

POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Instrumento integrante do Programa de Privacidade, Proteção de Dados Pessoais e Segurança da Informação aplicável ao Cartório do 1º Ofício Tabelionato de Notas e Protestos Raphael Chociai – Naviraí/MS (CNS 06.239-8), elaborado em conformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), com a legislação extrajudicial pertinente, com o Código Nacional de Normas e demais atos vigentes do Conselho Nacional de Justiça (CNJ), com as normas da Corregedoria-Geral de Justiça competente e com os instrumentos internos de governança, segurança da informação, continuidade, resposta a incidentes, inventário de dados, avaliação de riscos e planos de ação que compõem o Programa.

Histórico de Versões.

DATA	VERSÃO	DESCRIÇÃO	AUTOR
25 de abril de 2023	1.0	PP Versão 1.0	STQ DIGITAL LTDA
20 de março de 2026	2.0	PP Versão 2.0	STQ DIGITAL LTDA

Versão 2.0

Naviraí, Mato Grosso do Sul, março de 2026

Sumário

POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS	4
INTRODUÇÃO	4
PROPÓSITO	5
APLICAÇÃO, ESCOPO E INTEGRAÇÃO COM O PROGRAMA	7
CENÁRIOS TÍPICOS DE TRATAMENTO DE DADOS.....	8
DIRETRIZES OPERACIONAIS DO TRATAMENTO DE DADOS PESSOAIS NO CARTÓRIO	9
TERMOS E DEFINIÇÕES	12
REFERÊNCIA LEGAL E DE BOAS PRÁTICAS	17
DECLARAÇÕES DA POLÍTICA.....	21
CAPÍTULO I – DAS DISPOSIÇÕES GERAIS	21
CAPÍTULO II – DO TRATAMENTO DE DADOS PESSOAIS	21
ORIENTAÇÕES GERAIS AOS TITULARES DE DADOS PESSOAIS	23
CAPÍTULO III – DA CONSCIENTIZAÇÃO, CAPACITAÇÃO E SENSIBILIZAÇÃO	24
CAPÍTULO IV – DA SEGURANÇA E DAS BOAS PRÁTICAS	25
CAPÍTULO V – DA AUDITORIA, MONITORAMENTO E CONFORMIDADE	25
CAPÍTULO VI – DAS FUNÇÕES E RESPONSABILIDADES.....	26
CAPÍTULO VII – DOS CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES	27
CAPÍTULO VIII – DAS PENALIDADES.....	27
CAPÍTULO IX – DAS DISPOSIÇÕES FINAIS.....	28
ANEXO I – COMITÊ DE PROTEÇÃO DE DADOS PESSOAIS.....	29

POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Responsável:	Administração Superior da serventia, com apoio do Comitê de Adequação à LGPD, da Encarregada pelo Tratamento de Dados Pessoais, dos responsáveis de processo e do suporte técnico quando aplicável.
Aprovado por:	GRAZIELA SANT ANNA DE FARIA RIBEIRO
Políticas Relacionadas:	Política de Segurança da Informação; Política de Backup; Plano de Continuidade de Negócio (PCN); Plano de Resposta a Incidentes (PRI); Inventário e Mapeamento de Dados Pessoais (IDP); Relatório de Impacto à Proteção de Dados Pessoais (RIPD); Planos de Ação por Setor; ata do Comitê de Adequação à LGPD; termo de ratificação e manutenção da Encarregada pelo Tratamento de Dados Pessoais; demais atos e instrumentos de governança do Programa de Adequação aplicáveis.
Localização de Armazenamento:	Repositório institucional do Programa de Adequação, em ambiente controlado, com acesso por necessidade, preservação de rastreabilidade e guarda da versão vigente, das versões históricas relevantes e das evidências correlatas sob guarda controlada do cartório.
Data da Aprovação:	abril de 2026
Data de revisão:	abril de 2027

INTRODUÇÃO

A serventia realiza, por natureza de suas atribuições notariais e de protesto, tratamento contínuo e estruturado de dados pessoais para viabilizar a prática dos atos, a identificação das partes e interessados, a formalização de instrumentos, a emissão de certidões, o cumprimento de comunicações obrigatórias, a organização do acervo e a preservação da segurança jurídica inerente ao serviço extrajudicial. Nesse contexto, o tratamento de dados pessoais não constitui

atividade acessória ou eventual, mas parte integrante da própria operação institucional da serventia, em meio físico e digital, com reflexos diretos sobre autenticidade, publicidade, rastreabilidade, continuidade e proteção das informações tratadas.

Na prática, os dados pessoais ingressam na serventia por diferentes meios e em diferentes suportes, como documentos apresentados no atendimento, requerimentos, declarações, certidões, sistemas, comunicações institucionais, controles internos e registros necessários à execução dos fluxos de notas, protesto e rotinas administrativas correlatas. Esses dados são coletados, conferidos, utilizados, organizados, armazenados, acessados, compartilhados e preservados em conformidade com a finalidade do ato ou do processo correspondente, integrando um ciclo de vida que exige critérios claros de necessidade, controle e evidência mínima, especialmente em ambiente que combina atendimento ao público, produção documental, acervo físico e uso de sistemas de apoio.

A presente Política parte do entendimento de que a transparência institucional e a proteção de dados pessoais não são valores incompatíveis. Ao contrário, no contexto da serventia, a transparência deve ser praticada com proporcionalidade, finalidade e observância dos limites legais e regulatórios aplicáveis, de modo a assegurar ao titular informações claras sobre o tratamento de seus dados, sobre os canais de atendimento disponíveis e sobre os direitos que podem ser exercidos, sem transformar o dever de publicidade do serviço em exposição indevida de informações pessoais ou em circulação informal de dados sem necessidade.

Esta Política consolida, assim, um instrumento institucional de governança e operação voltado a orientar o tratamento de dados pessoais em coerência com a Lei Geral de Proteção de Dados Pessoais, com o marco normativo extrajudicial vigente e com os demais documentos que integram o Programa da serventia, especialmente o Inventário e Mapeamento de Dados Pessoais, o Relatório de Impacto à Proteção de Dados Pessoais, a Política de Segurança da Informação, a Política de Backup, o Plano de Continuidade de Negócio, o Plano de Resposta a Incidentes e os Planos de Ação por Setor. Seu propósito introdutório é fixar, desde logo, que privacidade, segurança da informação, rastreabilidade, evidência mínima e responsabilidade institucional devem ser tratadas de forma integrada, auditável e compatível com a realidade operacional do cartório.

PROPÓSITO

O propósito desta Política de Privacidade e Proteção de Dados Pessoais é estabelecer um conjunto coerente de princípios, diretrizes e regras operacionais que orientem o tratamento de dados pessoais no âmbito da serventia, assegurando que a gestão das informações ocorra em

conformidade com as exigências legais e normativas aplicáveis e preserve a confiança depositada pelos usuários, titulares, colaboradores, parceiros e demais pessoas que se relacionam com a serventia no exercício da atividade extrajudicial.

A Política busca traduzir, para a realidade da atividade notarial, de protesto e administrativa da serventia, o conteúdo da Lei Geral de Proteção de Dados Pessoais, da legislação de regência do serviço extrajudicial, dos atos normativos vigentes do Conselho Nacional de Justiça e das regulamentações aplicáveis da Autoridade Nacional de Proteção de Dados, convertendo esse conjunto normativo em referência prática de conduta institucional. Seu propósito não é apenas afirmar conformidade em tese, mas orientar, de modo objetivo, como os dados pessoais devem ser tratados em coerência com a finalidade pública do serviço, com a segurança jurídica dos atos, com a transparência responsável e com a proteção da privacidade.

Esta Política tem a função de sistematizar o comportamento institucional no tratamento de dados pessoais, transformando obrigações jurídicas e normativas em rotinas práticas de controle, prevenção, rastreabilidade e evidência mínima, de modo a permitir que os atos notariais, os atos de protesto, as comunicações obrigatórias, a emissão de certidões, o atendimento ao usuário e as rotinas administrativas correlatas sejam conduzidos com segurança jurídica, transparência proporcional e respeito à privacidade das pessoas envolvidas.

A Política também define parâmetros de responsabilidade compartilhada, determinando que todo colaborador, preposto, operador ou prestador de serviço vinculado à serventia participe ativamente da proteção das informações, adotando condutas compatíveis para reduzir riscos, preservar a confiabilidade dos dados tratados e evitar práticas informais que eliminem rastros, ampliem exposição indevida ou comprometam a prestação de contas.

Entre os principais objetivos desta Política, destacam-se:

- **fortalecer a governança de dados da serventia**, estruturando papéis, responsabilidades, fluxos e registros para demonstrar conformidade e permitir auditoria sobre as operações de tratamento;
- **integrar a proteção de dados ao funcionamento real da serventia**, conectando-a às práticas de segurança da informação, backup, continuidade de negócio, resposta a incidentes, controle de acesso, gestão documental e organização do acervo;
- **reduzir riscos de exposição indevida**, especialmente em atividades de atendimento presencial, manipulação de documentos, uso de sistemas, circulação de informações e compartilhamentos com terceiros legitimados;

- **promover cultura institucional de conformidade**, por meio de orientação, conscientização, capacitação e sensibilização de colaboradores, prepostos e demais envolvidos no tratamento de dados pessoais;
- **garantir que a transparência ocorra com proporcionalidade**, conciliando o dever de publicidade do serviço extrajudicial com o respeito à privacidade e aos direitos dos titulares;
- **padronizar a comunicação com os titulares**, definindo canais oficiais e procedimentos de registro, resposta e rastreabilidade das solicitações;
- **demonstrar responsabilidade ativa perante a Corregedoria competente**, o Conselho Nacional de Justiça, a Autoridade Nacional de Proteção de Dados e a sociedade, comprovando a efetividade das medidas adotadas.

Esta Política possui natureza institucional e evolutiva, devendo ser mantida coerente com os demais instrumentos do Programa, especialmente com o Inventário e Mapeamento de Dados Pessoais, com o Relatório de Impacto à Proteção de Dados Pessoais, com a Política de Segurança da Informação, com a Política de Backup, com o Plano de Continuidade de Negócio, com o Plano de Resposta a Incidentes e com os Planos de Ação por Setor, de modo que decisões administrativas, contratuais, tecnológicas e comportamentais relacionadas à privacidade e à proteção de dados sejam orientadas por critérios verificáveis, com rastreabilidade e capacidade de prestação de contas.

APLICAÇÃO, ESCOPO E INTEGRAÇÃO COM O PROGRAMA

Esta Política aplica-se a todo tratamento de dados pessoais realizado no âmbito da serventia, em qualquer etapa da atividade, em meio físico ou digital, desde o primeiro contato no atendimento até a prática do ato, a organização de documentos, a emissão de certidões, as comunicações obrigatórias, a conservação do acervo e o encerramento das rotinas administrativas correlatas. Seu alcance abrange, portanto, os fluxos de notas, protesto, atendimento, apoio administrativo, sistemas, repositórios, arquivos e demais estruturas institucionais que participem do ciclo de vida dos dados pessoais no ambiente do cartório.

A Política alcança dados de partes e interessados, representantes, procuradores, testemunhas, usuários do serviço, colaboradores, prestadores e fornecedores, bem como dados constantes de documentos apresentados para instrução, comprovantes, anexos, registros e lançamentos em sistemas, arquivos digitais de apoio, livros, repositórios físicos e materiais temporários que possam conter informações identificadas ou identificáveis. O seu escopo não se limita, assim, ao dado formalmente inserido no ato, mas compreende também os elementos

informacionais que circulam para viabilizar qualificação, conferência, emissão, comunicação, guarda, rastreabilidade e prova do serviço prestado.

A aplicação desta Política alcança colaboradores, prepostos, estagiários, terceiros autorizados e também se projeta sobre operadores contratados que realizem atividades envolvendo dados pessoais em nome da serventia, como fornecedores de software, infraestrutura, suporte técnico, segurança, armazenamento, conectividade e serviços correlatos. Nesses casos, o acesso deve ser justificado pela necessidade do serviço, limitado ao mínimo necessário e submetido a controles compatíveis com o risco, incluindo confidencialidade, restrição de permissões, rastreabilidade, cooperação institucional e observância das regras documentais e operacionais vigentes.

Esta Política deve ser observada de forma integrada com os demais instrumentos do Programa, especialmente com o Inventário e Mapeamento de Dados Pessoais, com o Relatório de Impacto à Proteção de Dados Pessoais, com a Política de Segurança da Informação, com a Política de Backup, com o Plano de Continuidade de Negócio, com o Plano de Resposta a Incidentes e com os Planos de Ação por Setor. Seu escopo, portanto, não se esgota em diretriz isolada de transparência, mas funciona como referência geral de aplicação institucional, enquanto os demais documentos aprofundam controles, riscos, evidências, continuidade, resposta a incidentes, compartilhamentos, repositórios e medidas específicas de governança e operação.

CENÁRIOS TÍPICOS DE TRATAMENTO DE DADOS

No âmbito da serventia, o tratamento de dados pessoais ocorre como parte indissociável da atividade notarial, da atividade de protesto e das rotinas administrativas que lhes dão suporte. Os dados não são tratados apenas no momento final do ato, mas ingressam, circulam e permanecem vinculados a procedimentos internos, sistemas, livros, arquivos, repositórios e comunicações institucionais que sustentam a qualificação, a formalização, a publicidade devida, a segurança jurídica e a preservação do acervo, compondo um fluxo contínuo e institucional de tratamento.

Um cenário típico é o atendimento e a instrução do ato, em que documentos e informações são apresentados, conferidos, qualificados e organizados para permitir a identificação das partes e interessados, a verificação de legitimidade, a análise de requisitos formais e a preparação da providência correspondente. Nessa etapa inserem-se, entre outros, fluxos ligados à abertura de firma, reconhecimento de firma, autenticação de cópias, requerimentos, apostilamento, certidões e atendimentos correlatos, inclusive no ambiente de protesto, com uso de documentos físicos e digitais, formulários, comprovantes, telas, arquivos de apoio e registros operacionais mínimos.

Outro cenário recorrente é a formalização, emissão e preservação do ato, em que os dados pessoais passam a compor termos, escrituras, certidões, registros de protesto, cartas de anuência, intimações e demais documentos ou lançamentos institucionais, com inserção em sistemas, livros, diretórios e acervo físico ou digital. Nessa fase, o tratamento deixa de ser apenas preparatório e assume caráter documental mais estável, exigindo preservação, rastreabilidade, controle de acesso, coerência entre o que foi praticado e o que ficou registrado e disciplina compatível com a natureza do ato e do repositório envolvido.

Também constituem cenário típico de tratamento as comunicações, entregas e compartilhamentos decorrentes do serviço, inclusive com centrais, sistemas oficiais, autoridades requisitantes, solicitantes legitimados, instituições financeiras, contabilidade, operadores e terceiros que participem de fluxos específicos. Nesses casos, os dados circulam para atender finalidade institucional delimitada, devendo existir coerência entre o conteúdo compartilhado, a legitimidade do destinatário, o fundamento do fluxo e a evidência mínima capaz de demonstrar a regularidade da comunicação, da emissão, da entrega ou do protocolo correspondente.

Por fim, há cenários transversais de tratamento que não se confundem com o “ato principal”, mas ainda assim integram a realidade informacional da unidade, como rotinas administrativas e de gestão de pessoas, suporte técnico, registros de treinamento, arquivos auxiliares, impressões de conferência, rascunhos, cópias de trabalho, materiais temporários, diretórios de apoio, registros de restauração, controles de contingência e outros elementos que podem conter dados pessoais. Embora nem sempre componham o acervo definitivo, esses materiais permanecem sujeitos a necessidade, guarda compatível, rastreabilidade, descarte seguro e integração com os demais instrumentos do Programa, justamente porque também participam do ciclo real de tratamento de dados no ambiente do cartório.

DIRETRIZES OPERACIONAIS DO TRATAMENTO DE DADOS PESSOAIS NO CARTÓRIO

O tratamento de dados pessoais no cartório deve ocorrer de forma controlada, previsível e compatível com a finalidade do ato, da rotina administrativa ou da obrigação institucional correspondente, evitando improvisos, informalidades e ampliações indevidas de uso que aumentem risco de exposição. Para isso, toda operação de tratamento — da coleta à guarda, do acesso ao compartilhamento e do uso ao descarte — deve observar necessidade, adequação e minimização, de modo que apenas os dados efetivamente indispensáveis sejam utilizados para a execução do serviço, para o cumprimento de obrigação legal ou regulatória ou para o exercício regular de direitos no âmbito da serventia.

No atendimento presencial, devem ser adotadas medidas práticas para reduzir exposição visual e circulação desnecessária de documentos. Documentos apresentados para conferência devem permanecer sob controle do atendente e fora do alcance de terceiros não envolvidos no ato, evitando permanência indevida em balcões, mesas ou áreas comuns. Da mesma forma, telas de computador devem ser utilizadas de modo a impedir visualização por terceiros, com bloqueio sempre que houver afastamento do posto de trabalho e com cuidado reforçado em atendimentos simultâneos ou em ambiente de maior circulação.

O uso de cópias, impressões, rascunhos e materiais temporários deve ser tratado como ponto crítico de risco. Esses materiais somente devem ser produzidos quando necessários ao fluxo, mantidos sob controle enquanto úteis e descartados com segurança ao término da finalidade. Não devem ser reutilizados para fins diversos nem mantidos indefinidamente fora do fluxo institucional, e qualquer eliminação deve impedir reconstrução indevida do conteúdo, observando a rotina interna de descarte seguro e a preservação do que, por dever legal, regulatório ou institucional, deva permanecer guardado.

No ambiente digital, o acesso a dados pessoais deve obedecer ao princípio do menor privilégio, com permissões compatíveis com a função e com a necessidade concreta do usuário, vedando-se acesso amplo e indistinto a sistemas, diretórios, pastas e arquivos quando isso não for indispensável à atividade correspondente. A criação, a alteração e a revogação de acessos devem observar controle interno mínimo, e a serventia deve manter disciplina de credenciais, incluindo proteção de senhas, vedação de compartilhamento de usuário, bloqueio por inatividade e revisão sempre que houver mudança de função, desligamento ou suspeita de comprometimento.

Quanto ao arquivamento, à conservação e ao fornecimento de informações, deve ser preservada distinção clara entre aquilo que integra o conteúdo formal do ato e passa a compor o acervo institucional, e aquilo que constitui material provisório de apoio. O que compõe o acervo deve ser mantido com integridade, rastreabilidade e controle de acesso compatíveis com sua natureza; o que for transitório deve ter disciplina de uso, prazo e descarte seguro. A expedição de certidões, o fornecimento de informações e os compartilhamentos necessários devem observar legitimidade, finalidade, minimização e, quando cabível, validação de identidade, uso de canal apropriado e produção de registro mínimo do atendimento ou da comunicação.

Essas diretrizes operacionais devem ser executadas em consonância com a Política de Segurança da Informação, com a Política de Backup, com o Plano de Continuidade de Negócio e com o Plano de Resposta a Incidentes. Assim, qualquer suspeita de acesso indevido, perda de documento, envio equivocado, uso informal de cópia, comprometimento de credencial, falha de sistema ou outra ocorrência capaz de afetar dados pessoais deve ser comunicada internamente e

tratada conforme o fluxo institucional aplicável, assegurando contenção, preservação de evidências, rastreabilidade e mitigação adequada.

TERMOS E DEFINIÇÕES

Para fins de interpretação e aplicação desta Política, adotam-se as definições abaixo, as quais devem ser compreendidas em consonância com a Lei Geral de Proteção de Dados Pessoais, com os normativos vigentes do Conselho Nacional de Justiça, com a regulamentação aplicável da Autoridade Nacional de Proteção de Dados e com a realidade operacional da serventia. As definições aqui apresentadas têm finalidade jurídico-operacional e buscam uniformizar a compreensão dos termos utilizados ao longo deste documento, evitando ambiguidades e assegurando coerência com os demais instrumentos do Programa.

Termo	Definição
Dados pessoais	Informação relacionada a pessoa natural identificada ou identificável, tratada no âmbito da serventia em razão da atividade notarial, da atividade de protesto, das rotinas administrativas ou dos fluxos de apoio. Incluem-se, entre outros, dados constantes de documentos apresentados para instrução, requerimentos, certidões, cadastros, livros, sistemas, comunicações institucionais, registros operacionais, arquivos físicos e digitais e materiais necessários à qualificação, formalização, emissão, comunicação, guarda e prova dos atos e procedimentos.
Dados pessoais sensíveis	Dados pessoais 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 vinculados a pessoa natural. Quando presentes no fluxo institucional, exigem maior cautela quanto à necessidade de coleta, limitação de acesso, forma de circulação, base legal predominante, compartilhamento, guarda, evidência mínima e proteção contra exposição indevida.
Titular	Pessoa natural a quem se referem os dados pessoais tratados pela serventia. No contexto desta Política, podem ser titulares as partes e interessados do ato, representantes, procuradores, testemunhas, usuários do serviço, colaboradores, candidatos, prestadores, fornecedores e demais pessoas

	naturais cujos dados ingressem ou circulem em fluxos institucionais, ainda que o tratamento não resulte, ao final, na prática de ato formal.
Tratamento	Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração. Para fins desta Política, o tratamento deve ser lido em todo o ciclo de vida do dado, desde o ingresso da informação no atendimento ou na rotina interna até sua preservação, comunicação, revisão, eventual descarte e manutenção de evidências correlatas.
Controlador	A serventia, representada por sua Administração Superior, a quem competem as decisões institucionais referentes às finalidades do tratamento, aos meios empregados, à organização da governança, à aprovação dos instrumentos do Programa e à definição das medidas administrativas necessárias à proteção dos dados pessoais tratados em seu ambiente operacional.
Operador	Pessoa natural ou jurídica que realiza tratamento de dados pessoais em nome do Controlador e conforme suas instruções, quando sua atuação envolver acesso, processamento, armazenamento, suporte, manutenção, hospedagem, conectividade, segurança, assinatura eletrônica, contabilidade, medicina ocupacional ou outros serviços correlatos. O operador não substitui a responsabilidade institucional da serventia, devendo atuar dentro do escopo contratual, com limitação de acesso, finalidade definida e observância das diretrizes documentais e técnicas aplicáveis.
Encarregada pelo Tratamento de Dados Pessoais	Pessoa indicada pelo Controlador para atuar como canal de comunicação entre a serventia, os titulares e a Autoridade Nacional de Proteção de Dados, bem como para apoiar a orientação interna, a coerência documental, a governança do Programa, o tratamento das demandas dos titulares e a articulação institucional em temas relacionados à proteção de dados pessoais.

Agentes de tratamento	Controlador e Operador, considerados em conjunto para fins da LGPD e das rotinas institucionais de governança, evidência, responsabilização e prestação de contas.
Uso compartilhado de dados	Comunicação, difusão, transferência ou disponibilização de dados pessoais a terceiro legitimado, quando necessária ao cumprimento de obrigação legal ou regulatória, à execução do serviço, ao exercício regular de direitos, à integração com sistemas oficiais, ao atendimento de requisição válida ou a fluxo institucional compatível com a finalidade do tratamento. O uso compartilhado deve observar necessidade, minimização, adequação do canal, identificação do destinatário e produção de evidência mínima quando cabível.
Incidente de segurança com dados pessoais	Evento confirmado ou sob suspeita que resulte, ou possa resultar, em acesso não autorizado, perda, destruição, vazamento, alteração indevida, indisponibilidade relevante, extravio, envio incorreto ou qualquer comprometimento de confidencialidade, integridade, disponibilidade, autenticidade ou rastreabilidade de dados pessoais tratados pela serventia. Exige registro, apuração, preservação de evidências e tratamento institucional conforme o Plano de Resposta a Incidentes e a regulamentação aplicável.
Canal do titular	Meio institucional disponibilizado pela serventia para recebimento de solicitações, esclarecimentos, reclamações e exercício de direitos relacionados a dados pessoais. Deve permitir registro rastreável da demanda, triagem, resposta formal e guarda mínima do histórico, observadas as particularidades do serviço extrajudicial e os limites legais aplicáveis ao acesso a informações.
Acervo institucional	Conjunto de livros, documentos, registros, assentamentos, sistemas, repositórios e demais suportes que integram a memória operacional, a prova dos atos e a preservação documental da serventia. Nem todo dado pessoal tratado ingressa no acervo definitivo, mas todo dado que o integra deve observar regime de guarda, rastreabilidade, controle de acesso e conservação compatíveis com sua natureza.

Material temporário de apoio	Documentos, impressões, rascunhos, cópias de trabalho, anotações operacionais, arquivos auxiliares e outros suportes utilizados de forma transitória para conferência, triagem, preparação ou execução de atos e rotinas. Embora não componham, em regra, o acervo definitivo, continuam sujeitos a necessidade, guarda compatível, limitação de acesso e descarte seguro, evitando retenção paralela, circulação informal e exposição indevida.
Repositório institucional	Ambiente físico ou digital oficialmente utilizado para guarda de documentos, registros, evidências, arquivos operacionais ou materiais do Programa. Para fins desta Política, a referência a repositório institucional indica local controlado, com acesso por necessidade, organização mínima, possibilidade de localização posterior e preservação compatível com a criticidade da informação armazenada.
Evidência mínima	Elemento documental ou registro objetivo suficiente para demonstrar que determinada ação, providência, comunicação, revisão, controle, teste, descarte, atendimento ou decisão efetivamente ocorreu. Pode consistir, conforme o caso, em protocolo, relatório, print, log, lista, ata, planilha, histórico de sistema, registro de conferência, comprovante de envio, evidência de teste ou outro documento equivalente apto a sustentar rastreabilidade e prestação de contas.
Base legal predominante	Fundamento jurídico que autoriza ou legitima o tratamento de dados pessoais em determinado fluxo, observado o contexto real da operação e a natureza do serviço prestado. A identificação da base legal predominante não dispensa a análise de finalidade, necessidade, adequação, retenção, compartilhamento e direitos dos titulares, nem autoriza uso ampliado do dado para finalidades incompatíveis com o fluxo que motivou sua coleta.
Minimização	Aplicação prática do princípio da necessidade, pela qual a serventia limita a coleta, o uso, a circulação, o compartilhamento e a retenção dos dados pessoais ao mínimo necessário para a execução do ato, da rotina ou da obrigação correspondente. A minimização deve orientar tanto o conteúdo do

	tratamento quanto a extensão do acesso, a quantidade de cópias, a exposição visual e o volume de informação compartilhada com terceiros.
Rastreabilidade	Capacidade institucional de demonstrar, com apoio em registros, evidências e organização documental mínima, o que foi tratado, por quem, em qual contexto, por qual canal, com qual finalidade e sob quais providências de controle. A rastreabilidade é requisito importante para auditoria, apuração de incidentes, revisão do Programa, atendimento a titulares e prestação de contas perante autoridades e órgãos de controle.

REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

A presente Política fundamenta-se na Constituição Federal de 1988, inclusive no reconhecimento da proteção de dados pessoais como direito fundamental, na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e na legislação aplicável à atividade extrajudicial desenvolvida pela serventia, em especial a Lei nº 8.935/1994 e a Lei nº 9.492/1997, bem como nos demais diplomas legais e infralegais que disciplinam a prática dos atos notariais, de protesto e das rotinas administrativas correlatas, quando pertinentes ao caso concreto.

No âmbito correicional e regulatório do foro extrajudicial, esta Política observa os provimentos e o Código Nacional de Normas da Corregedoria Nacional de Justiça aplicáveis aos serviços notariais e de registro, com destaque para o marco vigente de padrões mínimos de tecnologia, segurança da informação, rastreabilidade e continuidade operacional, especialmente o regime hoje estruturado em torno do Provimento CNJ nº 213/2026 e de suas integrações ao Código Nacional de Normas, com parâmetros proporcionais de resiliência, disponibilidade, integridade, autenticidade e continuidade dos serviços.

No âmbito estadual, esta Política considera as normas e orientações da Corregedoria-Geral de Justiça competente aplicáveis ao serviço extrajudicial, inclusive aquelas que tratam de privacidade, proteção de dados pessoais, política de privacidade, canal de atendimento ao titular, gestão documental, fluxo informacional e controles internos da serventia, sem prejuízo da aplicação direta da legislação federal e dos atos nacionais do Conselho Nacional de Justiça.

Complementarmente, são observados os regulamentos e orientações emitidos pela Autoridade Nacional de Proteção de Dados, especialmente aqueles relacionados à atuação da Encarregada pelo Tratamento de Dados Pessoais, à comunicação de incidentes de segurança com dados pessoais e aos parâmetros de responsabilização e prestação de contas, sempre de forma compatível com o regime jurídico do serviço extrajudicial e com as obrigações de publicidade, autenticidade, segurança jurídica e preservação institucional inerentes à atividade.

Para temas de gestão documental, preservação, integridade, autenticidade, rastreabilidade e conservação de documentos em suporte digital, são consideradas as normas e diretrizes aplicáveis à digitalização, ao arquivamento eletrônico, à guarda mínima, à temporalidade documental e ao descarte seguro, inclusive no que couber ao contexto de custódia do acervo, de documentos de apoio e de repositórios digitais utilizados pela serventia.

Como referência de boas práticas técnicas e organizacionais, esta Política adota, quando aplicável, parâmetros reconhecidos de segurança da informação, privacidade, continuidade e governança documental, sem que isso represente alegação de certificação formal. Tais referências operam como apoio metodológico complementar e não substituem os requisitos obrigatórios fixados em lei, nos provimentos do Conselho Nacional de Justiça, nas orientações da ANPD e nas normas correicionais aplicáveis.

Referência legal / de boas práticas	Aplicação e alcance no contexto desta Política
Constituição Federal de 1988 (incluindo a proteção de dados pessoais como direito fundamental)	Base constitucional da tutela da privacidade, da autodeterminação informativa, da intimidade e da proteção de dados pessoais, orientando a interpretação desta Política em consonância com os direitos fundamentais e com a atuação institucional da serventia.
Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)	Eixo principal desta Política, disciplinando princípios, bases legais, direitos dos titulares, agentes de tratamento, segurança, responsabilização, prestação de contas e parâmetros gerais para o tratamento de dados pessoais no ambiente institucional da serventia.
Lei nº 8.935/1994 (Serviços Notariais e de Registro)	Moldura institucional da atividade extrajudicial, definindo a natureza técnica e administrativa do serviço e sua vinculação à publicidade, autenticidade, segurança e eficácia dos atos jurídicos, o que influencia diretamente a forma de tratamento, guarda, emissão e preservação de dados e documentos.
Lei nº 9.492/1997 (Protesto de Títulos e Outros Documentos de Dívida)	Referência setorial necessária em razão da atividade de protesto exercida pela serventia, impactando fluxos de recepção, qualificação, intimação, certidão, comunicação, compartilhamento e preservação de informações vinculadas aos atos de protesto.
Código Nacional de Normas do Foro Extrajudicial (CNJ)	Base regulatória setorial aplicável à atividade extrajudicial, incluindo diretrizes sobre adequação à LGPD, canal do titular, aviso de privacidade, inventário, RIPD, política interna, fluxo de atendimento e demais obrigações de governança relacionadas ao tratamento de dados pessoais nas serventias.
Provimento CNJ nº 213/2026	Marco vigente de padrões mínimos de tecnologia da informação e comunicação aplicáveis aos serviços notariais e de registro, com impacto direto sobre segurança, integridade, disponibilidade, autenticidade,

	rastreabilidade, continuidade operacional, gestão de incidentes e controles mínimos relacionados ao ambiente de tratamento de dados.
Provimento CNJ nº 214/2026	Ato normativo que atualiza o regime setorial e compatibiliza o Código Nacional de Normas ao marco posterior do Provimento CNJ nº 213/2026, reforçando a necessidade de leitura atualizada da política e afastando referências superadas do ciclo anterior.
Normas e orientações da Corregedoria-Geral de Justiça competente aplicáveis ao serviço extrajudicial	Camada estadual/correcional complementar, aplicável à serventia no que se refere a política de privacidade, canal de atendimento ao titular, gestão documental, controles internos, tratamento de incidentes, governança operacional e demais exigências específicas do foro extrajudicial sob competência local.
ANPD – Resolução CD/ANPD nº 18/2024 (atuação da Encarregada pelo Tratamento de Dados Pessoais)	Referência regulatória para a atuação da Encarregada como canal entre a serventia, os titulares e a ANPD, bem como para sua função de orientação institucional, apoio à governança e articulação dos fluxos de proteção de dados pessoais.
ANPD – Resolução CD/ANPD nº 15/2024 (Regulamento de Comunicação de Incidente de Segurança)	Referência para critérios e procedimentos relacionados à avaliação e comunicação de incidentes de segurança com dados pessoais, reforçando registro, apuração, responsabilização, evidência mínima e coerência entre esta Política e o Plano de Resposta a Incidentes.
ANPD – Resolução CD/ANPD nº 4/2023 (dosimetria e aplicação de sanções administrativas)	Referência complementar para compreensão do ambiente regulatório da LGPD, útil para calibragem de riscos, priorização de controles, robustez de evidências e avaliação preventiva de conformidade institucional.
Lei nº 12.682/2012 e Decreto nº 10.278/2020 (digitalização e documentos digitalizados)	Referências aplicáveis à integridade, autenticidade, rastreabilidade, digitalização, armazenamento eletrônico e valor probatório de documentos em suporte digital, quando pertinentes ao fluxo documental e ao ambiente operacional da serventia.
Lei nº 8.159/1991 (Política Nacional de Arquivos)	Referência para gestão documental, preservação, custódia, organização arquivística e proteção especial dos documentos de arquivo, com impacto na retenção, conservação, descarte seguro e governança do acervo institucional.

Provimento CNJ nº 50/2015, com atualização pelo Provimento nº 185/2024	Referência setorial relevante para temporalidade documental, conservação, descarte e organização dos documentos do serviço extrajudicial, especialmente quando a definição de guarda e eliminação depender de critério normativo específico aplicável ao tipo documental ou ao ato praticado.
Lei nº 12.965/2014 (Marco Civil da Internet) e Decreto nº 8.771/2016	Referência complementar para segurança, proteção de registros, canais eletrônicos e medidas aplicáveis quando o tratamento envolver serviços digitais, comunicação eletrônica, aplicações de internet ou infraestrutura conectada à rede.
Lei nº 14.063/2020 (assinaturas eletrônicas)	Referência aplicável aos fluxos em que a serventia utilize ou interaja com mecanismos de assinatura eletrônica, autenticação digital, aceite eletrônico ou formalização eletrônica de documentos e comunicações, quando cabível.
Padrões e boas práticas técnicas e organizacionais (ex.: ABNT NBR ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, ISO 22301, frameworks de segurança e continuidade)	Referenciais complementares de apoio metodológico para organização de controles, segurança da informação, continuidade, gestão de riscos, privacidade e melhoria contínua, sem que sua menção represente alegação de certificação formal ou substituição das exigências legais, regulatórias e correicionais obrigatórias.
Documentos internos do Programa (IDP, RIPD, PSI, Política de Backup, PCN, PRI, PAS, ata do Comitê e termo da Encarregada)	Referências internas de execução e governança que concretizam, no ambiente da serventia, os requisitos legais e regulatórios acima indicados, servindo como evidência institucional, base de coerência documental, apoio à implementação e prestação de contas do Programa.

DECLARAÇÕES DA POLÍTICA

CAPÍTULO I – DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Política estabelece diretrizes institucionais para o tratamento de dados pessoais realizado pela serventia, em meios físicos e digitais, no exercício de suas atribuições notariais, de protesto, administrativas e de apoio, com o objetivo de assegurar governança, transparência responsável, segurança da informação e proteção dos direitos dos titulares.

Art. 2º Esta Política aplica-se a colaboradores, prepostos, escreventes, estagiários, terceiros autorizados, operadores contratados, prestadores de serviço e demais pessoas que atuem, de forma direta ou indireta, em atividades que envolvam tratamento de dados pessoais no ambiente institucional do cartório, observadas as salvaguardas documentais, contratuais e operacionais pertinentes.

Art. 3º O tratamento de dados pessoais no âmbito da serventia será orientado por finalidade legítima e definida, adequação, necessidade, minimização, transparência proporcional, segurança, prevenção e prestação de contas, observando-se que a proteção de dados deve coexistir com os deveres de preservação do acervo, autenticidade, publicidade legalmente exigida, sigilo quando aplicável e segurança jurídica inerentes ao serviço extrajudicial.

Art. 4º Esta Política integra o Programa de Privacidade, Proteção de Dados Pessoais e Segurança da Informação da serventia e deve ser interpretada em conjunto com o Inventário e Mapeamento de Dados Pessoais (IDP), com os Planos de Ação por Setor, com a Política de Segurança da Informação, com a Política de Backup, com o Plano de Continuidade de Negócio, com o Plano de Resposta a Incidentes e com o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), de modo a garantir coerência entre o que está mapeado, o que é executado e o que pode ser comprovado por evidências mínimas.

CAPÍTULO II – DO TRATAMENTO DE DADOS PESSOAIS

Art. 5º O tratamento de dados pessoais no âmbito da serventia observará os princípios previstos na LGPD e sua leitura aplicada ao contexto extrajudicial, de modo que a coleta, o uso, a conservação, o acesso, o compartilhamento e a disponibilização de dados ocorram apenas na medida necessária à prática do ato, ao cumprimento de obrigação legal ou regulatória, à execução do serviço ou ao exercício regular de direitos, evitando-se tratamentos excessivos, informais, paralelos ou sem finalidade definida.

Art. 6º A serventia adota como diretriz central a transparência proporcional, pela qual a publicidade e a transparência inerentes ao serviço não se confundem com exposição ampla ou

irrestrita de dados pessoais. A disponibilização de informações e o acesso a conteúdo institucional ocorrerão conforme legitimidade, finalidade, base normativa aplicável e limites do caso concreto, com minimização de exposição e adoção de controles compatíveis com a sensibilidade do conteúdo.

Art. 7º No atendimento presencial e na execução interna dos serviços, deverão ser adotadas medidas organizacionais para reduzir risco de exposição indevida, incluindo controle de documentos em balcão e mesas, limitação de circulação de papéis, posicionamento de monitores para impedir visualização por terceiros, bloqueio de tela quando houver afastamento do posto de trabalho e orientações contínuas de conduta a colaboradores e prepostos.

Art. 8º A produção de cópias, impressões, rascunhos, arquivos intermediários e materiais temporários será limitada ao estritamente necessário. Materiais que contenham dados pessoais deverão permanecer sob controle do responsável e serão descartados de forma segura quando cessada sua finalidade, vedada a reutilização de folhas ou documentos que contenham dados pessoais sem descaracterização completa do conteúdo e sem observância do procedimento interno aplicável.

Art. 9º O acesso a sistemas, pastas, arquivos e repositórios digitais observará o princípio do menor privilégio, devendo ser concedido apenas na extensão necessária ao desempenho da função. A criação, alteração e revogação de acessos devem ser formalizadas e rastreáveis, com revisão periódica e registro mínimo de mudanças relevantes, especialmente quando envolverem bases sensíveis, pastas administrativas, compartilhamentos relevantes ou acervo digital.

Art. 10º O compartilhamento de dados pessoais será realizado somente quando necessário para cumprir obrigações legais e regulatórias, atender requisições válidas, viabilizar comunicações obrigatórias e integrações oficiais ou executar serviços mediante operadores contratados. Em qualquer hipótese, deverá ser observado o mínimo necessário, com cautela quanto a destinatários, meios de envio, legitimidade, finalidade e registro quando aplicável, sobretudo em situações sensíveis, atípicas ou de maior risco.

Art. 11º A serventia manterá coerência entre esta Política e os documentos do Programa, especialmente a Política de Segurança da Informação, a Política de Backup, o Plano de Continuidade de Negócio, o Plano de Resposta a Incidentes, o IDP e o RIPD, assegurando que o tratamento de dados pessoais possua controles preventivos, capacidade de recuperação, disciplina de evidência e resposta estruturada a eventos adversos, com melhoria contínua.

Parágrafo único. A serventia manterá canal institucional adequado para recebimento, triagem e resposta às solicitações dos titulares, assegurando identificação mínima do requerente e do vínculo com o ato, atendimento ou relação correspondente, a fim de evitar fraude, acesso

indevido ou entrega de informações a terceiros não autorizados. O exercício dos direitos será preferencialmente formalizado por protocolo interno, formulário eletrônico ou requerimento escrito, com registro da data, do conteúdo solicitado, da validação de identidade e da resposta prestada. Quando necessário, poderão ser solicitadas informações complementares para localizar o fluxo, verificar legitimidade e delimitar o escopo da resposta, sempre observados minimização e sigilo quando aplicável.

ORIENTAÇÕES GERAIS AOS TITULARES DE DADOS PESSOAIS

A serventia trata dados pessoais de forma contínua para viabilizar a prática dos atos notariais e de protesto, a emissão de certidões, a organização e preservação do acervo, a gestão administrativa e o cumprimento de obrigações legais e regulatórias. Por essa razão, nem todo pedido do titular resultará em eliminação, bloqueio ou restrição de acesso, pois há hipóteses em que o tratamento decorre de dever legal ou regulatório, da própria natureza pública e permanente do acervo, de exigências de prova, de rastreabilidade institucional e de regras específicas de publicidade, acesso ou sigilo aplicáveis ao serviço extrajudicial. Ainda assim, a serventia assegura canais e procedimentos para orientar o titular, corrigir informações quando cabível, registrar decisões e demonstrar conformidade.

I – SE VOCÊ É PARTE, INTERESSADO, SOLICITANTE DE CERTIDÃO, REPRESENTANTE, PROCURADOR OU USUÁRIO DO SERVIÇO

Seus dados pessoais são utilizados para identificação, qualificação, verificação de legitimidade, formalização de atos, emissão de certidões, comunicações obrigatórias e preservação do acervo. Caso deseje confirmar se há tratamento, obter informações sobre categorias de dados e finalidades, solicitar correção ou atualização de dados de cadastro, ou esclarecer compartilhamentos obrigatórios, você poderá acionar o canal institucional da serventia para temas de dados pessoais, por meio do e-mail protestonavirai@outlook.com e do telefone/WhatsApp (67) 98434-4904, informando, sempre que possível, referência do ato, protocolo, data e tipo do serviço, além de apresentar documento de identificação. Em pedidos que envolvam acesso a informações de terceiros, a serventia analisará legitimidade e aplicará as restrições necessárias, inclusive exigindo procuração, comprovação de vínculo e/ou fundamento jurídico aplicável.

II – SE VOCÊ É COLABORADOR, PREPOSTO, ESTAGIÁRIO, CANDIDATO OU EX-COLABORADOR

Seus dados pessoais são tratados para gestão da relação de trabalho ou de vínculo, controles internos, cumprimento de obrigações legais, organização de escalas, treinamentos,

segurança institucional, auditorias internas e atendimento a fiscalizações. Você poderá solicitar informações sobre os dados mantidos a seu respeito, requerer correções quando cabíveis e registrar manifestações pelos canais internos definidos pela serventia, que manterá registro do atendimento e das providências adotadas.

III – SE VOCÊ É FORNECEDOR, PRESTADOR DE SERVIÇOS, PARCEIRO OU OPERADOR CONTRATADO

Dados pessoais de representantes, sócios, prepostos e pessoas vinculadas ao contrato podem ser tratados para diligências de contratação, formalização e execução contratual, pagamentos, prestação de contas, auditorias, segurança e controles correlatos. Solicitações relacionadas aos seus dados deverão indicar o vínculo contratual e, quando aplicável, o(s) sistema(s), ambiente(s) ou fluxo(s) em que ocorre a operação, para permitir resposta objetiva e verificável. Quando o fornecedor atuar como operador, poderá ser demandado a cooperar com a serventia no atendimento ao titular e na apuração de incidentes, conforme as cláusulas e instruções aplicáveis.

Como o pedido é tratado (fluxo mínimo)

A serventia registra a solicitação, valida identidade e legitimidade, analisa a base legal e as restrições aplicáveis, responde em prazo razoável e, quando não for possível atender integralmente, comunica de forma motivada as razões de fato e de direito, indicando, quando couber, alternativas cabíveis, como correção de cadastro, emissão de certidão, orientação sobre o procedimento adequado ou encaminhamento à autoridade ou instância competente.

CAPÍTULO III – DA CONSCIENTIZAÇÃO, CAPACITAÇÃO E SENSIBILIZAÇÃO

Art. 12º A serventia promoverá ações de conscientização, capacitação e sensibilização sobre privacidade e proteção de dados pessoais dirigidas a colaboradores, prepostos, substitutos, escreventes, estagiários, terceiros autorizados e demais pessoas com acesso relevante a dados pessoais, em níveis proporcionais às funções exercidas e aos riscos associados ao ambiente de tratamento.

Art. 13º As ações poderão incluir integração de novos colaboradores, treinamentos periódicos, orientações operacionais por função, comunicados, reciclagens, reforços temáticos e materiais internos de apoio, abrangendo, no mínimo, dever de confidencialidade, conduta no atendimento, proteção de telas, controle de cópias, descarte seguro, uso adequado de e-mail e mensageria, gestão de credenciais e reporte de incidentes.

Art. 14º A serventia manterá evidências mínimas das ações realizadas, tais como listas de presença, registros eletrônicos, atas, conteúdos utilizados, termos de ciência ou documentos equivalentes, para fins de prestação de contas, auditoria interna e demonstração de conformidade.

CAPÍTULO IV – DA SEGURANÇA E DAS BOAS PRÁTICAS

Art. 15º Para mitigar riscos e incidentes envolvendo dados pessoais, a serventia adotará medidas técnicas e administrativas compatíveis com sua realidade operacional, observando a Política de Segurança da Informação, a Política de Backup, o Plano de Continuidade de Negócio e o Plano de Resposta a Incidentes, integrando controles de segurança ao ciclo do dado e à rotina dos processos.

Art. 16º Consideram-se boas práticas mínimas, sem prejuízo de outras medidas: controle de acesso por necessidade e função, gestão de credenciais e senhas, proteção de estações de trabalho e telas, guarda adequada de documentos físicos, regras para circulação de pastas e cópias de trabalho, rastreabilidade de acessos e decisões relevantes, uso criterioso de dispositivos móveis e mídias removíveis e descarte seguro de rascunhos, impressões e materiais temporários contendo dados pessoais.

Parágrafo único. Na ausência de recursos tecnológicos mais avançados, poderão ser adotadas soluções proporcionais à realidade da serventia, como controles manuais, planilhas de registro, listas de conferência e procedimentos padronizados em papel, desde que formalizados, supervisionados e capazes de reduzir riscos de exposição indevida, mantendo rastreabilidade mínima e evidências de execução.

Art. 17º Qualquer incidente de segurança, ou ocorrência sob suspeita, que possa acarretar risco ou dano relevante aos titulares de dados pessoais deverá ser prontamente comunicado às instâncias internas responsáveis e tratado em conformidade com o Plano de Resposta a Incidentes, para fins de contenção, preservação de evidências, apuração, avaliação de impacto e eventual comunicação às autoridades e aos titulares quando aplicável.

CAPÍTULO V – DA AUDITORIA, MONITORAMENTO E CONFORMIDADE

Art. 18º A serventia poderá realizar verificações periódicas de conformidade, por amostragem ou por risco, para avaliar aderência a esta Política e aos demais documentos do Programa, incluindo revisão de acessos, análise de compartilhamentos, verificação de cópias de trabalho, testes de backup e restauração quando aplicáveis, checagens de segurança física e conferência de registros de incidentes e solicitações de titulares.

Art. 19º Achados relevantes deverão ser registrados e tratados por meio de plano de ação, com definição de responsáveis, prazos e evidências de conclusão, preferencialmente alinhado ao Plano de Ação por Setor, ao IDP e ao RIPD, preservando rastreabilidade e melhoria contínua.

CAPÍTULO VI – DAS FUNÇÕES E RESPONSABILIDADES

Art. 20º A titularidade e a gestão do Programa de Privacidade, Proteção de Dados Pessoais e Segurança da Informação cabem à Administração Superior da serventia, que define diretrizes, aprova esta Política, delibera sobre decisões sensíveis, assegura recursos mínimos para implementação e manutenção dos controles e responde institucionalmente pela coerência do Programa.

Art. 21º A Encarregada pelo Tratamento de Dados Pessoais atua como canal de comunicação com titulares e com a ANPD, apoia a governança do Programa, orienta a leitura dos fluxos sob a ótica da proteção de dados, acompanha temas relevantes de incidentes e auxilia na manutenção da coerência entre esta Política e os demais instrumentos correlatos.

Parágrafo único. Compete ainda à Encarregada, no âmbito desta Política:

- promover a proteção de dados pessoais e a adequação contínua ao marco legal e regulatório aplicável;
- acompanhar e apoiar a elaboração, a revisão e a atualização desta Política e de normas internas correlatas;
- propor diretrizes e prioridades para o Programa, podendo sugerir planos de ação, projetos e cronogramas;
- incentivar ações de conscientização, capacitação e sensibilização dos envolvidos no tratamento de dados pessoais;
- analisar, quando necessário, relatórios de impacto, incidentes relevantes e propostas de uso compartilhado de dados, emitindo recomendações à Administração Superior.

Art. 22º O Comitê de Adequação à LGPD, ou estrutura equivalente de governança de proteção de dados, atua com natureza consultiva e propositiva para apoiar a implementação, o acompanhamento e a melhoria contínua do Programa, sem prejuízo da competência decisória da Administração Superior.

Art. 23º Compete aos responsáveis por processos, áreas e rotinas internas zelar para que as atividades sob sua responsabilidade estejam alinhadas a esta Política, mantendo atualizados os registros e controles aplicáveis, revisando formulários, sistemas, fluxos e compartilhamentos e adotando medidas corretivas sempre que identificada inconformidade ou risco relevante.

Art. 24º Compete aos operadores e prestadores com acesso a dados pessoais atuar dentro do escopo contratual, observar finalidade, necessidade, confidencialidade, restrição de acesso e cooperação em temas de incidente, auditoria, atendimento ao titular e evidência mínima, nos limites da relação mantida com a serventia.

Art. 25º Compete a todos os usuários e integrantes da serventia utilizar de forma adequada os recursos e sistemas institucionais, zelar pela confidencialidade de credenciais de acesso, evitar o uso de mídias, contas, aplicativos ou serviços não autorizados para armazenamento e transmissão de dados pessoais, comunicar prontamente suspeitas de incidente de segurança e cumprir as orientações desta Política e das demais normas internas correlatas.

CAPÍTULO VII – DOS CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES

Art. 26º Contratos e instrumentos com operadores, fornecedores e prestadores que tenham acesso a dados pessoais deverão conter, quando aplicável, cláusulas de confidencialidade, requisitos mínimos de segurança, delimitação de escopo de acesso, dever de cooperação no atendimento a titulares, comunicação de incidentes, regras de subcontratação e responsabilidades compatíveis com o risco da operação.

Art. 27º Sempre que necessário, a serventia poderá definir, em anexo contratual, termo específico ou documento técnico, o escopo do acesso, os ambientes autorizados, perfis e permissões, prazos de retenção, forma de devolução ou eliminação de cópias de trabalho, deveres de preservação de evidências e padrões mínimos de proteção, continuidade e resposta aplicáveis ao serviço.

CAPÍTULO VIII – DAS PENALIDADES

Art. 28º O descumprimento desta Política e dos normativos correlatos poderá ensejar medidas internas e contratuais, incluindo orientação formal, reforço de supervisão, restrição de acesso, medidas disciplinares cabíveis, responsabilização contratual e demais providências necessárias à mitigação de risco e à preservação da segurança do acervo, do ambiente institucional e dos direitos dos titulares, observadas a natureza do vínculo e a gravidade do caso.

Art. 29º Situações de não conformidade relevantes, tais como tratamento fora da finalidade, compartilhamento indevido, ausência reiterada de registros essenciais do Programa, falhas graves de segurança, uso informal de canais ou descumprimento de orientações institucionais em matéria de proteção de dados, deverão ser formalmente registradas, analisadas pelas instâncias competentes e tratadas por meio de plano corretivo, sem prejuízo das consequências funcionais, administrativas ou contratuais cabíveis.

CAPÍTULO IX – DAS DISPOSIÇÕES FINAIS

Art. 30º Esta Política integra o conjunto de governança do Programa de Privacidade, Proteção de Dados Pessoais e Segurança da Informação da serventia e deve ser interpretada em harmonia com o IDP, com o RIPD, com as políticas de segurança e backup, com o PCN, com o PRI, com os Planos de Ação por Setor e com os normativos aplicáveis ao serviço extrajudicial.

Art. 31º As dúvidas quanto à aplicação desta Política e de seus documentos complementares serão submetidas à Administração Superior, com apoio da Encarregada pelo Tratamento de Dados Pessoais e, quando pertinente, do Comitê de Adequação à LGPD ou estrutura equivalente, que poderão expedir orientações complementares no âmbito de suas competências.

Art. 32º Esta Política poderá ser revista periodicamente, ou sempre que houver mudanças relevantes em processos, sistemas, operadores, riscos, orientação regulatória, exigências correicionais ou ocorrência de incidentes relevantes, mantendo-se histórico de versões e registro das alterações essenciais.

Art. 33º Os casos omissos serão resolvidos pela Administração Superior da serventia, ouvida, quando necessário, a Encarregada pelo Tratamento de Dados Pessoais e/ou o Comitê de Adequação à LGPD, no âmbito de suas competências.

Parágrafo único. Esta Política deverá ser revisada, no mínimo, anualmente, contados da data de sua aprovação, ou antes desse prazo sempre que houver mudanças relevantes que impactem o ciclo de vida dos dados pessoais, como alteração de processos, sistemas, fornecedores, formas de atendimento, acervo físico ou digital, incidentes de segurança, auditorias, correições ou alterações normativas. Sempre que a revisão do PCN, da Política de Backup, do PRI, do IDP ou do RIPD alterar fluxos, responsabilidades, riscos ou evidências críticas, esta Política deverá ser reavaliada para manter consistência documental.

ANEXO I – COMITÊ DE PROTEÇÃO DE DADOS PESSOAIS

1. Constituição e natureza

Para fins desta Política, o Comitê de Proteção de Dados Pessoais corresponde à estrutura interna de governança instituída pela serventia para apoiar a adequação contínua à Lei Geral de Proteção de Dados Pessoais, em coerência com a ata vigente do Comitê de Adequação à LGPD e com os demais instrumentos do Programa.

O Comitê possui natureza consultiva e propositiva, com a finalidade de apoiar a implementação, o acompanhamento e a melhoria contínua do Programa, contribuindo para conformidade regulatória, prevenção de riscos, coerência documental, fortalecimento da cultura de privacidade e integração entre proteção de dados, segurança da informação, continuidade, gestão documental e controles operacionais.

2. Composição

A composição do Comitê observará a estrutura definida em ata ou ato formal vigente da serventia, preferencialmente contemplando representantes de áreas estratégicas relacionadas à gestão administrativa, atividades finalísticas, suporte técnico, segurança da informação, arquivo/acervo, contratos com operadores, atendimento e demais funções consideradas relevantes para o Programa.

A Encarregada pelo Tratamento de Dados Pessoais participa da governança do Programa em articulação com o Comitê, nos termos do ato formal de manutenção vigente e das competências já reconhecidas pelos demais instrumentos do Programa.

§ 1º O cartório poderá, por ato interno da Administração Superior, alterar, ampliar ou reduzir a composição do Comitê, desde que preservadas a pluralidade mínima de áreas e a capacidade de discussão adequada dos temas de proteção de dados pessoais.

§ 2º Sempre que houver alteração na composição do Comitê, deverá ser lavrada ata e/ou emitido ato formal de designação, que passará a integrar o dossiê de governança do Programa.

3. Atribuições do Comitê

Compete ao Comitê, sem prejuízo de outras atribuições definidas em ato próprio:

- apoiar a implementação, a manutenção e a revisão desta Política e dos demais instrumentos do Programa;
- propor, revisar e acompanhar planos de ação, prioridades e cronogramas relacionados à adequação contínua da serventia às normas de proteção de dados pessoais;

- analisar, quando necessário, inventários de dados, fluxos de tratamento, relatórios de impacto, incidentes relevantes e propostas de uso compartilhado de dados;
- emitir recomendações à gestão sobre ajustes em processos, formulários, sistemas, contratos, controles e rotinas internas que envolvam tratamento de dados pessoais;
- apoiar a Encarregada na interlocução com as áreas internas, com titulares, com autoridades e com operadores, quando cabível;
- acompanhar e avaliar incidentes relevantes de segurança envolvendo dados pessoais, colaborando na proposição de medidas corretivas e preventivas;
- incentivar e apoiar ações de conscientização, capacitação e sensibilização em proteção de dados pessoais;
- contribuir para a integração do tema proteção de dados com segurança da informação, continuidade de negócio, gestão de riscos, controle interno e transparência institucional.

4. Funcionamento

O funcionamento do Comitê observará, no mínimo, as seguintes diretrizes:

- as reuniões ordinárias deverão ocorrer com periodicidade mínima compatível com a governança do Programa, admitida periodicidade semestral ou intervalo menor quando assim definido pela Administração Superior ou pelo próprio Comitê;
- poderão ser realizadas reuniões extraordinárias sempre que a complexidade dos temas tratados assim o exigir, a exemplo de incidentes relevantes, exigências regulatórias, auditorias, correções, revisões documentais ou projetos específicos de adequação;
- as reuniões deverão ser registradas por meio de ata, relatório ou documento equivalente, contendo, sempre que possível, pauta, principais encaminhamentos, recomendações formuladas e definição de responsáveis quando cabível;
- as deliberações do Comitê terão caráter recomendatório, cabendo à Administração Superior, aos responsáveis por processos e à Encarregada avaliar sua implementação no âmbito de suas competências.

5. Mandato, substituição e participação

§ 1º O mandato dos membros do Comitê será definido em ato interno de designação emitido pela Administração Superior, admitida recondução, sem prejuízo da possibilidade de substituição a qualquer tempo, por conveniência administrativa, necessidade operacional ou em caso de vacância.

§ 2º Em caso de afastamento, desligamento ou mudança de função que impeça a permanência do membro no Comitê, caberá à Administração Superior designar substituto, preferencialmente de área com perfil e atribuições semelhantes às do membro substituído.

§ 3º Poderão ser convidados, a critério do Comitê ou da Administração Superior, colaboradores, consultores, prestadores de serviço e representantes de operadores ou fornecedores envolvidos em processos com tratamento de dados pessoais para participar de reuniões específicas, sem direito a voto, quando a natureza dos temas tratados assim o justificar.