devem ser tratados exclusivamente dentro do órgão de pesquisa e estritamente para a finalidade do estudo.

e) Execução de contrato

Os dados pessoais podem ser utilizados para executar ou preparar um contrato do qual o titular seja parte, a pedido do titular.

É o caso, por exemplo, de dados que precisam ser fornecidos para formalizar a contratação de um funcionário ou o aluguel de um imóvel; ou de dados que precisam ser usados para garantir o cumprimento do contrato em si.

Vale ressaltar, inclusive, que as hipóteses de tratamento de dados estejam previstas no contrato.

f) Exercício regular de direto em processo

Hipótese que permite o tratamento de dados para resguardar o direito da parte em processo judicial, administrativo ou arbitral.

Ou seja, a proteção de dados não impede o uso de dados dentro da legalidade para produzir provas e se defender em processos, garantindo o direito ao contraditório e à ampla defesa.

Esta também é uma base legal que pode ser muito utilizada no cartório, principalmente no Departamento Humano Organizacional, que armazena os dados de colaboradores que integram ou integraram o quadro de funcionários da serventia, para se resguardar de eventual ação trabalhista ou previdenciária proposta pelo colaborador.

g) Proteção da vida ou da incolumidade física do titular ou de terceiro

Uma base legal bastante específica da LGPD é o tratamento de dados pessoais para a proteção da vida ou da integridade física do titular ou de terceiros. Como

exemplo, podemos citar o acesso a documentos de uma pessoa caso ela sofra um acidente e esteja impossibilitada de chamar uma ambulância ou de se comunicar com a família.

Quando o uso desses dados pessoais for realizado para garantir a vida e a integridade física da pessoa, então, estará respaldado pela lei.

h) Tutela da saúde

Profissionais da saúde, serviços de saúde ou autoridade sanitária têm o respaldo legal da LGPD para tratar dados pessoais que sejam necessários para a realização de suas atividades.

É o caso, por exemplo, da análise de dados necessária para uma campanha de vacinação ou para notificar um paciente sobre o resultado de um exame.

i) Legítimo Interesse

O legítimo interesse é uma das bases legais mais genéricas e flexíveis previstas na LGPD.

A lei diz que dados pessoais podem ser tratados “quando necessário para atender aos interesses legítimos do controlador ou de terceiros”, desde que isso não se sobreponha a direitos e liberdades fundamentais do titular.

No artigo 10º, a lei esclarece um pouco mais a respeito dos limites do legítimo interesse. Ela determina, por exemplo, que o tratamento deve ser feito para finalidades legítimas, consideradas a partir de situações concretas.

Como exemplo, a lei cita o apoio e promoção de atividades do controlador e a proteção do exercício de direitos e da prestação de serviços que beneficiem o titular.

Um ponto importante ao considerar o legítimo interesse como base legal é que ele traz também mais responsabilidades para a serventia extrajudicial, que tem que estar preparada para justificar a qualquer momento o uso dos dados.

Além disso, o legítimo interesse não pode ser utilizado para justificar o tratamento de dados pessoais sensíveis.

A LGPD deixa claro que, se o tratamento tiver como fundamento o legítimo interesse, a ANPD, responsável por fiscalizar o cumprimento da lei, pode solicitar ao

controlador o relatório de impacto à proteção de dados pessoais (documento que descreve os tipos de dados coletados, a forma como foram obtidos e utilizados, dentre outros detalhamentos).

j) Proteção do crédito

A décima e última hipótese para o tratamento de dados pessoais é a proteção do crédito.

Ela é, basicamente, uma garantia aos órgãos de proteção ao crédito, como o Serasa, para que possam continuar incluindo dados de consumidores em cadastros positivos e, também, para que as empresas com as quais o titular tenha pendências financeiras possam comunicar aos órgãos competentes que existe essa dívida.

Dessa forma, o mercado pode continuar consultando os órgãos de proteção ao crédito para avaliar o perfil do pagador.

4.3. Das especificidades para o tratamento de dados pessoais sensíveis

A LGPD traz regramento específico para o tratamento de dados pessoais sensíveis, que são definidos no art. 5º, inciso II como "*dado pessoal 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, dado genético ou biométrico, quando vinculado a uma pessoa natural*".

São dados cujo tratamento pode ensejar a discriminação do seu titular, e por isso, são sujeitos a proteção mais rígida.

O artigo 11 da LGPD elenca as hipóteses em que o tratamento de dados pessoais sensíveis pode ser realizado. Primeiro a lei traz a possibilidade de tratamento mediante consentimento do titular e enumera as hipóteses que dispensam o consentimento, por meio de rol extensivo.

O tratamento mediante consentimento exige que se registre a manifestação de vontade do titular de forma específica e destacada, dando ciência do conhecimento sobre as finalidades específicas daquele tratamento.

Já o tratamento de dados pessoais sensíveis sem o fornecimento de consentimento do titular somente pode ocorrer 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, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
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 terceiros;
f) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
g) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (resguardados os direitos do titular mencionados no art. 9º da lei sobre o acesso facilitado às informações quanto ao tratamento dos seus dados. A exceção a este item é no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais).

Verifica-se que o legítimo interesse não é uma das bases legais que permitem o tratamento de dados sensíveis. Com isso, podemos entender que estes dados não poderão ser utilizados de forma comercial, para campanhas de publicidade ou direcionamento de vendas, por exemplo.

Cabe destacar que a lei determina o tratamento desse tipo de dado apenas em **situações indispensáveis**. Isso traz para o controlador o ônus da prova da alegada indispensabilidade.

4.4. Especificidades para o tratamento de dados de crianças e adolescentes

Assim como para o caso das informações pessoais sensíveis, a LGPD dedica também atenção especial ao tratamento de dados de crianças e adolescentes.

Apesar de não ser um tratamento de dados frequentemente realizado pelas serventias extrajudiciais, importante destacar que muitas oferecem aos seus colaboradores benefícios corporativos como plano de saúde, que possibilita a inclusão de dependentes menores de idade. Neste caso, embora o tratamento não tenha relação com as atividades exercidas pelo Cartório, este acaba tratando dados de menores para conceder benefícios aos seus funcionários.

A LGPD determina, em seu artigo 14, que o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, **mediante consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.**

A única hipótese que dispensa o consentimento mencionado acima ocorre quando a coleta for necessária para contatar os pais, ou o responsável legal, ou, ainda, para a própria proteção da criança ou adolescente. Nesses casos, os dados deverão ser utilizados uma única vez, vedados o armazenamento e o seu repasse a terceiros.

Contudo, a hipótese de coleta de consentimento dos pais ou responsáveis **não se confunde com situações nas quais o tratamento do dado é necessário para o exercício de direitos da criança ou adolescente ou para lavratura de registros públicos.**

4.5. O tratamento de dados pessoais pelos cartórios

A regra para o poder público, que se aplica aos cartórios, é não poder transferir para entidades privadas dados pessoais constantes de bases de dados em relação às quais tenha acesso. A comunicação ou o uso compartilhado desses dados com pessoas de direito privado deverão ser informados à Autoridade Nacional e dependerão de consentimento do titular.

Excepcionalmente, no entanto, esse consentimento do titular e a informação à Autoridade Nacional serão dispensados. São os casos de:

- Hipóteses de dispensa de consentimento previstas na LGPD;
- Nos casos de uso compartilhado de dados, cuja previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, sejam divulgados em veículos de fácil acesso, preferencialmente em seus sites;
- Em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
- Em que os dados forem acessíveis publicamente, observadas as disposições da lei;
- Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres (nesse caso, o teor desses contratos e convênios devem ser informados à Autoridade Nacional, a ser implementada);
- Na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

A Autoridade Nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

4.6 Dos Padrões de Segurança

4.6.1 Garantir a Segurança dos Dados Pessoais

O **REGISTRADOR E TABELIÃO DINAMARCO** está comprometido com a implementação de medidas técnicas de Segurança da Informação e com a Proteção de Dados Pessoais com vistas a garantir o direito fundamental do indivíduo à autodeterminação da informação. Dentre as medidas se incluem, mas não se limitam a, **(i)** instalação de programas de informática seguros, com alto nível de rastreabilidade e resistente a invasões; **(ii)** instituição de senhas de acesso aos computadores; **(iii)** instalação de níveis de acesso para os Dados digitais e de barreiras físicas com controle de acesso por categoria para os arquivos físicos.

4.6.2 Da Obrigação do Sigilo de Dados Pessoais

Todos os Colaboradores com acesso a Dados Pessoais estão obrigados aos deveres de confidencialidade dos Dados quando do ingresso no **REGISTRADOR E TABELIÃO DINAMARCO** até posteriormente à saída quanto aos Dados pessoais obtidos em função de sua atividade, sendo expressamente vedado o compartilhamento destes Dados com qualquer pessoa alheia ao **REGISTRADOR E TABELIÃO DINAMARCO**, exceto no cumprimento das finalidades propostas, sob pena de responsabilização pessoal de acordo com a lei por eventuais prejuízos causados aos Titulares ou ao cartório.

4.6.3 Da Privacidade de Dados Pessoais por Concepção e por Padrão

Ao implementar novos processos, procedimentos ou sistemas que envolvam o Tratamento de Dados Pessoais, o **REGISTRADOR E TABELIÃO DINAMARCO** adotará medidas para garantir que as regras de Privacidade e Proteção de Dados sejam adotadas desde a fase de concepção até o lançamento/implantação destes projetos.

4.7 Dos Prestadores de Serviços Terceirizados

Os prestadores de serviços terceirizados que tratem Dados Pessoais sob as instruções do **REGISTRADOR E TABELIÃO DINAMARCO** estão sujeitos às obrigações impostas aos Operadores de acordo com a legislação e regulamentação de proteção de Dados Pessoais aplicáveis.

O **REGISTRADOR E TABELIÃO DINAMARCO** deve assegurar que no contrato de prestação de serviço sejam contempladas as cláusulas de privacidade que exijam que o Operador de Dados terceirizado implemente medidas de segurança, bem como controles técnicos e administrativos apropriados para garantir a confidencialidade e segurança dos Dados Pessoais e especifiquem que o Operador está autorizado a tratar Dados Pessoais apenas quando seja formalmente solicitado pelo **REGISTRADOR E TABELIÃO DINAMARCO**.

4.8 Do Gerenciamento de Incidentes de Segurança e de Utilização de Dados

Todos os incidentes e potenciais violações à segurança de Dados Pessoais devem ser reportadas ao Encarregado/DPO. Todos os Colaboradores devem estar cientes de sua responsabilidade pessoal de encaminhar possíveis problemas aos respectivos responsáveis, bem como de denunciar suspeitas de má utilização ou desvio de finalidade de Dados Pessoais assim que as identificarem.

No momento em que um incidente for identificado, é essencial que seja informado e formalizado de forma tempestiva, o mais breve possível, considerada a prudência e a existência mínima de indícios que toda acusação demanda, conforme determina a [***PQ TIN 02*** – Política de Gestão de Incidentes de Segurança e de Dados Pessoais] da Serventia.

4.9 Das Auditorias de Proteção de Dados

O **REGISTRADOR E TABELIÃO DINAMARCO** deve garantir que existam revisões periódicas a fim de confirmar que as iniciativas de Privacidade, seu sistema, medidas, processos, precauções e outras atividades incluindo o gerenciamento de proteção de Dados Pessoais são efetivamente implementados e mantidos e estão em conformidade com a legislação e regulamentação aplicáveis.

5. DOS DIREITOS DOS TITULARES

A LGPD traz como seu principal objetivo a proteção dos direitos fundamentais de liberdade e de privacidade dos indivíduos. Para tanto, apresenta um rol de princípios e direitos especialmente voltados à garantia de informações claras ao Titular dos Dados e imposição de limitações ao seu Tratamento.

Além de ter o direito a informações claras acerca do Tratamento de Dados, o Titular tem o direito a obter gratuitamente as seguintes providências, mediante requisição expressa ao controlador (artigo 18 da LGPD):

a) A informação, no momento em que os Dados Pessoais são fornecidos, sobre como seus Dados Pessoais serão tratados;

b) A informação sobre o Tratamento de seus Dados Pessoais e os meios de acesso aos Dados Pessoais que a **REGISTRADOR E TABELIÃO DINAMARCO** detenha sobre eles;

c) A retificação dos Dados Pessoais imprecisos, incorretos ou incompletos;

d) Quando permitido pela legislação especial e quando não houver prejuízo às atividades do **REGISTRADOR E TABELIÃO DINAMARCO**, a exclusão, bloqueio e/ou anonimização de Dados Pessoais. Isso pode incluir, mas não se limita a, circunstâncias em que não é mais necessária a retenção de seus Dados Pessoais para os propósitos para os quais foram coletados;

e) A restrição do Tratamento de Dados Pessoais em determinadas circunstâncias;

f) Opor-se ao Tratamento, se baseado em legítimo interesse;

g) A retirar o Consentimento a qualquer momento, se o Tratamento dos Dados Pessoais se basear no Consentimento do indivíduo para um propósito específico;

h) A portabilidade dos Dados Pessoais a outro fornecedor de serviço ou produto, quando permitida por lei;

i) A apresentação de queixa ao Encarregado/DPO do **REGISTRADOR E TABELIÃO DINAMARCO** ou à Autoridade de Proteção de Dados competente, se o Titular dos Dados Pessoais tiver motivos fundamentados para supor que qualquer um de seus direitos de proteção de Dados Pessoais tenha sido violado.

Tais informações deverão ser disponibilizadas de forma clara, adequada e ostensiva.

Importante frisar que a qualquer momento o Titular dos Dados Pessoais tem o direito de ver efetivados os direitos acima expostos perante o **REGISTRADOR E TABELIÃO DINAMARCO**.

As solicitações serão enviadas para o e-mail do Encarregado/DPO, juntamente com a comprovação de sua identidade e, conforme prevê a Procedimento de Atendimento aos Direitos dos Titulares [***PR TIN 13*** - Procedimento de Atendimento aos Direitos dos Titulares de Dados Pessoais].

6. DAS POLÍTICAS GERAIS

Neste tópico serão abordadas as políticas estabelecidas pelo **REGISTRADOR E TABELIÃO DINAMARCO**, que estabelecem as diretrizes a serem adotadas para conformidade com a Lei Geral de Proteção de Dados e toda legislação aplicável.

As orientações abaixo descritas deverão ser sempre observadas pelos envolvidos no Tratamento, de forma que o descumprimento será considerado incidente de segurança e de utilização de Dados com a apuração das responsabilidades devidas.

6.1 Política de Classificação da Informação

É Intuito desta Política de Classificação da Informação identificar quais os níveis de proteção que as informações disponíveis no **REGISTRADOR E TABELIÃO DINAMARCO** requerem. Também é do escopo deste documento definir os níveis de proteção e os controles a serem implementados ao longo do ciclo de vida da informação.

6.1.1 Das Responsabilidades

Proprietário dos dados: Pessoa responsável pela coleta e mantimento dos dados e das informações feitas por seu departamento ou divisão e suas responsabilidades são:

- **Revisar e categorizar** os dados e a informação coletados por seu departamento ou divisão;
- **Definir as classificações dos dados** baseado no potencial de impacto destes;
- **Compilar os dados** e assegurar que os dados compilados de múltiplas fontes sejam classificados, em relação à níveis de segurança;

- **Coordenar a classificação dos dados** e assegurar que os dados compartilhados entre departamentos estejam ao menos consistentemente classificados e protegidos;
- **Assegurar que a informação com alto e moderado impactos** estejam seguras de acordo com as diretrizes legais nacionais;
- **Desenvolver protocolos de acesso de dados** para cada classificação de dados predefinida.

Curador dos dados: Coordenador do Departamento de TI, responsável por manter e suportar os sistemas, bancos de dados e servidores que armazenam os dados organizacionais.

É também responsável pelo desdobramento de todas as regras estabelecidas pelo proprietário de dados, bem como se assegurar de que as regras aplicadas aos sistemas estão funcionando. Algumas das atribuições do curador dos dados são:

- **Assegurar que controles de acesso adequados sejam implementados,** monitorados e auditados de acordo com a classificação de dados definida pelo Proprietário de dados;
- **Submeter relatório** trimestral aos proprietários de dados levando em conta a disponibilidade, a integridade e a confidencialidade dos dados classificados;
- **Fazer backups dos dados**;
- **Validar**, periodicamente, **a integridade** dos dados;
- **Restaurar os dados** das mídias de backup;
- **Preencher os requerimentos especificados** na política de segurança da organização que trata de segurança da informação e proteção de dados;
- **Monitorar e gravar as atividades de dados,** inclusive informações acerca dos indivíduos que acessaram quais dados;
- **Criptografar dados sensíveis** mantidos em armazenamento;
- **Assegurar que a informação com alto e moderado impactos** estejam seguras de acordo com as diretrizes legais nacionais;

- **Desenvolver protocolos de acesso de dados** para cada classificação de dados predefinida.

Usuário de dados: Pessoa, entidade ou organização que possua acesso a dados e informações do **REGISTRADOR E TABELIÃO DINAMARCO** com o propósito de executar uma tarefa autorizada pelo proprietário dos dados. O usuário de dados deve utilizar os dados de forma consistente com o propósito objetivado e estar de acordo com as políticas aplicadas ao uso dos dados que tiverem acesso.

6.1.2 Das definições da classificação

- **Informação Pública:** Trata-se da informação destinada ao público em geral que já tenha sido divulgada ou de conhecimento público (por exemplo, para o público geral, fornecedores, parceiros), cuja utilização por quaisquer indivíduos independe de autorização do titular da informação e cuja divulgação dessas informações, para pessoas dentro ou fora do cartório, não seja capaz de gerar prejuízos para o **REGISTRADOR E TABELIÃO DINAMARCO**. São aquelas que não necessitam de proteção elaborada contra vazamentos, pois são de conhecimento público, no entanto, devem permanecer disponíveis e íntegras, como é o caso dos atos notariais e registrais já aperfeiçoados, as certidões impressas por solicitação, as políticas, os formulários de solicitação etc.
- **Informação Interna:** Trata-se da informação que guarde assuntos exclusivamente pertinentes à esfera interna do **REGISTRADOR E TABELIÃO DINAMARCO**, cujo acesso é liberado apenas às pessoas internas designadas para tal e que, embora o **REGISTRADOR E TABELIÃO DINAMARCO** não tenha interesse em divulgar a indivíduos externos da organização, a disponibilização dessa informação não tem o potencial de causar danos sérios ao cartório. São informações de baixo nível de confidencialidade, que não causarão grandes prejuízos caso divulgadas, porém ainda assim devem ser acessadas apenas por pessoal interno. Sua

classificação se dá principalmente com a intenção de garantir sua integridade, como é o caso dos documentos instrutórios dos atos notariais e registrais, que podem circular no ambiente interno, enquanto não se conclui a lavratura do respectivo ato.

- **Informação Restrita ou Confidencial:** Trata-se de informação sigilosa que não deve ser divulgada, total ou parcialmente, pelos Colaboradores, cujo uso é restrito a um determinado número de pessoas que tenham a necessidade de conhecê-la para desempenharem as suas atividades profissionais vinculadas ao **REGISTRADOR E TABELIÃO DINAMARCO**, que podem ser protegidas através de restrição de pastas ou diretórios de rede específicos e cuja divulgação não autorizada pode causar prejuízos ao cartório (tais como danos financeiros, ações judiciais, depreciação da imagem, etc.). **Independentemente de qualquer marcação, serão sempre consideradas Informações Confidenciais** as informações financeiras, de recursos humanos, de procedimentos de segurança e de dados pessoais sensíveis (nos termos da Lei Geral de Proteção de Dados) e que não sejam públicos por Lei.

Todas estas informações em conjunto são denominadas "**Informações Protegidas**", conforme também determina a Política de Segurança da Informação.

6.1.3 Classificação de Dados Confidenciais

Informações que devem ser classificadas como **Confidenciais,** sem prejuízo de outras que eventualmente se encaixarem no conceito exposto no item anterior:

- **Informações de autenticação:** Informações de autenticação são aqueles dados utilizados para provar a identidade de um indivíduo, podendo se tratar de sistemas ou serviços. Eles incluem: senhas, chaves e criptográficas.
- **Informação eletrônica protegida:** Toda a informação que é armazenada no formato de mídia eletrônica, isto inclui *hard drives* de computadores, todas

as formas de mídia móvel, (pen-drives, HDs removíveis, CDs, discos ópticos e *memory cards.*

As formas de transmissão incluem troca de informação pelo meio eletrônico, como internet, intranet, redes privadas, linhas discadas e transporte físico.

- **Informações de cartões de pagamento:** Informação definida pela combinação de uma ou mais das seguintes informações: Nome do titular do cartão, código de serviço, data de expiração, PIN, conteúdo da linha magnética do cartão de crédito.
- **Informação pessoal sensível:** Qualquer informação relativa a uma pessoa singular identificada ou identificável, que possa gerar qualquer tipo de discriminação, como por exemplo os dados 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, dado genético ou biométrico.
- **Informações Financeiras:** Todas as informações pessoais de cunho financeiro, como dados relativos às contas bancárias pessoais, números de cartão de crédito, saldo pessoal, dados relativos à inadimplência, bem como todos os dados relativos à protestos às pessoas físicas e jurídicas, credores e devedores.

6.1.4 Procedimentos para classificação de dados

Cabe ao proprietário de dados revisar os dados sob sua responsabilidade e determinar seu nível de impacto levando em conta:

- Caso as informações estejam incluídas de acordo com item 6.1.3, ou seja, classificadas como confidenciais, deverão ser assinaladas com nível de impacto Alto.
- Se a informação não estiver compreendida pela relação do item 6.1.3, cabe ao proprietário de dados determinar o tipo e o impacto baseados na tabela de delimitação de impacto logo abaixo.

- Se, ainda assim, não for possível caracterizar a informação em relação ao seu tipo, o proprietário de dados deverá trabalhar junto com o curador de dados para definir em qual nível de segurança está situada a informação.
- A classificação dos dados deve ser feita em função de seu nível de impacto:

Nível de impacto	Classificação
Alto	Confidencial
Moderado	Restrito
Baixo	Uso Interno
Nulo	Pública

- Cabe ao proprietário do dado apontar o nível de impacto e a classificação de cada dado e ao curador do dado, cabe aplicar aos dados o controle de segurança adequado ao nível de impacto assinalado;

6.1.5 Diretrizes para determinação do nível de impacto

Objetivo da Segurança	Impacto Potencial			
	Nulo	**Baixo**	**Moderado**	**Alto**
Confidencialidade: Restringir acesso aos dados apenas a usuários autorizados visando proteger a privacidade e assegurar a propriedade da informação.	A divulgação dessas informações não terá efeitos nas operações, ativos organizacionais ou indivíduos.	A divulgação não autorizada dessas informações terá efeitos adversos limitados nas operações, ativos organizacionais ou indivíduos.	A divulgação não autorizada dessas informações terá um efeito adverso relevante sobre operações, ativos organizacionais ou indivíduos.	A divulgação não autorizada dessas informações terá um efeito adverso grave ou muito grave nas operações, ativos organizacionais ou indivíduos.
Integridade: Guardar a informação contra modificações	A modificação ou destruição não autorizada não	A modificação ou destruição não autorizada das	A modificação ou destruição não autorizada das	A modificação ou destruição não autorizadas das

impróprias e destruição de dados garantindo a integridade e autenticidade da informação.	acarretará nenhum efeito nas operações, ativos ou indivíduos.	informações terá efeito adverso limitado nas operações, ativos ou indivíduos.	informações deverá terá efeito adverso relevante sobre operações, ativos ou indivíduos.	informações terão efeito adverso grave ou muito grave nas operações, ativos ou indivíduos.
Disponibilidade: Assegurar a confiabilidade e disponibilidade do acesso e uso da informação.	A interrupção do acesso ou uso das informações ou do sistema terá efeito leve nas operações, ativos ou indivíduos.	A interrupção do acesso ou uso das informações ou do sistema de informações terá efeito adverso limitado nas operações, ativos ou indivíduos.	A interrupção do acesso ou uso das informações ou do sistema de informações terá efeito adverso relevante nas operações, ativos ou indivíduos.	A interrupção do acesso ou uso das informações ou do sistema de informações terá efeito adverso grave ou muito grave nas operações, ativos ou indivíduos.

6.2 Política de Retenção e Descarte de Dados Pessoais

O tratamento dos dados deverá ser encerrado quando:

- A finalidade para a qual o consentimento foi obtido for alcançada;
- Os dados pessoais coletados deixam de ser necessários à finalidade pretendida;
- Transcorrer o período de tratamento;
- O titular dos dados retirar o consentimento que fundamentou o tratamento;
- Houver uma determinação legal nesse sentido.

Uma vez encerrado o tratamento, os dados pessoais deverão ser corretamente eliminados. Em alguns casos, a LGPD autoriza a guarda desses dados de forma segura, como por exemplo, para atender o cumprimento de obrigação legal ou regulatória pelo controlador.

Sobre isso, o Provimento CNJ nº 134/2022 determina no artigo 14 que a **inutilização** e **eliminação de documentos deverá ser feita em conformidade com a Tabela de Temporalidade de Documentos prevista no Provimento n. 50/2015, da Corregedoria Nacional de Justiça**.

Lembrando que a inutilização e eliminação de documentos não afasta os deveres previstos na LGPD, 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 unidade dos serviços extrajudiciais de notas e de registro.

Os Dados Pessoais não podem ser mantidos por mais tempo do que o necessário para requisitos operacionais. Isso significa que o **REGISTRADOR E TABELIÃO DINAMARCO** apenas poderá armazenar dados pessoais que estiverem fundamentados em alguma das bases legais trazidas pela legislação de proteção de dados.

Para os Dados Pessoais que envolvam questões de ordem tributária, trabalhista e previdenciária, o **REGISTRADOR E TABELIÃO DINAMARCO** se reserva no direito de mantê-los armazenados até o fim do prazo prescricional estipulado em lei.

No caso de qualquer categoria de documentos não especificados na **Tabela de Temporalidade de Documentos prevista no Provimento CNJ n. 50/2015** ou exigidos de outra forma pela lei aplicável, os dados serão armazenados de acordo com a necessidade do **REGISTRADOR E TABELIÃO DINAMARCO**, devendo ser analisado caso a caso com o Encarregado.

6.2.1 Do Armazenamento de Dados Pessoais

Todas as Informações Protegidas que devam ser armazenadas em suporte físico ou digital, quando da sua guarda pelo Colaborador, devem respeitar os seguintes cuidados, de acordo com a classificação da informação:

Suporte físico: Todos os documentos contendo Informações Internas, Confidenciais e Restritas devem ser armazenados em arquivos físicos próprios indicados pelo

REGISTRADOR E TABELIÃO DINAMARCO, de acordo com os métodos de identificação do conteúdo.

Documentos utilizados pelo Colaborador em sua estação de trabalho, quando não estiverem sendo utilizados, devem sempre ser guardados em gaveta ou armário, garantindo que tais gavetas e armários permaneçam trancados quando se tratar de Informações Confidenciais.

Nenhuma anotação relacionada às Informações Protegidas deve ser deixada à mostra, seja em cima da mesa, do computador ou em divisórias, mesmo quando o Colaborador estiver presente.

Quando o Colaborador não estiver nas dependências do **REGISTRADOR E TABELIÃO DINAMARCO**, os documentos contendo Informações Internas, Confidenciais ou Restritas não devem ficar expostos. Havendo a necessidade de transporte dos documentos, o Colaborador deve garantir que seu conteúdo não esteja aparente, por meio da utilização de pastas opacas e, caso o documento seja retirado dos arquivos físicos do **REGISTRADOR E TABELIÃO DINAMARCO**, deve solicitar autorização do responsável por seu arquivamento.

Suporte digital: Todo e qualquer arquivo que contenha Informação Interna, Confidencial ou Restrita deve ser salvo na rede corporativa do **REGISTRADOR E TABELIÃO DINAMARCO**, em diretório específico, que inviabilize o acesso por Colaboradores não autorizados. Tais arquivos devem ser salvos de forma a identificá-los quanto ao seu conteúdo.

Todo e qualquer documento ou arquivo que contenha Informações Confidenciais somente poderá ser movimentado se houver a possibilidade de recuperação ou análise dos registros de tal arquivo ou documento em caso de falhas de segurança que acarretem a perda ou o extravio das Informações Protegidas.

6.2.2 Do Armazenamento de Dados Pessoais em Dispositivos Móveis e E-mail

Para desempenho de suas funções, é vedado a todos os colaboradores o recebimento de quaisquer documentos que contenham Dados Pessoais em dispositivos particulares, seja via *WhatsApp* ou e-mail, que deverão ser recebidos apenas e tão somente por e-mail institucional, fornecido pelo **REGISTRADOR E TABELIÃO DINAMARCO** (… @tabeliaodinamarco.com.br).

6.2.3 Eliminação

A responsabilidade geral pelo descarte de dados é do CSI. Uma vez tomada a decisão de eliminá-los, de acordo com o calendário de Retenção do CNJ ou da necessidade do **REGISTRADOR E TABELIÃO DINAMARCO** – fundamentada em uma base legal –, os dados devem ser excluídos, triturados ou destruídos levando em conta se são em papel ou em formato eletrônico, considerando seu grau de equivalência, o seu valor para terceiros e o seu nível de confidencialidade, conforme abaixo:

- **Suporte físico:** os documentos que possuírem **Informações Públicas** poderão ser descartados no lixo comum; já aqueles que possuírem **Informações Internas, Confidenciais e Restritas** devem ser destruídos manualmente ou, preferencialmente, pelo aparelho fragmentador antes do descarte. No caso de **Informações Confidenciais**, o uso do aparelho fragmentador é obrigatório. Em caso de impossibilidade da utilização do aparelho fragmentador ou quando houver um grande volume de documentos a ser destruído, o Colaborador deverá acionar o gestor responsável, que por sua vez, irá promover descarte adequado.
- **Suporte digital:** os documentos deverão ser apagados permanentemente.
- **Mídias físicas:** ao serem descartadas devem ser formatadas, apagadas e conferidas para ter certeza de que estão vazias. Após esse processo, os discos são destruídos e suas mídias são perfuradas, sempre com supervisão da Equipe de TI.

O CSI deve documentar e aprovar o processo de destruição, a fim de manter um histórico que possibilite a realização de auditorias, caso necessário.

Na hipótese de o titular dos dados pessoais optar por exercer seu direito de eliminação dessas informações, seus dados pessoais deverão ser descartados prontamente pelo **REGISTRADOR E TABELIÃO DINAMARCO**, excetuadas as hipóteses de cumprimento de obrigação legal ou regulatória.

6.3 Do Manuseio das Informações Protegidas

O Colaborador é responsável pelo uso que fizer das Informações Protegidas. Assim, as regras abaixo deverão ser observadas para garantir um nível mínimo de segurança da informação.

6.3.1 Cuidados com Impressoras e Copiadoras

Os Colaboradores estão cientes que todo e qualquer uso dos equipamentos como copiadoras e impressoras, deve ser feito exclusivamente no âmbito das suas atividades profissionais, sendo vedado seu uso para fins pessoais.

Deve-se evitar imprimir documentos contendo Informações Confidenciais e, para todos os tipos de informação, os documentos impressos ou copiados devem ser retirados imediatamente dos equipamentos, sendo que o volume de cópias deve ser limitado à quantidade exata e necessária para cada tarefa, a fim de inviabilizar o acesso das Informações Protegidas por pessoas não autorizadas.

6.3.2 Uso de Informações Protegidas

O Colaborador deve tomar o máximo de cuidado com o uso que faz das Informações Protegidas, atentando-se para não deixar anotações que contenham Informações Protegidas em quadros brancos e/ou a sua manutenção em salas após o término de eventual reunião.

É proibida a transmissão de Informações Confidenciais por qualquer meio – exceto se necessário para a finalidade coletada –, assim como também é vedada reutilização de papéis para rascunho que contenham informação classificada como Confidencial ou Restrita, exceto para uso interno. Da mesma forma que os Colaboradores não devem copiar e compartilhar as Informações Protegidas sem autorização do **REGISTRADOR E TABELIÃO DINAMARCO**, estes devem tomar todos cuidados necessários para evitar o acesso por terceiros às Informações Protegidas.

Nos casos envolvendo a contratação de serviços de terceiros que justifiquem a necessidade de compartilhamento de Informações Protegidas pelo Colaborador, estas somente poderão ser compartilhadas com esses terceiros após a assinatura dos instrumentos contratuais pertinentes ou, ainda, de Termo de Confidencialidade.

6.3.3 Do Compartilhamento de Dados

O Compartilhamento de Dados Pessoais de Clientes e Colaboradores do **REGISTRADOR E TABELIÃO DINAMARCO** deverá ser feito por meio seguro e somente no estritamente necessário para a finalidade da qual os Dados Pessoais foram coletados.

Quando necessária a transmissão eletrônica de Dados Pessoais, todos os Colaboradores deverão se comprometer a utilizar padrões mínimos de segurança, podendo abranger desde a aplicação de métodos de criptografia ou similar, bloqueio de acesso por senha, uso de aplicativo de apagamento remoto, ou outros métodos de proteção, controle e rastreabilidade viáveis.

Deve-se evitar ao máximo o compartilhamento de Dados sem necessidade e verificar sempre o destinatário dos Dados, com objetivo de evitar o compartilhamento indevido.

6.3.4 Do Recebimento, Envio e Compartilhamento de Arquivos

O Colaborador é responsável pelos arquivos que recebe, envia e compartilha por meio eletrônico, através da infraestrutura tecnológica do **REGISTRADOR E TABELIÃO DINAMARCO**, seja por meio dos equipamentos de propriedade do cartório disponibilizados para o uso do Colaborador, seja por meio dos equipamentos do próprio Colaborador, ou ainda, por meio de serviços de *cloud* (nuvem).

Para garantir níveis mínimos de segurança da infraestrutura tecnológica do **REGISTRADOR E TABELIÃO DINAMARCO**, é vedado ao Colaborador:

a) Receber, enviar e compartilhar arquivos que: **(i)** tenham finalidades diversas e não relacionadas às atividades de interesse do cartório ou relativas aos seus negócios; **(ii)** contenham pornografia ou conteúdo de cunho racista, discriminatório ou qualquer outro que viole a legislação em vigor, a moral e os bons costumes; **(iii)** viole direitos de terceiros, em especial direitos de proteção de dados, direitos de propriedade intelectual, direitos autorais, direitos de imagem, entre outros; **(iv)** caracterize uma infração civil ou penal e possam causar prejuízos à **REGISTRADOR E TABELIÃO DINAMARCO** e a terceiros; **(v)** configure concorrência desleal ou quebra de sigilo profissional; e **(vi)** contenham vírus, malware ou outros códigos maliciosos.

7. DO CONTATO FACILITADO

As solicitações recebidas do titular de dados para exercer seus direitos durante todo o período de tratamento serão respondidas da forma e dentro dos prazos exigidos pelas normas aplicáveis. O Encarregado/DPO é o Sr. Afonso Pereira Oliveira Neto, que pode ser contatado através do e-mail dpo@tabeliaodinamarco.com.br ou através de formulário disponível em nossa página na internet www.tabeliaodinamarco.com.br, para exercício de seus direitos, esclarecimentos de dúvidas ou para obter mais informações sobre esta Política.

8. DAS DISPOSIÇÕES GERAIS

Os Colaboradores são responsáveis por conhecer e compreender todos os Documentos Orientadores que lhes forem aplicáveis. De forma similar, os Coordenadores são responsáveis por exigir que todos os Colaboradores de sua equipe compreendam e sigam os Documentos Orientadores aplicáveis ao **REGISTRADOR E TABELIÃO DINAMARCO**.

Os Colaboradores que tiverem perguntas ou dúvidas a respeito desta Política, incluindo seu escopo, termos ou obrigações, devem procurar o Encarregado/DPO.

Violações de qualquer documentação orientadora de Proteção de Dados podem resultar em consequências graves ao **REGISTRADOR E TABELIÃO DINAMARCO** e aos Colaboradores envolvidos. Portanto, a falha em cumprir esta Política ou relatar o conhecimento de violação desta Política poderá resultar em ação disciplinar para qualquer Colaborador envolvido.

Caso qualquer Colaborador e/ou Terceiro tenha conhecimento de uma potencial conduta ilegal ou antiética, devem imediatamente reportar a potencial violação ao Encarregado por meio do seguinte endereço eletrônico: dpo@tabeliaodinamarco.com.br.

Todos os Coordenadores devem continuamente encorajar seus liderados a reportar violações ao Encarregado.

Nenhuma regra prevista nas documentações orientadoras do **REGISTRADOR E TABELIÃO DINAMARCO**, incluindo esse Documento, proibirá que Colaboradores ou Terceiros possam reportar preocupações ou atividades ilegais para as autoridades reguladoras correspondentes.

A presente Política é desvinculada e autônoma em relação ao contrato celebrado entre o Colaborador e o **REGISTRADOR E TABELIÃO DINAMARCO**, e suas disposições deverão sobreviver após a alteração ou extinção da relação decorrente de tal contrato.

Essa Política poderá ser revista, atualizada e alterada anualmente ou a qualquer tempo, a exclusivo critério do **REGISTRADOR E TABELIÃO DINAMARCO**, sempre que algum fato relevante ou evento motive sua revisão antecipada.

* * *

Aprovação desta Política		
Nome	**Cargo**	**Data**
Rodrigo Dinamarco	Tabelião	04/09/2025
Afonso Netto	DPO	04/09/2025
Elder Rodrigues	Coordenador de TI	04/09/2025
Rosana Bighetti	Coordenadora Financeira	04/09/2025

Registro de histórico de alterações					
Versão	**Data**	**Descrição da alteração**	**Páginas alteradas**	**Revisado por**	**Aprovado por**
00	30-03-2023	Criação	---	CSI	CSI
00	10/05/2024	Revisão – sem alterações	---	CSI	CSI
00	02/09/2025	Revisão – sem alterações	---	CSI	CSI

AFONSO PEREIRA OLIVEIRA NETO:09107701667
Assinado de forma digital por AFONSO PEREIRA OLIVEIRA NETO:09107701667
Dados: 2025.09.11 13:44:46 -03'00'

ROBERTO ISSAO YOKOMIZO:29730692890
Assinado de forma digital por ROBERTO ISSAO YOKOMIZO:29730692890
Dados: 2025.09.11 16:12:01 -03'00'

RODRIGO VALVERDE DINAMARCO:13404412842
Assinado de forma digital por RODRIGO VALVERDE DINAMARCO:13404412842
Dados: 2025.09.11 18:59:28 -03'00'

ELDER RODRIGUES BARBOSA:03711082505
Assinado de forma digital por ELDER RODRIGUES BARBOSA:03711082505
Dados: 2025.09.11 16:23:40 -03'00'

ROSANA PELLICCI BIGHETTI:07568824861
Assinado de forma digital por ROSANA PELLICCI BIGHETTI:07568824861
Dados: 2025.09.11 17:05:21 -03'00'