MANUAL DE BOAS PRÁTICAS

DE GOVERNANÇA DE DADOS PARA CARTÓRIOS

COMISSÃO DE PROTEÇÃO DE DADOS DA CORREGEDORIA NACIONAL DE JUSTIÇA

CNJ CONSELHO NACIONAL DE JUSTIÇA

MANUAL DE BOAS PRÁTICAS

DE GOVERNANÇA DE DADOS PARA CARTÓRIOS

COMISSÃO DE PROTEÇÃO DE DADOS DA CORREGEDORIA NACIONAL DE JUSTIÇA

CNJ CONSELHO NACIONAL DE JUSTIÇA

CONSELHO NACIONAL DE JUSTIÇA

Presidente
Ministro Luiz Edson Fachin

Corregedor Nacional de Justiça
Ministro Mauro Campbell Marques

Conselheiros
Jaceguara Dantas da Silva
Fabio Francisco Esteves
Guilherme Guimarães Feliciano
Silvio Amorim Junior
João Paulo Schoucair
Marcello Terto
Ulisses Rabaneda
Daiane Nogueira de Lira
Rodrigo Badaró

Secretária-Geral
Clara da Mota

Secretário de Estratégia e Projetos
Paulo Marcos de Farias

Diretor-Geral
Bruno César de Oliveira Lopes

Comissão de Proteção de Dados da Corregedoria Nacional de Justiça

Presidente da Comissão
Ministro Ricardo Villas Bôas Cueva

Márcia Dalla Dea Barone
Agamenilde Dias Vieira Dantas
Claudia Catafesta
Fernando Chemin Cury
Lucio Barreto Guerreiro
Alisson Alexsandro Possa
Fabrício da Mota Alves
Flávia Pereira Hill
João Rodrigo de Morais Stinghen
Laura Schertel Ferreira Mendes
Michely Freire Fonseca Cunha
Mônica TiemyFujimoto
Patricia Peck Pinheiro
Ricardo de Vasconcelos Martins

Secretários da Comissão
Alexandre Gomes Carlos
Luciano Almeida Lima

EXPEDIENTE
SECRETARIA DE COMUNICAÇÃO SOCIAL

Secretária de Comunicação Social
Ana Gabriela Guerreiro Leite

Coordenador de Multimeios
Jônathas Seixas de Oliveira

Projeto gráfico
Eron Castro

Revisão
Caroline Iltchenco Zanetti
Matheus Bacelar

2026

CONSELHO NACIONAL DE JUSTIÇA
SAF SUL Quadra 2 Lotes 5/6 - CEP: 70070-600
Endereço eletrônico: www.cnj.jus.br

SUMÁRIO

INTRODUÇÃO 7

CONCEITOS DE PROTEÇÃO DE DADOS APLICADOS AOS CARTÓRIOS 9

OPERAÇÕES DE TRATAMENTO 9

DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS 10

TITULARES DE DADOS 12

AGENTES DE TRATAMENTO 15

CONDIÇÕES DE LEGITIMIDADE PARA O TRATAMENTO DE DADOS 18

PRINCÍPIOS 18

BASES LEGAIS 23

NORMAS APLICÁVEIS ÀS OPERAÇÕES DE TRATAMENTO REALIZADAS POR CARTÓRIOS 26

PRINCIPAIS OPERAÇÕES DE TRATAMENTO DE DADOS ENVOLVENDO CARTÓRIOS 29

PRIORIDADES PARA ADEQUAÇÃO DOS CARTÓRIOS À LGPD 33

REGISTRO DE OPERAÇÕES DE TRATAMENTO 36

IDENTIFICAÇÃO DAS BASES LEGAIS 37

INDICAÇÃO DE UM ENCARREGADO 38

IDENTIFICAÇÃO DOS PAPÉIS DOS AGENTES DE TRATAMENTO 40

IMPLEMENTAR UMA POLÍTICA DE GOVERNANÇA E PROTEÇÃO DE DADOS 42

IMPLEMENTAR PROCESSOS PARA TRANSPARÊNCIA E ATENDIMENTO AOS DIREITOS DOS TITULARES 43

CRIAR PROGRAMAS INTERNOS DE TREINAMENTO E CONSCIENTIZAÇÃO DOS FUNCIONÁRIOS 45

DEFINIÇÃO DE MEDIDAS TÉCNICAS E ADMINISTRATIVAS PARA SALVAGUARDAR OS DADOS PESSOAIS TRATADOS 45

REVISÃO DE CONTRATOS E GESTÃO DO RELACIONAMENTO COM TERCEIROS 47

DIRETRIZES ESPECÍFICAS APLICÁVEIS AOS CARTÓRIOS 50
TABELIONATO DE NOTAS 50
REGISTRO CIVIL DE PESSOAS NATURAIS 51
REGISTRO DE TÍTULOS E DOCUMENTOS E CIVIL DE PESSOAS JURÍDICAS 53
REGISTRO DE IMÓVEIS 53
PROTESTO DE TÍTULOS E DOCUMENTOS 55

CONCLUSÃO 57

INTRODUÇÃO

A Lei Geral de Proteção de Dados (Lei n. 13.709/18 — LGPD)[1] inaugurou um novo arcabouço jurídico dedicado exclusivamente à regulação do tratamento de dados pessoais no Brasil. Por meio dessa lei, todos os agentes que processam dados pessoais, sejam eles agentes públicos ou privados, passam a estar obrigados a seguir uma série de normas jurídicas para garantir a devida proteção às informações de pessoas físicas. Essa lei não impõe uma barreira ao tratamento de dados, mas apresenta balizas que devem ser consideradas para que essa atividade ocorra de forma ética, transparente e segura, em consonância com os direitos fundamentais à privacidade, liberdade e autodeterminação informativa.

No contexto das serventias extrajudiciais, notadamente cartórios de registro civil, tabelionatos de notas, de protestos, registros de imóveis, de registro de contratos marítimos e de títulos e documentos de pessoas naturais e pessoas jurídicas, a adequação à LGPD é imperativa, considerando a natureza estratégica dos dados pessoais tratados rotineiramente pelos cartórios. Notários e registradores atuam como agentes delegados do poder público e, nesse papel, exercem funções de fé pública que envolvem o tratamento de dados pessoais e pessoais sensíveis que afetam diretamente a esfera privada dos indivíduos.

A ausência de um programa de governança de dados pode implicar sanções administrativas e civis, além de comprometer a confiança da população na integridade e segurança das atividades desempenhadas pelos cartórios. Além disso, a conformidade com a LGPD é um requisito crescente para a modernização e integração das serventias com plataformas eletrônicas de registros públicos.

Desenvolver e implementar um programa de governança em privacidade, com medidas técnicas e administrativas adequadas, é, portanto, não apenas uma exigência legal, mas também uma condição essencial para o aprimoramento da gestão documental, redução de riscos jurídicos e fortalecimento da segurança jurídica no âmbito dos serviços extrajudiciais.

Em atenção às mudanças definidas pela LGPD, o CNJ aprovou o Código Nacional de Normas da Corregedoria Nacional de Justiça — Foro Extrajudicial (CNN/CN/CNJ-Extra) por meio do Provimento n. 149/2023[2]. Este Provimento dedicou o Título VI à matéria de proteção de dados e ratificou a atuação da Comissão de Proteção de Dados (CPD/CN/

1 Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.
2 Disponível em: https://atos.cnj.jus.br/atos/detalhar/5243.

CNJ) em seu art. 81, originalmente criada pelo art. 3º do Provimento n. 134/2022[3]. A referida comissão tem caráter consultivo, sendo responsável por propor, independentemente de provocação, diretrizes e critérios sobre a aplicação, interpretação e adequação das serventias à LGPD.

Como resultado das atividades dessa Comissão, este Manual, portanto, foi elaborado com o objetivo de destacar boas práticas para a aplicação da LGPD no âmbito dos serviços notariais e registrais, bem como auxiliar as serventias no processo de adequação e interpretação de outras normas aplicáveis, como é o caso dos provimentos do CNJ.

Dadas as especificidades das serventias cartorárias, a sua regulação e dinâmica própria, é fundamental estabelecer diretrizes adaptadas a essa realidade. Esse é justamente o objetivo deste Manual, que cumpre o artigo 50 da LGPD ao ilustrar regras de governança e boas práticas setoriais, para facilitar o cumprimento da lei para cartórios. Essas diretrizes e conceitos reunidos neste Manual podem, a critério do responsável pela serventia, ser incorporados aos respectivos programas de governança.

Por meio deste Manual, os responsáveis que atuam nas serventias extrajudiciais passam a conhecer as melhores práticas para cumprir a LGPD sem comprometer a acessibilidade da informação pública, promovendo uma gestão responsável e segura dos dados tratados. O objetivo é garantir que as serventias, ao desempenharem suas funções, protejam os dados pessoais, respeitando os princípios de proteção de dados, em conformidade com as exigências legais e normativas pertinentes.

3 Disponível em: https://atos.cnj.jus.br/files/original141307202208256307837 3a0892.pdf.

CONCEITOS DE PROTEÇÃO DE DADOS APLICADOS AOS CARTÓRIOS

OPERAÇÕES DE TRATAMENTO

Nos termos do art. 5º, X da LGPD, o tratamento de dados abrange qualquer operação realizada com dados pessoais, desde a coleta até a eliminação, incluindo na análise de todos os contratos com dados pessoais das partes. Veja alguns exemplos práticos de tratamento de dados no ambiente cartorário:

- **Coleta**: preenchimento de dados em requerimentos físicos ou eletrônicos, como nos pedidos de expedição de certidão que exijam a identificação do solicitante; coleta de cópias de documentos que contenham dados pessoais para atos notariais e registrais; filmagens de ambiente por meio de câmeras de segurança; coleta de dados de candidatos a vagas de emprego ou de colaboradores para recrutamento, seleção e assinatura de contrato de trabalho.
- **Utilização**: uso dos dados para cumprir a finalidade do serviço solicitado, como lavrar uma escritura, registros, averbação ou emitir uma certidão; uso de dados dos colaboradores para operacionalizar a gestão de recursos humanos; uso das filmagens de câmeras de segurança para diferentes finalidades, como por exemplo monitoramento para proteção do acervo, a depender do contexto fático que justifique sua utilização.
- **Acesso**: visualização de dados por integrantes do quadro funcional do cartório para execução dos serviços, de acordo com as políticas internas de restrição. Acesso ao banco de dados por fornecedores de serviços de software e tecnologia para manutenção.
- **Reprodução**: geração de cópias físicas ou digitais dos atos para arquivamento, emissão de certidão ou criação de backup.
- **Transmissão**: envio de informações obrigatórias para órgãos públicos, como Receita Federal através da Declaração de Operação Imobiliária ou para o INSS no caso de registro de óbitos.
- **Armazenamento ou conservação**: guarda dos documentos e livros cartorários pelo prazo legal determinado para cada tipo de ato, em vias físicas ou digitais.
- **Exclusão ou eliminação**: descarte de documentos que não precisam ser mantidos, respeitados os prazos legais. O descarte envolve arquivos físicos e digitais.

DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

Nos termos do art. 5º, I da LGPD, um dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável. Os dados pessoais podem identificar uma pessoa de forma direta, como CPF, foto, documento de identidade. Em outros casos, a identificação ocorre indiretamente, por meio da combinação de diversas informações, como primeiro nome, data de nascimento, preferências ou placa do carro.

Dentro da categoria de dados pessoais, há aqueles classificados como dados sensíveis, que exigem um nível de proteção complementar devido ao seu potencial impacto sobre direitos fundamentais dos titulares. De acordo com o art. 5º, II da LGPD, dados sensíveis incluem informações sobre:

- origem racial ou étnica;
- convicção religiosa;
- opinião política;
- filiação a sindicato ou à organização de caráter religioso, filosófico ou político;
- dado referente à saúde ou à vida sexual;
- dado genético ou biométrico.

Por fim, conforme o art. 5º, III da LGPD, os dados anonimizados são aqueles que não permitem a identificação do titular e, por isso, não são considerados dados pessoais, desde que não possam ser revertidos por meios técnicos razoáveis[4].

4 Para mais informações sobre a anonimização dos dados, consulte o estudo técnico realizado pela ANPD sobre a anonimização de dados na LGPD. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd___analise_juridica.pdf; https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd_uma_visao_de_processo_baseado_em_risco_e_tecnicas_computacionais.pdf; https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/estudo_de_casos_sobre_anonimizacao_de_dados_na_lgpd_.pdf.

CONCEITO DE DADO PESSOAL — EXEMPLO 1

Jéssica dá à luz a sua filha, Bruna, em uma maternidade em Minas Gerais que possui convênio com o Cartório de Registro Civil das Pessoas Naturais para a realização do registro de nascimento diretamente no hospital. Logo após o parto, o setor administrativo da maternidade recolhe os documentos necessários e envia, de forma eletrônica, os dados para o cartório responsável.

Para efetuar o registro, são informados, dentre outros: o nome completo da mãe, seu CPF, número de identidade, endereço residencial, bem como dados constantes na Declaração de Nascido Vivo (DNV), como a data, hora e local do nascimento, o sexo de Bruna e, quando reconhecido, o nome completo e dados do pai. A partir dessas informações, o cartório realiza o registro do nascimento e emite a certidão eletrônica, que é entregue a Jéssica ainda durante o período de internação hospitalar.

Todos os dados coletados para esse procedimento — nome, documentos de identificação, endereço, filiação, data e local de nascimento — constituem dados pessoais nos termos da LGPD, pois permitem a identificação inequívoca dos titulares (Jéssica, Bruna e eventualmente o pai).

Esse exemplo ilustra como o tratamento de dados pessoais está presente desde os primeiros atos da vida civil e demonstra a importância de que os cartórios e os sistemas de registro digital observem os princípios da finalidade, necessidade, segurança da informação e transparência, assegurando a proteção dos dados pessoais dos cidadãos desde o nascimento.

CONCEITO DE DADO PESSOAL — EXEMPLO 2

Amanda adquire um apartamento em Teresina(PI) e apresenta a escritura pública de compra e venda ao Cartório de Registro de Imóveis da circunscrição competente.

Para realizar o registro, o escrevente responsável extrai da escritura e documentos pessoais apresentados os dados de qualificação básica das partes, como nome completo, CPF, estado civil, regime de bens, profissão e endereço.

Além disso, são tratados dados específicos do imóvel, como a matrícula, descrição do bem (metragem, localização, confrontações), valor da transação e informações sobre os gravames que incidem sobre o imóvel. Após o exame de legalidade, o registrador lança o ato no fólio real.

Todos esses elementos — dados de qualificação das partes e dados vinculados à operação imobiliária — constituem dados pessoais para fins da LGPD, pois identificam de forma clara os compradores, vendedores e até terceiros envolvidos (como fiadores, cônjuges, confrontantes e titulares de outros direitos reais).

Embora se refiram ao bem, os dados do imóvel tornam-se *dados pessoais* ao se vincularem às pessoas naturais que constam na matrícula.

TITULARES DE DADOS

É titular de dados a pessoa natural a quem se referem os dados objeto de tratamento[5]. Nesse conceito, enquadram-se apenas pessoas naturais vivas, uma vez que a ANPD fixou entendimento de que pessoas falecidas também não são objeto de tutela na LGPD[6]. Esse entendimento já vinha sendo apontado também pelo CNJ ao prever menor restrição à publicização de dados de pessoas falecidas[7].

Na prática dos cartórios, os titulares são, em sua grande maioria, os usuários, solicitantes e pessoas que figuram nos títulos e documentos apresentados dos serviços notariais e registrais, conceito que abarca todas as partes qualificadas nos atos praticados. Além disso, são titulares os colaboradores da serventia, prestadores de serviço e todos os visitantes de suas instalações, sobretudo quando há coleta de imagens por meio de câmeras de segurança instalados pelo responsável pela serventia.

5 Presente no art. 5º, V da LGPD, esse conceito estabelece que apenas pessoas naturais podem ser consideradas titulares de dados pessoais, excluindo-se, portanto, dados de pessoas jurídicas.

6 Nota Técnica n. 3/2023/CGF/ANPD. A referida nota cita que outras normas do ordenamento jurídico brasileiro visam proteger os direitos de pessoas falecidas como nos direitos de personalidade. A LGPD, portanto, não é a seara adequada para proteção dos direitos da personalidade, porque já existem outras leis que tutelam os direitos de pessoas falecidas.

7 CNN: "Art. 110. A certidão de testamento somente poderá ser fornecida ao próprio testador ou mediante ordem judicial. Parágrafo único. Após o falecimento, a certidão de testamento poderá ser fornecida ao solicitante que apresentar a certidão de óbito"; "Art. 119. As restrições relativas aos dados sensíveis elencados pelo inciso II do art. 5º da Lei n. 13.709/2018 não se aplicam ao caso de pessoa falecida".

CONCEITO DE TITULAR DE DADOS — EXEMPLO 1

Isabel, proprietária de um imóvel urbano em Curitiba, comparece ao Cartório de Registro de Imóveis para averbar a construção de uma edícula em sua residência. Para isso, apresenta os documentos exigidos: sua identidade, CPF, dados sobre seu endereço, número da matrícula do imóvel e o alvará de construção expedido pelo José, responsável pelo setor de obras da prefeitura. Todas essas informações são processadas e incluídas na matrícula do imóvel, passando a integrar os registros públicos daquela serventia.

Nesse contexto, Isabel e José são titulares dos dados pessoais tratados pelo cartório. Conforme a LGPD (art. 5º, V), o titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Ou seja, é ela quem possui direitos sobre as informações que a identificam e que estão sendo manipuladas pela serventia — ainda que esse tratamento esteja fundamentado em obrigação legal, como ocorre nos registros públicos.

Essa pessoa não precisa autorizar o uso de seus dados para a realização do ato, pois há base legal para esse tipo de tratamento[8]. Ainda assim, como titular, tem garantidos direitos como acesso às informações registradas, correção de eventuais dados incompletos ou incorretos e a transparência quanto à finalidade do uso dessas informações, conforme previsto nos artigos 18 e 23 da LGPD.

Esse exemplo mostra como o titular de dados é o centro da proteção jurídica conferida pela LGPD. Ainda que os cartórios tenham respaldo legal para tratar dados pessoais, devem fazê-lo com responsabilidade, segurança e respeito aos direitos dos titulares, especialmente no que diz respeito à precisão, transparência e minimização do tratamento.

CONCEITO DE TITULAR DE DADOS — EXEMPLO 2

O advogado Rafael atua representando seus clientes em um processo de cidadania italiana. Para instruir o pedido, precisa obter certidões de nascimento relacionados à família Bianchi, cujos antepassados constam registrados em uma serventia de Registro Civil das Pessoas Naturais de Belo Horizonte.

Para fazer a solicitação, Rafael preenche o requerimento pela plataforma Registro Civil, informando seus próprios dados pessoais, que serão utilizados para identificação do solicitante, emissão de protocolo e envio das certidões solicitadas.

Embora não conste como registrado nos livros do cartório, Rafael é titular de dados pessoais, pois seus dados pessoais são tratados pela serventia. O fato de ele representar clientes não altera sua condição: os dados pessoais fornecidos para a solicitação são dele e, portanto, estão protegidos pela LGPD.

8 LGPD, art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

(...) II — sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; e LGPD, Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...)

II — para o cumprimento de obrigação legal ou regulatória pelo controlador;

A LGPD estabelece uma categoria especial de titulares, que são as crianças e adolescentes. O tratamento de seus dados deve sempre observar o princípio da proteção integral e o melhor interesse do titular (art. 14, caput, LGPD), em consonância com o Estatuto da Criança e do Adolescente, Lei n. 8.069/1990, e com a Lei n. 15.211/2025, que dispõe especificamente sobre a proteção de crianças e adolescentes em ambientes digitais, que entrou em vigor em 17 de março de 2026.

Nos serviços notariais e de registro, isso significa que:

- O atendimento deve ser feito com sensibilidade, garantindo transparência e linguagem acessível aos pais ou responsáveis (art. 14, §§ 2º e 6º, LGPD).
- O tratamento deve respeitar os limites da finalidade, sem solicitar dados além dos estritamente necessários para a prática do ato (art. 14, §4º, LGPD).
- O registrador deve adotar medidas de segurança para resguardar as informações, tanto no ambiente físico quanto no digital (Lei n. 8.935/94, art. 30, I).

A coleta e guarda de informações de crianças e adolescentes nos cartórios se fundamenta no cumprimento de obrigação legal ou normativa (art. 7º, II, LGPD), já que os dados inseridos em livros e sistemas integram o acervo público e possuem natureza permanente.

Insta destacar que os registros, livros e documentos, assim como os compartilhamentos obrigatórios de informações com outros órgãos públicos (por exemplo, Receita Federal ou tribunais), não podem ser apagados ou suprimidos, pois atendem a comandos legais e à função pública desempenhada pela serventia[9].

Contudo, em situações **facultativas e acessórias**, pode haver coleta de dados mediante consentimento dos pais ou responsáveis, sendo possível a sua revogação a qualquer tempo, com a consequente exclusão dos dados.

TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES — EXEMPLO

Um cartório criou em seu site uma seção de notícias institucionais para divulgar eventos de cidadania. Em determinado ano, foi realizado um Dia de Cidadania, e uma mãe autorizou, por escrito, a publicação da foto dela e de seu filho de 12 anos na matéria vinculada ao site.

No ano seguinte, a criança pediu para que a imagem fosse retirada, alegando não querer que os colegas da escola tivessem acesso público ao tema do evento. Nesse caso, como se trata de uso de imagem para finalidade de comunicação institucional opcional, o consentimento pode ser retirado, e o cartório deve remover a fotografia do site.

9 Provimento n. 50/2015/CNJ c/c arts. 7º, II e 15, III, LGPD.

Sobre o tema, insta destacar uma distinção essencial:

- **Atos registrais obrigatórios**: consentimento não é a base legal e a retirada não autoriza exclusão de dados (ex.: registro em livros e arquivos).
- **Serviços facultativos**: consentimento é a base legal, podendo ser retirado a qualquer tempo com a exclusão dos dados (ex.: foto em notícia institucional, cadastro em newsletter, participação em pesquisa de satisfação).

AGENTES DE TRATAMENTO

De acordo com o art. 5º, IX, da LGPD, são agentes de tratamento de dados pessoais o controlador e o operador. O controlador é aquele que toma as principais decisões sobre o tratamento de dados pessoais, incluindo a definição das finalidades e os meios utilizados para esse tratamento.

No caso dos cartórios, de acordo com o art. 82 do Código Nacional e Normas da Corregedoria Nacional de Justiça (CNN), os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro, na qualidade de titulares das serventias, interventores ou interinos, são controladores no exercício da atividade típica registral ou notarial, a quem compete as decisões referentes ao tratamento de dados pessoais. Ainda, os administradores dos Operadores Nacionais de registros públicos e de Centrais de serviços compartilhados são controladores para fins da legislação de proteção de dados pessoais. Não se trata de uma controladoria conjunta com as serventias, na medida em que não há tomada de decisões em conjunto, mas apenas compartilhamento de dados entre controladores autônomos.

Já o operador é aquele que realiza o tratamento de dados pessoais em nome do controlador e conforme as instruções recebidas. O operador não tem autonomia para definir a finalidade do tratamento e deve seguir as determinações do controlador.

De acordo com o art. 83 do CNN, é pessoa externa ao quadro funcional da serventia, contratada para serviço que envolva o tratamento de dados pessoais em nome e por ordem do controlador.

Nos serviços notariais e de registro, entretanto, a figura do **controlador** assume contornos específicos:

1. **Oficial como controlador formal** — O art. 82 do CNN dispõe que os titulares de delegação, interventores ou interinos são considerados controladores. No entanto, essa controladoria não significa liberdade para escolher finalidades. Diferentemente de uma empresa privada, o oficial **não cria as finalidades do tratamento**, pois estas já estão **definidas em lei ou em atos normativos**.

2. **Finalidade legalmente predeterminada** — Conforme o art. 23, §4º, da LGPD, os serviços notariais e de registro exercidos por delegação do Poder Público recebem o mesmo tratamento dado a pessoas jurídicas de direito público. Isso significa que o tratamento de dados deve sempre observar a **finalidade pública**, vinculada ao cumprimento de atribuições legais, sem margem de discricionariedade para o oficial.

3. **Operador externo** — Já o art. 83 do CNN define o operador como pessoa externa ao quadro funcional da serventia contratada para executar serviços que envolvam tratamento de dados em nome do controlador. Exemplo: empresa de TI contratada para armazenar ou processar dados em nuvem.

4. **Compartilhamento entre controladores autônomos** — Os administradores de Operadores Nacionais de registros públicos e centrais de serviços eletrônicos também são controladores, mas de forma autônoma. Não há controladoria conjunta com as serventias, apenas **compartilhamento de dados entre controladores distintos**, cada um com sua responsabilidade legal.

CONCEITO DE AGENTE DE TRATAMENTO — EXEMPLO 1

Em uma cidade do interior de São Paulo, um Cartório de Registro Civil e Tabelionato de Notas decide modernizar seus serviços e implantar um sistema digital para a lavratura e o arquivamento eletrônico de escrituras públicas. O responsável pela serventia, nomeado por concurso público e titular da delegação, é quem define as finalidades desse tratamento de dados, como a digitalização de atos notariais, o armazenamento seguro de documentos e o compartilhamento de dados com o Operador Nacional do Registro Civil. Ele também escolhe quais fornecedores contratar, quais tecnologias utilizar, e determina quais dados pessoais serão coletados, como nome, CPF, endereço e estado civil dos usuários.

Nesse cenário, o titular da serventia exerce a função de controlador de dados pessoais, nos termos do art. 5º, VI, da LGPD e do art. 82 do CNN, pois é ele quem toma as decisões essenciais sobre o tratamento, inclusive quanto à finalidade e aos meios a serem utilizados. A responsabilidade pelas decisões relativas ao uso dos dados é sua, ainda que ele atue em nome de uma delegação pública.

Para implantar o novo sistema digital, o cartório contrata uma empresa especializada em tecnologia da informação, que desenvolverá a plataforma e realizará a manutenção do ambiente virtual. Essa empresa terá acesso aos dados pessoais dos usuários da serventia durante a execução do serviço, mas não poderá utilizá-los para nenhuma outra finalidade, nem tomar decisões autônomas sobre seu uso. Ela apenas seguirá as orientações fornecidas pelo titular da serventia sobre como e quando tratar esses dados.

Nesse caso, a empresa contratada atua como operadora de dados pessoais, conforme previsto no art. 83 do CNN e no art. 5º, VII, da LGPD. Trata-se de uma pessoa jurídica externa ao cartório que realiza o tratamento em nome e por ordem do controlador, sem autonomia decisória sobre a finalidade do tratamento.

Esse exemplo mostra, de forma prática, como se dá a distinção entre controlador e operador no âmbito das serventias extrajudiciais. O controlador (titular da serventia) toma decisões estratégicas e legais sobre os dados, enquanto o operador executa tarefas técnicas sob sua supervisão, sempre dentro dos limites estabelecidos. A correta identificação desses papéis é fundamental para a responsabilização adequada de cada agente de tratamento e para garantir a conformidade com a LGPD.

Eliminando dúvida conceitual sobre os agentes de tratamento, a Diretriz n. 7/2024 da Comissão de Proteção de Dados reforça o entendimento de que o colaborador da serventia não é considerado operador para os fins da LGPD:

> **DIRETRIZ 7/2024** (CPD/CN, 14ª Sessão Ordinária, Processos 05252/2024 e 0008172-52.2023.2.00.0000, j. 13/06/2024)
>
> O operador, previsto no artigo 83 do Código Nacional e Normas da Corregedoria Nacional de Justiça, deverá ser, necessariamente, pessoa externa ao quadro da Serventia[10].

10 Ver PDF 04586/2023. Disponível em: Comissão de Proteção de Dados da Corregedoria Nacional de Justiça — Portal CNJ. Acesso em: 4 de maio de 2025.

CONDIÇÕES DE LEGITIMIDADE PARA O TRATAMENTO DE DADOS

PRINCÍPIOS

Os princípios previstos na LGPD (art. 6º) podem ser utilizados como parâmetro norteador ao longo de todo o tratamento de dados pessoais realizado. Eles se encontram listados na tabela abaixo, que explica o significado de cada princípio e o que as serventias devem fazer para garantir o seu cumprimento.

PRINCÍPIO	DEFINIÇÃO	EXEMPLOS
Boa-fé (art. 6º, caput)	O princípio da boa-fé fundamenta os demais princípios e deve guiar a atuação dos cartórios e a interpretação das autoridades fiscalizadoras (ANPD e corregedorias). A presença de boa-fé pode atenuar sanções (art. 52, §1º, II, LGPD). A boa-fé subjetiva orienta que o tratamento seja feito com lealdade e honestidade; em sua modalidade objetiva, orienta o respeito aos direitos do titular e a implementação de medidas eficazes para segurança da informação. A boa-fé também exige que tal informação seja mantida em sigilo, não podendo ser objeto de conversas pessoais ("fofoca"), principalmente se o caso envolver pessoas famosas.	Um casal comparece ao tabelionato para lavrar uma escritura de união estável. Durante o atendimento, uma das partes menciona ter filhos de uma relação anterior. Apesar de essa informação surgir naturalmente na conversa, ela não é relevante para a lavratura da escritura, e não será mencionada no documento. Ao conversar pelo WhatsApp sobre a sua demanda no cartório, o cliente acaba revelando informações sobre sua saúde durante uma conversa. Embora não sejam necessárias para o ato, os colaboradores do cartório devem manter sigilo sobre ela.

PRINCÍPIO	DEFINIÇÃO	EXEMPLOS
Finalidade (art. 6º, I)	O tratamento de dados deve ocorrer para propósitos legítimos, específicos e informados ao titular. No setor público,[11] deve atender ao interesse público, com o objetivo de executar as competências legais. Logo, não se admite sua utilização dos dados tratados para fins incompatíveis com o interesse público e legalidade. Ainda que o titular torne públicos seus dados pessoais, eles continuam sujeitos à proteção da LGPD.	Um cartório registra dados de pais e recém-nascidos para lavrar a certidão de nascimento. Esses dados são tratados exclusivamente para fins do registro e emissão do documento. Utilizar essas informações para oferecer produtos de terceiros ou encaminhar a instituições privadas sem base legal válida violaria a finalidade. O tratamento deve se restringir ao escopo legal da atividade registral.
Adequação (art. 6º, II)	Os dados devem ser tratados de forma compatível com a finalidade informada aos titulares de dados, sem desvios de uso.	Para lavrar uma escritura pública de compra e venda, o tabelião coleta os dados das partes envolvidas e do imóvel. Pedir informações sobre a religião ou renda das partes não se ajusta à finalidade do ato. Isso caracterizaria um desvio da adequação do tratamento. Os dados devem ser compatíveis com o serviço prestado.
Necessidade (art. 6º, III)	A LGPD exige que o tratamento de dados seja limitado ao mínimo necessário para atingir a finalidade informada. O princípio da necessidade impõe tratamento mínimo e proporcional: não devem ser tratadas informações excessivas ou irrelevantes. Esse princípio também se aplica ao armazenamento, garantindo que os dados sejam mantidos apenas pelo tempo necessário para cumprir sua finalidade.	O credor apresenta um título para protesto contendo nome e CPF do devedor. O cartório deve se limitar a esses dados, sem exigir número de RG, endereço completo ou profissão, se não forem essenciais ao ato. Exigir dados desnecessários representa coleta excessiva.

11 Embora administradas em caráter privado, as serventias extrajudiciais são equiparadas ao setor público para fins de proteção de dados, conforme o art. 23, § 4º, da LGPD.

PRINCÍPIO	DEFINIÇÃO	EXEMPLOS
Livre acesso (art. 6º, IV)	Deve ser assegurado ao titular o acesso facilitado às informações sobre seus dados e sobre o tratamento realizado.	O cartório deve informar ao titular quais **dados pessoais** constam em seus sistemas administrativos (nome, CPF, RG, endereço, e-mail, filiação etc.), sem necessidade de indicar o livro correspondente. A **localização registral específica** (por exemplo, matrícula n. X ou livro de nascimento no registro civil) é fornecida apenas por meio de busca ou certidão, sujeita ao pagamento de emolumentos. (art. 98, CNN) As **atualizações cadastrais administrativas** (como telefone ou e-mail no prontuário de atendimento) são gratuitas. Já a **alteração de dados nos livros do cartório** (como estado civil) depende da apresentação do documento oficial e da prática do ato registral, com cobrança dos emolumentos devidos.
Qualidade dos dados (art. 6º, V)	Os dados devem ser exatos, claros, relevantes e atualizados, conforme a necessidade e a finalidade do tratamento.	Os dados que integram o **prontuário administrativo de usuários**, como telefone, e-mail ou endereço para contato, são regidos pela LGPD, estando sujeitos ao **princípio da atualização**, podendo ser corrigidos ou atualizados independentemente da prática de ato registral.
Transparência (art. 6º, VI)	O titular precisa saber como, por quem e para quê seus dados são tratados. Isso implica receber informações claras, precisas e acessíveis sobre quais dados estão sendo tratados, para quais finalidades, por quanto tempo serão armazenados e com quem serão compartilhados. A transparência reforça a confiança na serventia.	Dentro dos cartórios, o **princípio da transparência** na LGPD se concretiza por meio de medidas que asseguram ao titular informações claras sobre o tratamento de seus dados. Isso envolve: (i) disponibilizar **política de privacidade** acessível ao público, em linguagem simples, explicando quais dados são coletados, para qual finalidade e por quanto tempo permanecem armazenados; (ii) cumprir o **dever de comunicação em caso de incidente de segurança** que possa gerar risco ou dano relevante ao titular, conforme art. 48 da LGPD; (iii) indicar **encarregado de dados** (DPO) e divulgar sua identidade e formas de contato de maneira clara e objetiva, preferencialmente no site do cartório, como prevê o art. 41, §1º; (iv) manter **canal de atendimento ao titular** para pedidos de acesso, correção e atualização de dados; e (v) fornecer informações sobre eventuais **compartilhamentos obrigatórios** (como comunicações ao IBGE, Receita Federal, INSS, centrais eletrônicas).

PRINCÍPIO	DEFINIÇÃO	EXEMPLOS
Segurança (art. 6º, VII)	O princípio da segurança determina que as serventias adotem medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, vazamentos e outros incidentes de segurança. O objetivo dessas medidas é proteger a confiabilidade das informações, que se fundamenta em três elementos: (i) integridade — garantia de que os dados não serão alterados de forma indevida, acidental ou intencional, preservando sua exatidão e consistência; (ii) confidencialidade — restrição de acesso às informações apenas por pessoal autorizado; e (iii) disponibilidade — possibilidade de acessar as informações com agilidade, quando necessário. No contexto dos cartórios, a principal referência para essas medidas é o Provimento CNJ n. 213/2026, mas também podem ser consideradas as boas práticas indicadas pela ANPD em guias e regulamentos. Já a LGPD fixa que essas medidas devem guardar relação à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados.	**Cartório de pequeno porte** Em um cartório com apenas **dois funcionários**, a **pasta de pessoal** (com dados básicos, de saúde, férias, ponto, folha de pagamento) fica acessível a ambos, já que não há setores separados e a atividade exige que todos tenham ciência mínima das rotinas administrativas. O controle de acesso pode ser feito apenas por pastas físicas ou arquivos digitais compartilhados, sem medidas avançadas de segurança. **Cartório de grande porte** Já em um cartório com **dezenas de funcionários**, é possível e recomendável adotar **segmentação de acessos**: » Recursos humanos acessa apenas os dados trabalhistas e contratuais; » Financeiro acessa apenas os dados de pagamento e benefícios; » Setores de atendimento não têm acesso a essas pastas. Nesses casos, o princípio da transparência e da segurança (LGPD, art. 6º, VII) é atendido por meio de **controles de acesso**, com senhas, perfis de usuários, registro de logins e até **criptografia** para documentos sensíveis, limitando a exposição de dados pessoais ao mínimo necessário.

PRINCÍPIO	DEFINIÇÃO	EXEMPLOS
Prevenção (art. 6º, VIII)	O princípio da prevenção exige que as serventias adotem medidas para evitar violações de dados, ofensas aos direitos dos titulares e danos decorrentes do tratamento de dados.	O **princípio da prevenção** na LGPD impõe aos cartórios a adoção de medidas para evitar incidentes que possam violar dados pessoais ou causar danos aos titulares, de forma antecipada e proporcional ao porte da serventia. **Exemplo:** elaborar um **plano de continuidade de negócios** (Provimento 213/2026), instituir **política de segurança da informação**, manter equipe mínima de **profissionais de TI** conforme a norma, realizar treinamentos anuais, realizar **backup periódico do banco de dados** e **testar esses backups regularmente** para garantir sua efetividade.
Não Discriminação (art. 6º, IX)	O tratamento de dados pessoais não pode ser realizado para fins discriminatórios, ilícitos ou abusivos. Isso significa que nenhuma informação pessoal pode ser usada para restringir direitos de forma injustificada ou para prejudicar determinado grupo. Ressalte-se que a simples disponibilização de informação por meio de certidão não gera, por si só, tratamento discriminatório, ilícito ou abusivo.	Ao registrar filhos de casais homoafetivos, o cartório deve realizar o atendimento com respeito e igualdade. Dados sobre orientação sexual não podem ser tratados para diferenciação ou restrição de direitos. Ao realizar atendimento de um idoso com dificuldades de audição, o auxiliar do cartório precisa repetir várias vezes a mesma informação e explicar pausadamente os documentos que ele precisa trazer para realizar o ato desejado. Na LGPD, o **tratamento não discriminatório** significa que os dados pessoais não podem ser usados para fins discriminatórios, ilícitos ou abusivos (art. 6º, IX). Eis alguns exemplos práticos no contexto de cartórios: » **Discriminatório**: recusar ou dificultar o atendimento a uma pessoa porque ela possui nome social, orientação religiosa ou política diferente. O cartório deve atender a todos de forma igualitária, independentemente da informação que conste nos documentos. » **Ilícito**: utilizar dados coletados no registro de nascimento (como nome e endereço dos pais) para repassá-los a empresas privadas de planos de saúde ou fotografia. » **Abusivo**: manter um banco paralelo com telefones de usuários para enviar mensagens promocionais ou pessoais sem relação com a atividade registral.

PRINCÍPIO	DEFINIÇÃO	EXEMPLOS
Responsabilização e Prestação de Contas (art. 6º, X)	Este princípio determina que o responsável pela serventia esteja apto a demonstrar que adota medidas eficazes para assegurar o cumprimento da LGPD. O princípio da **responsabilização** impõe ao responsável pelo cartório o dever de responder por falhas no tratamento de dados, como a ausência de medidas mínimas de segurança que resulte em vazamento ou uso indevido de informações pessoais. Já o princípio da **prestação de contas** exige que a serventia demonstre, com evidências concretas e documentadas, que adota medidas eficazes e proporcionais de proteção de dados, conforme seu porte. A correição anual é o momento oportuno para garantir a prestação de contas, conforme previsão específica do art. 105 do CNN.	O cartório mantém registro de todas as operações de tratamento de dados realizadas, por meio de Inventário de Dados Pessoais atualizado anualmente (ou sempre que necessário). Em um cartório de pequeno porte, o servidor estava em área comum e um cliente conectou um pen drive infectado. O vírus facilitou o hackeamento e a extração de dados sensíveis. Essa situação demonstra a necessidade de restringir o acesso físico ao servidor, implementar bloqueio automático de portas USB e adotar rotinas preventivas, sob pena de responsabilização. O cartório realiza um **treinamento anual em LGPD e segurança da informação** com todos os colaboradores. Cada participante recebe um **certificado**, que é arquivado em pasta própria para comprovar a capacitação. Além disso, a serventia acompanha **indicadores de efetividade** das medidas técnicas e organizacionais, como a periodicidade e o sucesso dos **testes de *backup***, o controle de acessos aos sistemas e a aplicação da **política de segurança da informação**. Esses registros permitem demonstrar, em caso de fiscalização, que as práticas estão em conformidade com a LGPD e proporcionais ao porte da serventia. Em caso de fiscalização da ANPD ou das corregedorias, o cartório consegue demonstrar conformidade com a lei.

BASES LEGAIS

Como indicado anteriormente, todo tratamento de dados deve ser fundamentado por uma hipótese legal, dentre aquelas previstas no art. 7º e 11 da LGPD[12]. Cabe ressaltar, antes da apresentação das bases legais que fundamentam o tratamento de dados pessoais, que este Manual possui um caráter orientativo, e não normativo, para que os responsáveis pelas serventias extrajudiciais possam conhecer as melhores práticas segundo a LGPD e

12 Uma vez que este Manual tem como objetivo orientar o tratamento de dados em serventias extrajudiciais, não apresenta uma análise exaustiva do tema das bases legais, limitando-se a comentar aquelas que podem ser aplicadas no contexto dos cartórios. Assim, excluem-se deste documento as bases cuja aplicação exige agentes de tratamento de dados específicos, previstas no art. 7º, incisos IV e VIII, e no art. 11, inciso II, alíneas "c" e "f".

aplicá-las em suas atividades a depender de seu contexto de atuação e do seu respectivo programa de adequação.

No âmbito dos cartórios, a maior parte do tratamento de dados pessoais tem fundamento no cumprimento de obrigação legal ou regulatória, atraindo a incidência das hipóteses do art. 7º, II e do art. 11, II, "a" da LGPD. Reforça esse entendimento a previsão do art. 80 do CNN, a saber:

> Art. 80. O tratamento de dados pessoais destinado à prática dos atos inerentes ao exercício dos respectivos ofícios, consistentes no exercício de competências previstas em legislação específica, será promovido de forma a atender à finalidade da prestação do serviço, na persecução do interesse público, e com os objetivos de executar as competências legais e desempenhar atribuições legais e normativas dos serviços públicos delegados.

A partir do teor do dispositivo acima, o tratamento de dados destinado à prática dos atos inerentes ao exercício da atividade notarial e registral — tais como registro, inscrição, averbação, anotação, comunicação, emissão de certidão, dentre outros[13] — devem ser realizados a partir da legalidade. Isso indica que o tratamento de dados relacionado à prática de atos relacionados às atividades-fim e administrativas da serventia (prestação do serviço notarial e registral) se legitima pelo cumprimento de obrigação legal.

BASE LEGAL E PREVISÃO NA LGPD	EXEMPLOS
Obrigação legal ou regulatória (art. 7º, II e art. 11, II, "b")	» Registro de nascimento no Registro Civil. » Lavratura de escritura pública de compra e venda. » Comunicação obrigatória de atos à Receita Federal ou outros órgãos públicos e centrais eletrônicas. » Suscitação de dúvidas em relação a documentos.
Execução de contrato (arts. 7º, V, e art. 11, II, "d")	» O cartório, na pessoa do oficial, firma um contrato com uma operadora de saúde para oferecer cobertura aos seus funcionários. Para executar o contrato, é necessário tratar dados pessoais do oficial (como estipulante do plano) e dos colaboradores incluídos, tais como **nome, CPF, data de nascimento, estado civil, dependentes e dados de contato**.

13 Na falta de regulamento nacional sobre o tema, considera-se por sua didática, a disposição prevista nas Normas de Serviço dos Cartórios Extrajudiciais do Estado de São Paulo: "130.1 Consideram-se inerentes ao exercício dos ofícios os atos praticados nos livros mantidos por força de previsão nas legislações específicas, incluídos os atos de inscrição, transcrição, registro, averbação, anotação, escrituração de livros de notas, reconhecimento de firmas, autenticação de documentos; as comunicações para unidades distintas, visando as anotações nos livros e atos nelas mantidos; os atos praticados para a escrituração de livros previstos em normas administrativas; as informações e certidões; os atos de comunicação e informação para órgãos públicos e para centrais de serviços eletrônicos compartilhados que decorrerem de previsão legal ou normativa".

BASE LEGAL E PREVISÃO NA LGPD	EXEMPLOS
Exercício de direitos em juízo (arts. 7º, VI, e art. 11, II, "d")	» Dados de cidadãos, colaboradores e terceiros para defesa de direitos em processos judiciais, administrativos ou arbitrais. » Utilização de dados pessoais para instauração de processo administrativo de suscitação de dúvida a juízo competente.
Proteção da vida (art. 7º, VII, e art. 11, II, "e")	» Coleta de informações para acionar serviços de emergência para auxiliar em incidentes de saúde envolvendo colaboradores e cidadãos. » Repassar às autoridades competentes os dados pessoais da mulher atendida (cliente do cartório) e do seu agressor, sempre que houver manifestação do pedido de ajuda no âmbito do Programa Sinal Vermelho contra a Violência Doméstica, instituído pela Lei n. 14.188, de 28 de julho de 2021, e Recomendação n. 49/2022/CNJ.
Legítimo Interesse (art. 7º, IX)	» Coleta de cookies estritamente necessários no site e em aplicativos da serventia[14]. » Coleta de imagens por meio de câmeras de segurança[15].
Consentimento (art. 7º, I, e art. 11, II, "a")	» Uso de imagens de colaboradores para atividades não previstas em lei (ex.: premiações, campanhas, divulgação de atividades). » Uso de imagens de clientes para divulgação de atividades do cartório no site ou em redes sociais (ex.: fotografias de casamentos, campanhas de conscientização etc.). » Cartório solicita consentimento informado para cookies que não são estritamente necessários em seu site.

O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD[16], desde que observado e prevalecente o seu melhor interesse, a ser avaliado nos termos do art. 14 da LGPD e do Estatuto da Criança e do Adolescente.

No contexto das serventias extrajudiciais, esse cuidado se aplica especialmente aos atos que envolvem registros de nascimento, procurações, autorizações, testamentos, inventários, entre outros que envolvam diretamente menores de idade, tratados para a realização de registros civis, registros de nascimento, lavratura ou registro de escrituras envolvendo imóveis.

14 Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf.

15 A base legal para utilização de imagens de câmeras de segurança pode variar a depender da finalidade e contexto. É possível, por exemplo, que a coleta de imagens para proteção de arquivo cumpra com obrigação legal e regulatória, existindo outras bases legais aplicáveis.

16 Conforme Enunciado CD/ANPD n. 1/2023.

NORMAS APLICÁVEIS ÀS OPERAÇÕES DE TRATAMENTO REALIZADAS POR CARTÓRIOS

As atividades das serventias extrajudiciais são altamente reguladas, inclusive no que se refere à proteção de dados pessoais. A atuação dos cartórios deve harmonizar as obrigações legais impostas pela LGPD com os princípios da publicidade registral e demais normas administrativas que disciplinam sua atuação. Nesse sentido, esta seção objetiva listar as principais normas e fontes regulatórias que tratam do tema.

Como descrito até então, a principal norma que rege essa matéria é a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018 — LGPD). Essa lei estabelece princípios, obrigações e direitos relacionados ao uso de dados pessoais e se aplica também aos cartórios, que, ao prestarem serviços de natureza pública, tratam diariamente uma grande quantidade de informações identificáveis de pessoas naturais. A LGPD impõe às serventias o dever de garantir a segurança, a transparência e a limitação do uso dos dados, conforme sua finalidade legal e legítima.

Em complemento à LGPD, a Corregedoria Nacional de Justiça (CNJ), por meio do seu Código Nacional de Normas — Parte Geral do Foro Extrajudicial (CNN/CN/CNJ - Extra), publicado como Provimento n. 149 de 2023, regulamenta de forma mais específica a proteção de dados pessoais no âmbito dos cartórios. Os artigos 82 e 83 dessa norma são especialmente relevantes, pois estabelecem que os responsáveis pelas delegações, incluindo interventores e interinos, são os controladores dos dados pessoais tratados nas atividades típicas das serventias. A norma também define que empresas terceirizadas contratadas para tratar dados em nome do cartório, sem poder de decisão sobre sua finalidade, são consideradas operadoras, alinhando-se à definição da LGPD, além de outros conceitos e implicações que serão descritas neste Manual.

O Provimento n. 134, de 2022, editado pela Corregedoria Nacional de Justiça, atualmente incorporado ao CNN/CN/CNJ - Extra, reforça e atualiza as diretrizes relativas à proteção e ao tratamento de dados pessoais nas serventias extrajudiciais. Esse provimento dispõe sobre a adoção de políticas de governança e medidas de segurança da informação, alinhando as práticas dos cartórios às exigências da LGPD. Ele estabelece a necessidade de elaboração de um programa de proteção de dados pessoais que inclua avaliação de riscos, mapeamento dos fluxos de dados e capacitação dos servidores, visando garantir a conformidade com os princípios da transparência, finalidade e segurança.

O Provimento n. 134/2022 também detalha procedimentos para a correta guarda, armazenamento e descarte seguro dos dados pessoais e documentos eletrônicos e físicos, prevenindo o acesso não autorizado e a exposição indevida de informações. Além disso, traz orientações sobre a responsabilidade dos titulares das serventias quanto ao tratamento dos dados pessoais, reforçando o papel do controlador nos termos da LGPD e do Código Nacional de Normas. Essa norma demonstra o comprometimento da Corregedoria Nacional de Justiça em garantir que as serventias estejam preparadas para os desafios contemporâneos da proteção de dados, harmonizando a segurança jurídica com o direito à privacidade.

Outra norma essencial é o Provimento n. 213/2026 do CNJ[17], que dispõe sobre os padrões mínimos de tecnologia da informação e comunicação para garantir a segurança, a integridade, a disponibilidade, a autenticidade e a rastreabilidade, assegurando a continuidade das atividades dos serviços notariais e de registro do Brasil. Esse provimento exige que as serventias implementem estruturas tecnológicas mínimas e adotem boas práticas de segurança cibernética, como backups, criptografia, controle de acesso e auditoria de sistemas. Essas medidas estão diretamente relacionadas ao princípio da segurança previsto na LGPD, sendo fundamentais para a integridade dos dados tratados pelos cartórios.

Também merece destaque o Provimento n. 50/2015 do CNJ[18], que trata da tabela de temporalidade dos documentos físicos e eletrônicos mantidos pelas serventias. Essa tabela orienta o prazo de guarda e o descarte de documentos, servindo como base objetiva para cumprir os princípios da necessidade e da limitação da conservação de dados pessoais. Assim, documentos que não são mais necessários para fins legais ou de segurança jurídica devem ser descartados de forma segura, evitando acúmulo indevido de dados.

No que se refere ao registro de nascimento nas maternidades, o Provimento n. 13/2010 do CNJ[19] é outro instrumento normativo importante. Ele autoriza que o registro civil seja realizado diretamente nos hospitais, mediante integração eletrônica entre as maternidades e os cartórios. Essa prática envolve o tratamento e o compartilhamento de dados pessoais sensíveis, como os contidos na Declaração de Nascido Vivo, exigindo que tanto hospitais quanto serventias observem as diretrizes da LGPD quanto à base legal, finalidade e segurança do tratamento.

Além dessas normas nacionais, as serventias também devem observar atos normativos das corregedorias-gerais da Justiça dos estados, como provimentos, circulares e recomendações que detalham a aplicação da LGPD no âmbito local. Esses atos frequentemente adaptam as diretrizes nacionais à realidade regional e orientam sobre medidas

17 Disponível em: https://atos.cnj.jus.br/atos/detalhar/6734.
18 Disponível em: https://atos.cnj.jus.br/atos/detalhar/2512.
19 Disponível em: https://atos.cnj.jus.br/atos/detalhar/1298.

práticas de adequação à legislação de proteção de dados. Por fim, o CNJ tem emitido recomendações, notas técnicas e enunciados interpretativos que orientam os cartórios na harmonização entre os princípios registrais, como a publicidade e a autenticidade, e os princípios da LGPD, como a minimização e a confidencialidade. Essas orientações são essenciais para que as serventias possam desempenhar sua função pública com segurança jurídica e respeito à privacidade dos cidadãos.

Por fim, a Comissão de Proteção de Dados (CPF/CNJ) manifestou-se sobre a Lei de Acesso à Informação (Lei n. 12.527/2011 — LAI)[20] sob a ótica da Lei Geral de Proteção de Dados. A Diretriz n. 3/2023 da Comissão de Proteção de Dados destaca a compatibilização entre a Lei de Acesso à Informação (LAI) e a LGPD, especialmente no que se refere à divulgação de dados financeiros das serventias extrajudiciais.

A Diretriz orienta que, para garantir a transparência dos atos públicos sem comprometer a privacidade, é possível utilizar mecanismos de anonimização ou pseudonimização, de modo a proteger dados pessoais e sensíveis, como as informações sobre remuneração do responsável pela serventia. Essa abordagem assegura o cumprimento do princípio da publicidade, mantendo a conformidade com a LGPD e garantindo a proteção de dados pessoais enquanto se preserva o direito à informação pública.

20 Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

PRINCIPAIS OPERAÇÕES DE TRATAMENTO DE DADOS ENVOLVENDO CARTÓRIOS

No exercício das atividades de natureza registral e notarial, as serventias extrajudiciais cumprem demandas que resultam em diversas operações de tratamento de dados pessoais, conforme definido no art. 5º, X, da LGPD. Muitas dessas operações não são exclusivas de uma ou outra especialidade cartorária, mas comuns a todas as serventias, ainda que com variações quanto à natureza dos dados tratados ou ao contexto legal de sua utilização.

Entre as operações mais recorrentes, destaca-se a coleta de dados pessoais, realizada no momento em que o cidadão apresenta documentos e informações para a prática de um ato notarial ou registral. Esses dados incluem, por exemplo, nome completo, filiação, número de CPF e RG, estado civil, endereço, nacionalidade, profissão e outros elementos necessários à identificação das partes ou ao objeto do ato jurídico.[21]

Outra operação comum é a classificação e organização dos dados. Isso ocorre quando o cartório estrutura as informações recebidas em sistemas próprios, físicos ou digitais, muitas vezes de acordo com critérios técnicos ou legais, como numeração sequencial, temporalidade dos atos ou indexação por tipo de registro. A utilização, reprodução e armazenamento também são práticas universais.

O Provimento CNJ n. 149/2023 (CNN) dedica uma seção específica ao tema das certidões e do compartilhamento de dados, estabelecendo regras claras para a atuação dos notários e registradores. O art. 99 do referido Código impõe ao responsável pela serventia a obrigação de observar o conteúdo obrigatório das certidões conforme a legislação específica. O parágrafo único atribui ao responsável o dever de apurar a adequação, necessidade e proporcionalidade do conteúdo em relação à finalidade da certidão, especialmente quando o conteúdo não é explicitamente exigido ou é apenas autorizado pela lei. Essa disposição reflete o princípio da minimização de dados, fundamental na LGPD, garantindo que apenas as informações estritamente necessárias para a finalidade legítima sejam fornecidas.

No que tange ao compartilhamento de dados com as centrais de serviços eletrônicos, o art. 101 reconhece a compatibilidade dessa prática com a proteção de dados pessoais, desde que as centrais observem os princípios de adequação, necessidade e persecução

21 Provimento n. 61/2017/CNJ, art. 2º. Disponível em: atos.cnj.jus.br/atos/detalhar/2523.

da finalidade dos dados compartilhados, visando sempre a maior eficiência e conveniência dos serviços ao cidadão.

Quanto à organização das bases de dados entre a central de serviços eletrônicos compartilhados e as serventias, o parágrafo único desse artigo estabelece uma preferência clara pela modalidade de descentralização das bases de dados, incentivando o acesso pelas centrais às informações necessárias diretamente nas serventias, em detrimento da transferência de bases de dados completas. A transferência de bases de dados só seria justificável quando estritamente necessária para atingir a finalidade das centrais ou quando aspectos técnicos, como o volume de requisições, prejudicassem a eficiência do serviço prestado.

O compartilhamento de dados com órgãos públicos, que é tratado no art. 102 do CNN, pressupõe lei ou ato normativo do órgão solicitante, convênio ou outro instrumento formal com objeto compatível com as atribuições e competências legais da atividade notarial e registral. O CNN reitera a preferência pela modalidade de fornecimento de acesso a informações específicas adequadas, necessárias e proporcionais ao atendimento das finalidades presentes na política pública perseguida pelo órgão, observando-se os protocolos de segurança da informação e evitando-se a transferência de bancos de dados, a não ser quando estritamente necessária para a persecução do interesse público.

Caso o notário ou registrador entenda que a solicitação de compartilhamento por um órgão público é desproporcional, ele tem o dever de consultar a Corregedoria Nacional de Justiça no prazo de 24 horas, apresentando suas razões fundamentadas. Este dispositivo confere ao responsável pela serventia um papel ativo na salvaguarda dos dados, permitindo que conteste solicitações excessivas ou inadequadas.

As Diretrizes 1/2023, 2/2023 e 6/2024 da Comissão de Proteção de Dados do CNJ tratam do compartilhamento de dados notariais e registrais. A Diretriz 1/2023 (Processo 0005595-38.2022.2.00.0000) veda a transferência de bases de dados sem interesse público específico, permitindo apenas o compartilhamento por acesso. Já a Diretriz 2/2023 (Processos 006407/2023 e 0000272-86.2021.2.00.0000) admite a remessa de dados ao INSS como exceção legal, desde que limitada ao necessário e em conformidade com a LGPD. E, por fim, a Diretriz 6/2024 (Processos 005740/2024 e 0001707-61.2022.2.00.0000) define que a gestão do fornecimento de dados cabe exclusivamente aos notários e registradores, mediante convênios formais com entidades representativas, observando a legislação de proteção de dados.

Além das regras sobre as modalidades para o compartilhamento, o CNN também indica a adoção de medidas de segurança, como a criptografia e pseudonimização de dados, sempre que possível, aplicável e compatível com a finalidade perseguida e o tipo de

tratamento. Essas técnicas podem reduzir os riscos associados ao tratamento de dados, tornando-os menos identificáveis e, consequentemente, mais protegidos em caso de acesso não autorizado. Ainda, o CNN prevê a remessa de dados para a formação de indicadores estatísticos. Para essa finalidade específica, a norma exige que os dados sejam anonimizados na origem, nos termos da LGPD.

Por fim, a eliminação de dados também é uma operação importante, ainda que, em muitos casos, sujeita a limites legais. Documentos físicos digitalizados, cujos originais não precisam ser mantidos por exigência normativa, podem ser descartados de forma segura, conforme previsto em provimentos do CNJ, como o Provimento n. 50/2015.

Assim, é possível afirmar que, apesar das diferenças entre as serventias, todas as serventias realizam, com maior ou menor intensidade, operações de tratamento que envolvem coleta, registro, organização, utilização, compartilhamento, armazenamento e eliminação de dados pessoais, o que exige uma abordagem sistemática de adequação à LGPD e adoção de medidas contínuas de segurança, transparência e governança.

A partir das operações de tratamento comuns às serventias extrajudiciais, é possível traçar o seguinte ciclo de vida dos dados:

- **Passo 1 — Coleta dos dados:** a coleta ocorre no momento da solicitação de um serviço. Pode ser feita por meio de formulários físicos, documentos apresentados presencialmente ou plataformas digitais. Os dados coletados visam atender à exigência legal para a prática de ato jurídico (registro, autenticação, certidão etc.), por isso, os tipos de dados dependem do tipo de ato e da serventia, mas em geral incluem:
  - Dados pessoais comuns: nome completo, filiação, nacionalidade, estado civil, profissão, CPF, RG, endereço e e-mail.
  - Dados sensíveis (em casos específicos): religião (em casamento religioso com efeito civil), origem racial ou étnica, dados biométricos (em reconhecimentos por biometria), entre outros.
- **Passo 2 — Registro, classificação e organização**: após a coleta, os dados são registrados em sistemas internos, físicos ou eletrônicos. São organizados conforme o tipo de ato e o livro correspondente, e armazenados em bancos de dados indexados por chave de busca (como CPF ou nome). Esses dados são tratados para garantir a correta instrução do ato, permitir futura localização e emissão de certidões, cumprir obrigações legais de controle e publicidade registral.
- **Passo 3 — Utilização**: os dados são utilizados para fins específicos e determinados, como a lavratura de escrituras, registros e averbações, emissão de certidões, identificação das partes e autenticidade dos atos, ou a comunicação a órgãos públicos

ou centrais interligadas (CRC, SREI, ONR etc.). Esses dados são coletados para executar o serviço público delegado com observância da legalidade, segurança jurídica e publicidade.

- **Passo 4 — Compartilhamento**: dados pessoais podem ser compartilhados com terceiros, como nos casos em que essas informações são objeto de comunicação a órgãos públicos (como INSS, Receita Federal e Ministério Público), compartilhamento com centrais eletrônicas e sistemas oficiais (SREI, CRC Nacional, e-Notariado) ou mesmo atendimento a requisições judiciais ou legais. Esses dados são tratados para atender ao interesse público e à legalidade, garantir interoperabilidade de sistemas públicos e permitir o acesso a informações por direito.
- **Passo 5 — Armazenamento:** os dados são armazenados por prazos variáveis, conforme legislação específica e a tabela de temporalidade da Corregedoria Nacional de Justiça (Provimento n. 50/2015). Em muitos casos, os documentos têm guarda permanente (livros de registro) ou de longa duração (10, 20, 30 anos). Esses dados devem ser armazenados para assegurar a preservação da memória documental, garantir o acesso futuro a informações jurídicas e cumprir normas regulatórias.
- **Passo 6 — Eliminação ou descarte**: a eliminação deve seguir procedimentos que impeçam o acesso indevido (como fragmentação de papel ou limpeza digital certificada). Esse descarte ocorre para evitar acúmulo desnecessário de dados, reduzir riscos de violação de segurança e garantir o cumprimento do princípio da necessidade.

PRIORIDADES PARA ADEQUAÇÃO DOS CARTÓRIOS À LGPD

Para auxiliar nos processos de adequação das serventias à LGPD, este Manual apresenta um passo a passo a ser cumprido pelas serventias enquanto agentes de tratamento de dados pessoais. Esse passo a passo está alinhado ao art. 84 do CNN, que lista as principais linhas de ação para a estruturação do programa de governança:

> Art. 84. Na implementação dos procedimentos de tratamento de dados, o responsável pela serventia extrajudicial deverá verificar o porte da sua serventia e classificá-la, de acordo com o Capítulo I do Título I do Livro IV da Parte Geral deste Código Nacional de Normas, da Corregedoria Nacional de Justiça (Classe I, II ou III), e observadas as regulamentações da Autoridade Nacional de Proteção de Dados (ANPD), fazer a adequação à legislação de proteção de dados conforme o volume e a natureza dos dados tratados, de forma proporcional à sua capacidade econômica e financeira para aporte e custeio de medidas técnicas e organizacionais, adotar ao menos as seguintes providências:
>
> I — nomear encarregado pela proteção de dados;
>
> II — mapear as atividades de tratamento e realizar seu registro;
>
> III — elaborar relatório de impacto sobre suas atividades, na medida em que o risco das atividades o faça necessário;
>
> IV — adotar medidas de transparência aos usuários sobre o tratamento de dados pessoais;
>
> V — definir e implementar Política de Segurança da Informação;
>
> VI — definir e implementar Política Interna de Privacidade e Proteção de Dados;
>
> VII — criar procedimentos internos eficazes, gratuitos e de fácil acesso para atendimento aos direitos dos titulares;
>
> VIII — zelar para que terceiros contratados estejam em conformidade com a LGPD, questionando-os sobre sua adequação e revisando cláusulas de contratação para que incluam previsões sobre proteção de dados pessoais; e
>
> IX — treinar e capacitar os prepostos.

O presente item abordará as principais ações em forma de passo a passo simplificado a fim de instruir os agentes no processo de adequação à LGPD:

- **Prioridade 1: Elaborar o Registro de Operações de Tratamento (ROT)**[22]
  - Definir a metodologia para mapear e registrar as atividades de tratamento de dados pessoais efetuadas pela organização (como controladora e/ou operadora) e revisar periodicamente o ciclo de vida dos dados.

22 Cf.: ANPD divulga modelo de registro simplificado de operações com dados pessoais para Agentes de Tratamento de Pequeno Porte (ATPP) — Autoridade Nacional de Proteção de Dados. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-modelo-de-registro-simplificado-de-operacoes-com-dados-pessoais-para-agentes-de-tratamento-de-pequeno-porte-atpp.

- O CNN denomina esse registro de mapeamento das atividades de tratamento e seu produto é o "inventário de dados pessoais" (art. 85).

- **Prioridade 2**: **Identificar as bases legais mapeadas no ROT**
  - Identificar os indivíduos ou equipes que serão responsáveis por determinar as bases legais para o tratamento de dados pessoais — esses indivíduos deverão, como prioridade, definir em quais bases legais a organização se baseará.
  - Considerar quais processos devem ser implementados e/ou adaptados para a manutenção contínua das bases legais.

- **Prioridade 3: Indicar um encarregado**
  - Designar o encarregado, documentar e comunicar internamente seu papel e suas responsabilidades.
  - Identificar e envolver os principais agentes internos e líderes que estarão envolvidos no programa de governança de privacidade e proteção de dados pessoais e terão responsabilidade pela implementação do programa.
  - Identificar e envolver os principais agentes externos.

- **Prioridade 4: Identificar os papéis dos agentes envolvidos nos tratamentos mapeados no ROT**
  - Determinar o papel e as obrigações da organização como controladora ou operadora.
  - Comunicar essas obrigações aos indivíduos e às equipes relevantes dentro da organização.
  - Considerar atualizações necessárias aos contratos dos clientes para refletir o papel da organização.

- **Prioridade 5: Implementar uma política de governança e proteção de dados**
  - Implementar processo de avaliação de riscos aos indivíduos relacionados ao tratamento de dados pessoais.
  - Priorizar as medidas de conformidade relacionadas ao tratamento de dados pessoais que implicam maiores riscos para os indivíduos e para a organização.

- **Prioridade 6**: **Implementar processos para transparência e atendimento aos direitos dos titulares**
  - Preparar avisos de privacidade e outros recursos para fornecer informações facilmente acessíveis aos titulares de dados sobre o tratamento realizado pela organização.
  - Mapear os possíveis casos de exercícios de direitos pelos titulares relacionados aos seus dados pessoais, avaliar o tempo que a organização precisaria para responder e para desenvolver os processos relevantes.
  - Desenvolver processos para responder a tais solicitações.

- **Prioridade 7: Criar programas internos de treinamento e conscientização dos funcionários**
  - Implementar treinamento contínuo para todos os funcionários, incluindo os terceirizados e os recém-chegados.
  - Planejar atividades de treinamento e comunicação tanto no início do programa de governança de privacidade e proteção de dados pessoais quanto de forma contínua.

- **Prioridade 8**: **Definir medidas técnicas e administrativas para salvaguardar os dados pessoais tratados**
  - Trabalhar com as equipes de segurança da informação e de arquitetura de sistemas/dados para determinar as mudanças necessárias para implementar as medidas apropriadas de segurança.
  - Estabelecer um processo para a elaboração de relatórios internos, gerenciamento de incidentes de segurança, violações de dados pessoais e notificação da ANPD, se necessário.

- **Prioridade 9: Revisar contratos e gestão do relacionamento com terceiros**
  - Identificar os terceiros que realizam tratamento de dados pessoais em nome da organização e determinar se a organização trata dados pessoais em nome de terceiros.
  - Avaliar e adotar mecanismos de gerenciamento de terceiros, incluindo processos de due diligence e celebração de contratos relacionados ao tratamento de dados.

REGISTRO DE OPERAÇÕES DE TRATAMENTO

O ROT é uma das obrigações previstas na LGPD, especificamente no art. 37, em que é previsto que os agentes de tratamento devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. Esse registro é feito a partir de um mapeamento interno para que a serventia compreenda quando, para que finalidade e de que forma ela trata dados pessoais.

Segundo o art. 85 do CNN, o mapeamento de dados consiste na atividade de identificar o banco de dados da serventia, os dados pessoais objeto de tratamento e o seu ciclo de vida, incluindo todas as operações de tratamento a que estão sujeitos, como a coleta, o armazenamento, o compartilhamento, o descarte e quaisquer outras operações às quais os dados pessoais estejam sujeitos.

Para o mapeamento, recomenda-se três fontes de informação: (i) entrevistas com a equipe; (ii) questionários; e (iii) análise documental. Isso permite identificar as atividades de tratamento de dados pessoais sob diversos ângulos, que se complementam. Com isso, é possível registrar o fluxo de utilização dos dados pessoais nos processos do cartório (mapeamento de dados, ou data mapping), bem como os riscos a que estão sujeitas as atividades de tratamento (mapeamento de riscos ou *gap analysis*).

O resultado da atividade de mapeamento é a confecção de um documento chamado Inventário de Dados Pessoais (IDP). Ele deverá conter, no mínimo:

- finalidade do tratamento;
- categorias de dados pessoais e descrição dos dados utilizados nas respectivas atividades;
- identificação das formas de obtenção/coleta dos dados pessoais;
- base legal;
- descrição da categoria dos titulares;
- se há compartilhamento de dados com terceiros, identificando eventual transferência internacional;
- categorias de destinatários, se houver;
- prazo de conservação dos dados; e
- medidas de segurança organizacionais e técnicas adotadas.

O inventário de dados deve ser atualizado regularmente, no máximo a cada um ano, arquivado na serventia e disponibilizado caso seja solicitado pela Corregedoria-Geral da Justiça (CGJ), ANPD ou outro órgão de controle. Além disso, o responsável pela serventia pode utilizar ferramentas informatizadas e formulários personalizados para registrar e monitorar o fluxo dos dados pessoais em todas as fases do tratamento, desde a coleta até o armazenamento, compartilhamento e descarte. Essas soluções podem ser desenvolvidas ou fornecidas por associações de classe de notários e registradores para facilitar a gestão da conformidade.

A partir desse *gap analysis*, é possível elaborar um plano de ação que inclua a implementação de novos processos, procedimentos e controles, além da revisão e criação de documentos e formas eficazes de comunicação com os titulares, a ANPD e as corregedorias. Para garantir conformidade, a serventia deve realizar um gap assessment, avaliando vulnerabilidades no tratamento de dados pessoais e identificando lacunas que necessitam de ajustes. Com base nessa análise, serão tomadas decisões para corrigir as fragilidades e implementar adequações compatíveis com as exigências legais.

IDENTIFICAÇÃO DAS BASES LEGAIS

A escolha da base legal adequada é uma das etapas mais fundamentais para a conformidade dos cartórios com a LGPD. Esse processo deve ser conduzido com atenção e rigor técnico, pois a base legal não é uma escolha discricionária do controlador, e por não haver distinção hierárquica entre as bases legais. Em outras palavras, o cartório não pode simplesmente optar pela base que lhe parecer mais conveniente, ela deve refletir, com precisão, a natureza, o contexto e a finalidade do tratamento de dados realizado.

Após o mapeamento das operações de tratamento, o cartório deve avaliar qual é a finalidade real do tratamento. Se o tratamento de dados decorre de uma imposição normativa, como ocorre, por exemplo, nos registros civis de nascimento ou óbito, nos registros imobiliários ou nos protestos de títulos, a base legal será o cumprimento de obrigação legal ou regulatória.

A identificação correta da base legal é essencial porque ela define não apenas a legalidade do tratamento, mas também os direitos dos titulares e os deveres do controlador. Por exemplo, tratamentos baseados no consentimento permitem que o titular revogue sua autorização a qualquer momento, enquanto tratamentos fundamentados em obrigação legal não oferecem essa possibilidade.

Além disso, a base legal influencia diretamente na forma como o cartório deve comunicar o tratamento ao titular, seja no balcão de atendimento, seja em sua política de privacidade. A escolha da base legal correta também tem implicações diretas na relação do cartó-

rio com terceiros, como prestadores de serviços de tecnologia e operadores externos. Os contratos firmados devem estar alinhados com a base legal identificada para cada operação, a fim de garantir coerência e segurança nas responsabilidades atribuídas e nas medidas de proteção exigidas. Isso é especialmente relevante em um setor como o das serventias extrajudiciais, que opera sob delegação do poder público e está sujeito à fiscalização da ANPD.

Portanto, o cartório deve adotar uma abordagem criteriosa e técnica, documentando de forma clara e transparente a base legal aplicável a cada operação de tratamento. Recomenda-se que, sempre que possível, se identifique uma única base principal por operação, evitando sobreposições que possam gerar insegurança jurídica ou dificultar a resposta aos direitos dos titulares. Esse cuidado contribui para a prestação de serviços com segurança jurídica, eficiência e respeito à privacidade das pessoas, fundamentos centrais tanto da LGPD quanto da atividade notarial e registral.

INDICAÇÃO DE UM ENCARREGADO

Segundo o art. 88 do CNN, as serventias extrajudiciais devem designar um encarregado pelo tratamento de dados pessoais, conforme previsto no art. 41 da LGPD. A nomeação do encarregado não se confunde com a função do responsável pela delegação dos serviços extrajudiciais e deve ser formalizada por meio de contrato, arquivado em registro próprio.

A atuação do encarregado foi regulamentada pela Resolução CD/ANPD n. 18, de 16 de julho de 2024[23], que traz as características e obrigações do encarregado. Esse profissional pode ser terceirizado, contratado como pessoa física ou jurídica, desde que tenha capacitação adequada para a função. A escolha do encarregado é livre, cabendo ao responsável pela serventia estabelecer as qualificações profissionais necessárias para o desempenho das atribuições do encarregado, considerando seus conhecimentos sobre a legislação de proteção de dados pessoais, bem como o contexto, o volume e o risco das operações de tratamento realizadas, de acordo com o art. 7º da Resolução em questão.

Mesmo com a nomeação do encarregado, o responsável pela serventia continua obrigado a atender às solicitações dos titulares dos dados pessoais. Serventias classificadas como Classe I e Classe II podem compartilhar um encarregado, permitindo uma gestão conjunta da proteção de dados. A escolha do encarregado é de livre decisão do titular da serventia, podendo ser feita individualmente, coletivamente ou até subsidiada por entidades de classe.

23 Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074.

É muito comum que as serventias indiquem escreventes ou substitutos como encarregados de dados. Igualmente comum é a indicação de empresas que fornecem serviços de tecnologia. Tais práticas são aceitas pela legislação, mas é preciso garantir que esses profissionais exercerão suas funções com independência e eficácia.

Além disso, não há impedimento para que um mesmo profissional atue como encarregado em múltiplas serventias, desde que não haja conflito de interesses e que a qualidade dos serviços prestados seja garantida. É importante que se demonstre a inexistência de conflito na cumulação de funções e a manutenção da qualidade dos serviços prestados. As serventias têm flexibilidade para garantir a conformidade com a LGPD, adaptando-se às suas necessidades operacionais e estruturais.

Nesse sentido, o responsável pela serventia deve atentar para que o encarregado não exerça atribuições que acarretem conflito de interesse[24]. De acordo com o art. 2º, II, da Resolução CD/ANPD n. 18, conflito de interesse ocorre quando há situação que possa comprometer, influenciar ou afetar, de maneira imprópria, a objetividade e o julgamento técnico no desempenho das atribuições do encarregado.

Constatada a situação de conflito de interesses[25], o agente deve adotar providências cabíveis para solucionar a questão, como não indicar a pessoa para exercer a função de encarregado, implementar medidas para afastar o risco de conflito de interesse, ou substituir a pessoa designada para exercer a função de encarregado, sob pena de responsabilização, segundo o art. 21, da Resolução em questão.

Além disso, o responsável pela serventia deve prover os meios necessários para o exercício das atribuições do encarregado, tais como recursos humanos, técnicos e administrativos. Ainda que a disponibilidade desses recursos dependa da capacidade econômica da serventia, deve-se garantir um mínimo necessário para que o encarregado possa exercer sua atividade.

Um encarregado interno que atue sob regime celetista, por exemplo, precisa ter ao menos algumas horas de sua jornada semanal reservadas para atuar com demandas relativas à proteção de dados pessoais. Esse período deve ser suficiente para que o colaborador estude o tema, prepare e ministre treinamentos, redija documentações pertinentes e atenda eventuais demandas dos titulares de dados e das corregedorias.

24 Com efeito, o CNN exige que seja "demonstrável a inexistência de conflito na cumulação de funções e a manutenção da qualidade dos serviços prestados" (art. 88, § 3º).

25 Por exemplo, se há nomeação de um escrevente da própria serventia como encarregado de dados ou a contratação de advogado como encarregado que defenda o oficial da serventia como réu em processos.

De acordo com a Resolução CD/ANPD n. 18, bem como o art. 23, III, e art. 41, da LGPD, são atribuições do encarregado:

- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências cabíveis;
- receber comunicações da ANPD e adotar providências;
- orientar os funcionários e os contratados do agente de tratamento a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- executar as demais atribuições determinadas pelo agente de tratamento ou estabelecidas em normas complementares.

Além de atuar como ponto de contato entre o controlador, os titulares de dados e a ANPD, o encarregado deve promover ações de conscientização sobre a proteção de dados pessoais, conforme previsto no art. 94, IV, CNN. Também é sua responsabilidade participar dos treinamentos regulares organizados pela serventia, nos termos do art. 94, inciso V, e dar ciência no relatório de avaliação dos sistemas e bancos de dados utilizados no tratamento de dados pessoais e sensíveis, nos termos do art. 90, inciso II do mesmo provimento.

IDENTIFICAÇÃO DOS PAPÉIS DOS AGENTES DE TRATAMENTO

Para que os dados pessoais sejam tratados, é comum que vários agentes, sejam eles controladores ou operadores, atuem nesse processo. A identificação de todos eles é fundamental para a definição do grau de responsabilidade de cada um dos agentes que compõe a cadeia de tratamento dos dados pessoais.

É necessário ressaltar que a identificação precisa dos papéis de controlador e operador no tratamento de dados pessoais depende da análise do contexto fático dos processos das atividades desempenhadas. Embora os contratos firmados entre o cartório e prestadores de serviços e outras entidades possam indicar quem exerce qual função no tratamento de dados, é a realidade prática das atividades, e não apenas o que está formalmente previsto no contrato, que definirá a efetiva responsabilidade de cada agente de tratamento, especialmente em eventual apuração pela ANPD ou por órgãos correicionais.

De acordo com diretrizes internacionais, como as emitidas pelo European Data Protection Board (EDPB), e nacionais, como o Guia de Agentes de Tratamento da ANPD, os contratos são instrumentos relevantes para equilibrar as posições jurídicas entre as partes e garantir a conformidade com a LGPD.[26] Essa questão afeta, sobretudo, o campo das ser-

26 Disponível em: https://www.edpb.europa.eu/system/files_en?file=2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf.

ventias extrajudiciais, onde pode haver assimetria de informações entre os delegatários e os prestadores de serviços especializados em tecnologia, digitalização, segurança da informação e armazenamento de dados.

No contexto cartorário, os contratos firmados devem ir além da mera transcrição dos dispositivos legais, contemplando cláusulas específicas que estabeleçam as responsabilidades de cada parte, o nível de segurança exigido no tratamento de dados, obrigações de confidencialidade e previsões sobre riscos operacionais e jurídicos associados à natureza dos dados tratados. A revisão contratual será abordada nas seções seguintes e essa revisão deve ser feita com base na identificação dos agentes de tratamento envolvidos em cada uma das atividades de tratamento de dados pessoais.

Adicionalmente, é possível que duas ou mais entidades envolvidas no ecossistema de registros públicos, como cartórios, centrais eletrônicas ou entes públicos conveniados, compartilhem dados pessoais com finalidades legítimas e complementares. Nesses casos, pode haver configuração de controladores autônomos ou, em situações específicas, de cocontroladores, a depender da existência de decisões comuns ou convergentes sobre as finalidades e os meios do tratamento.[27]

Instrumentos contratuais ou convênios podem ser utilizados para delimitar as esferas de decisão e responsabilidade de cada parte, inclusive prevendo mecanismos de cooperação e resposta conjunta a incidentes de segurança ou requisições dos titulares. Assim, ainda que a LGPD não exija expressamente que os controladores e operadores celebrem contrato específico, tal formalização é altamente recomendável e se enquadra como boa prática de governança de dados para as serventias extrajudiciais.

Conforme aponta a ANPD,[28] esse tipo de contrato permite impor limites à atuação do operador, definir parâmetros objetivos para a responsabilidade de cada parte e mitigar os riscos regulatórios e operacionais. No contexto dos cartórios, os contratos devem prever, de forma clara e transparente, o objeto do tratamento, sua duração, finalidade, a natureza dos dados tratados, os tipos de dados pessoais envolvidos e as obrigações específicas de ambas as partes quanto ao cumprimento da LGPD.

27 Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf.

28 Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf.

IMPLEMENTAR UMA POLÍTICA DE GOVERNANÇA E PROTEÇÃO DE DADOS

A LGPD estabelece, no artigo 50, que os agentes de tratamento, entre eles os cartórios, na condição de controladores, devem adotar medidas de governança para demonstrar o compromisso com a proteção de dados pessoais. Essas medidas incluem boas práticas, procedimentos internos de segurança da informação, mitigação de riscos e responsabilização de todos os envolvidos no tratamento.

O tratamento de dados pessoais é central para praticamente todas as atividades cartorárias, desde registros civis de nascimento até escrituras públicas, registros imobiliários e protestos. Em razão da natureza de muitas dessas informações e do dever legal de manter a integridade, autenticidade e segurança dos atos praticados, é essencial que haja normas internas claras, atualizadas e eficazes sobre o tratamento de dados.

Uma política de governança bem estruturada permite ao cartório mapear e documentar suas operações de tratamento, estabelecer responsabilidades internas, definir medidas técnicas e administrativas de segurança, criar procedimentos para resposta a incidentes, garantir transparência aos titulares e preparar a equipe para lidar com os direitos previstos na LGPD, como acesso, retificação ou eliminação. Além disso, facilita o atendimento às fiscalizações, inclusive da ANPD.

Essa política deve funcionar como um instrumento formal que norteia a conduta da serventia em relação ao tratamento de dados pessoais, desde a coleta até o descarte, promovendo uma cultura de responsabilidade, segurança e transparência. Dessa forma, a política deve iniciar com a definição clara de seu objetivo, que é estabelecer diretrizes internas para garantir que todas as operações de tratamento de dados pessoais estejam alinhadas aos princípios e regras da LGPD.

Em seguida, deve ser delimitado o âmbito de aplicação da política, ou seja, quem está sujeito às suas normas, o que inclui o titular da delegação, substitutos, escreventes, atendentes, estagiários e eventuais operadores externos contratados. É recomendável que a política apresente, em linguagem clara, os conceitos fundamentais da LGPD, como dado pessoal, dado sensível, titular, controlador, operador, tratamento e anonimização, contextualizando-os à realidade dos cartórios. Também deve explicitar o compromisso da serventia com os princípios da proteção de dados, como a finalidade, adequação, necessidade, livre acesso, segurança, prevenção, transparência, responsabilização e boa-fé.

A política deve identificar os papéis e responsabilidades dos agentes de tratamento, destacando que o responsável pela delegação atua como controlador e que operadores podem ser contratados, por exemplo, para digitalização de acervos ou gestão de sistemas, deven-

do sempre atuar sob orientação do controlador. O encarregado, se designado, também deve ter sua função claramente definida.

Outro ponto fundamental é a previsão da obrigatoriedade de manter um registro ou inventário das atividades de tratamento, o que inclui a descrição dos tipos de dados tratados, suas finalidades, bases legais, prazos de retenção, medidas de segurança e eventuais compartilhamentos. A política também deve detalhar as bases legais aplicáveis aos tratamentos realizados, principalmente o cumprimento de obrigação legal ou regulatória e a execução de contrato, orientando a escolha adequada com base na finalidade da atividade.

Além disso, é essencial contemplar os direitos dos titulares de dados (como acesso, retificação, eliminação, oposição ao tratamento etc.) e os procedimentos para seu atendimento. Deve-se indicar os canais apropriados, prazos de resposta e responsáveis internos por esse atendimento. A política também deve disciplinar o compartilhamento de dados pessoais e impor critérios claros para o envio ou recebimento de informações entre controladores ou operadores.

As medidas de segurança da informação devem ser tratadas com destaque, prevendo procedimentos técnicos e administrativos para mitigar riscos, como controle de acesso, uso de senhas, backup de dados e descarte seguro de documentos. É igualmente importante que a política inclua diretrizes para capacitação e treinamento contínuo da equipe sobre proteção de dados e segurança da informação, pois a conscientização dos prepostos é um elemento essencial da governança. A política também deve prever um plano de resposta a incidentes, com medidas para notificação à ANPD, comunicação aos titulares afetados e procedimentos internos de contenção e apuração.

Por fim, a política deve estabelecer regras sobre sua revisão periódica e atualização, considerando mudanças legislativas, normativas ou organizacionais, assegurando que permaneça atual, eficaz e coerente com as práticas da serventia. Ainda, a política deve ter seu desempenho verificado pelos responsáveis por sua implementação, com indicadores de conformidade e planos de ação para correções de inconformidade.

IMPLEMENTAR PROCESSOS PARA TRANSPARÊNCIA E ATENDIMENTO AOS DIREITOS DOS TITULARES

O princípio da transparência está previsto no art. 6º, VI, da LGPD. Esse princípio influencia as determinações da Lei em diversos momentos, ela possui várias disposições que determinam como os agentes de tratamentos deverão implementar esse princípio na prática, como o art. 9º, que determina obrigações de informação sobre o tratamento, assim como mecanismos para a observância de direitos dos titulares, previstos no art. 18 da Lei.

O CNN prevê a implementação dessas medidas nos artigos 95 a 98, determinando que as serventias devem garantir transparência e acesso facilitado às informações sobre o tratamento de dados pessoais, respeitando os direitos dos titulares.

Assim, cabe ao responsável pela serventia, na qualidade de controlador, elaborar, por meio do canal do próprio encarregado, se terceirizado, e/ou em parceria com as respectivas entidades de classe:

- canal eletrônico específico para atendimento das requisições e/ou reclamações apresentadas pelos titulares dos dados pessoais; e
- fluxo para atendimento aos direitos dos titulares de dados pessoais, requisições e/ou reclamações apresentadas, desde o seu ingresso até o fornecimento da resposta.

As seguintes informações deverão ser divulgadas em local de fácil visualização e consulta pelo público:

- as informações básicas a respeito dos dados pessoais e dos procedimentos de tratamento;
- os direitos dos titulares dos dados;
- o canal de atendimento disponibilizado aos titulares de dados para que exerçam seus direitos; e
- os dados de qualificação do encarregado, com nome, endereço e meios de contato.

Essas informações podem ser divulgadas por meio de aviso de privacidade e proteção de dados físicos, afixado próximo ao balcão de atendimento. Além disso, se a serventia utilizar website, pode se valer de ferramentas diversas, como banner de cookies, aviso de privacidade e aviso de navegação.

Para garantir a segurança das informações, o notário ou registrador deve identificar corretamente o solicitante, evitando acessos indevidos e protegendo a confidencialidade dos dados. Portanto, a confirmação da identidade do solicitante deve sempre fazer parte do fluxo de atendimento aos direitos dos titulares de dados.

Ainda, não se pode confundir o direito de livre acesso gratuito com a publicidade notarial e registral, que somente se opera por busca ou certidão[29].

29 Por exemplo, se a proprietária deseja saber se seu nome consta na matrícula do imóvel na qualidade do estado civil de solteira ou casada, deverá solicitar certidão e não o atendimento disponibilizado pelo canal de LGPD do encarregado. A proprietária pode, de forma gratuita, solicitar a alteração de seu telefone nos cadastros internos do cartório sem que seja necessário praticar qualquer ato ou cobrança no cartório.

CRIAR PROGRAMAS INTERNOS DE TREINAMENTO E CONSCIENTIZAÇÃO DOS FUNCIONÁRIOS

Sem previsão expressa na LGPD, mas como parte essencial da estruturação de um programa de governança em privacidade, o art. 94 do CNN estabelece que as serventias extrajudiciais devem adotar medidas organizacionais compatíveis com o porte da unidade e com a natureza das atividades realizadas, incluindo ações de capacitação dos colaboradores e do encarregado pelo tratamento de dados pessoais. Vale acrescentar ainda que os treinamentos devem ser realizados, no mínimo, uma vez por ano.

Em cumprimento a essa norma, as serventias devem promover treinamentos regulares e contínuos com o objetivo de fortalecer a cultura institucional de proteção de dados, garantindo que todos os envolvidos compreendam os procedimentos e os controles necessários para o tratamento adequado das informações. Isso inclui a capacitação geral de todos os trabalhadores, bem como ações específicas para novos colaboradores.

Além disso, os treinamentos devem ser atualizados periodicamente, de modo a refletir novas exigências normativas, mudanças tecnológicas ou reestruturações internas. O encarregado de dados deve atuar de forma proativa na promoção de programas de sensibilização, capacitação e orientação de todos os envolvidos nas rotinas de tratamento de dados da serventia.

A serventia deve manter registro da participação dos colaboradores em cursos, conferências e seminários, documentando os conteúdos abordados e os responsáveis pela capacitação. Essa prática contribui para a rastreabilidade das ações de governança e demonstra o esforço institucional para a conformidade com a LGPD.

Adicionalmente, o responsável pela serventia pode solicitar apoio às entidades de classe para viabilizar treinamentos que contemplem as especificidades do serviço extrajudicial, reforçando o comprometimento com a transparência, segurança e responsabilidade no tratamento de dados pessoais.

DEFINIÇÃO DE MEDIDAS TÉCNICAS E ADMINISTRATIVAS PARA SALVAGUARDAR OS DADOS PESSOAIS TRATADOS

Assim como os art. 46 a 49 da LGPD estabelecem previsões de segurança mínimas para os agentes de tratamento, os artigos 90 a 93 do CNN detalham como tais obrigações devem ser observadas no âmbito das serventias extrajudiciais.

Na qualidade de controlador, o responsável pela serventia deve implementar medidas técnicas e administrativas capazes de proteger os dados pessoais contra acessos não au-

torizados, destruição, perda, alteração ou qualquer forma de tratamento inadequado. Para isso, as serventias devem implementar as medidas previstas no Provimento n. 213/2026 do CNJ, além de avaliar periodicamente os sistemas e bancos de dados utilizados, garantindo a segurança das integrações e do compartilhamento de dados com terceiros.

Através de diretrizes e normas, a Política de Segurança da Informação (PSI) permite controlar mais efetivamente as medidas de segurança implementadas. Isso porque uma política formal tem um papel fundamental em direcionar os recursos adequados para as necessidades de segurança da serventia.

A PSI visa minimizar o impacto e a probabilidade de incidentes de segurança, sabendo que esse é um risco intrínseco ao tratamento de dados pessoais. Esses incidentes geralmente se relacionam aos seguintes fatores: (i) falhas técnicas de equipamentos ou aplicações de tecnologia, tais como sistemas administrativos; (ii) conduta errônea do profissional responsável pelo uso e manutenção dos ativos; (iii) invasões por atores externos que promovem ataques mal-intencionados com o objetivo de roubar, sequestrar ou destruir dados[30].

Nesse sentido, o Plano de Resposta a Incidentes, documento que integra o PSI e regulado pelo art. 91 do CNN, tem como objetivo orientar os processos de detecção e resposta de incidentes de segurança, permitindo que todos os incidentes sejam documentados, analisados e resolvidos de forma estruturada. Com isso, é possível minimizar os impactos do incidente aos direitos dos titulares, além de investigar e compreender as causas do incidente, a fim de aprimorar as medidas preventivas.

Outro aspecto importante do Plano é orientar as comunicações necessárias. Em caso de incidentes de segurança envolvendo dados pessoais que possam acarretar risco ou dano relevante aos titulares, o responsável deve comunicar aos titulares afetados, à ANPD, ao juiz corregedor permanente e à Corregedoria-Geral da Justiça (CGJ) no prazo máximo de 48 horas, esclarecendo a natureza do incidente e as medidas adotadas para mitigação dos impactos.

A eliminação e inutilização de documentos deve ser realizada conforme a Tabela de Temporalidade de Documentos, prevista na Seção I do Capítulo I do Título II do Livro III da Parte Geral do Código, garantindo que os dados pessoais não possam ser identificados. A descaracterização dos dados deve garantir que a identificação dos titulares seja tecnicamente inviável. Ainda, de acordo com o Provimento 50/2015/CNJ, sempre que possível, os documentos físicos devem ser digitalizados e armazenados em locais seguros, com

30 A PSI e o PCN mencionam ainda Eventos Disruptivos, Criticidade dos Eventos Disruptivos, Identificação das Consequências e Riscos dos Eventos Disruptivos, Avaliação do Grau de Risco dos Eventos Disruptivos e o respectivo Plano de Ação.

controle de acesso, sendo permitida a eliminação física após a digitalização, respeitados os prazos legais.

REVISÃO DE CONTRATOS E GESTÃO DO RELACIONAMENTO COM TERCEIROS

As serventias extrajudiciais devem revisar e adequar todos os contratos que envolvam o tratamento de dados pessoais para garantir conformidade com a LGPD, de acordo com o art. 86 do CNN. Isso inclui a responsabilização dos agentes de tratamento, devendo ser observados os seguintes procedimentos:

- **Contratos trabalhistas**: revisão dos contratos dos empregados, assegurando a obrigatoriedade do respeito às normas de proteção de dados.
- **Minutas e convênios**: atualização dos modelos contratuais que envolvem o compartilhamento de dados pessoais.
- **Termos de Tratamento de Dados**: elaboração de documentos formais para operadores de dados, especificando os dados tratados, os titulares, as finalidades e os limites do tratamento.
- **Descarte de dados**: inclusão de cláusulas contratuais prevendo a eliminação de dados pessoais quando não forem mais necessários para a finalidade estipulada. Essa cláusula é especialmente importante no contrato com fornecedores de armazenamento, que podem ter acesso a grande volume de dados tratados pela serventia.
- **Contratações futuras**: criação de diretrizes para que novos contratos já estejam adequados à LGPD.
- **Auditorias regulares**: implementação de mecanismos de fiscalização sobre terceiros que compartilhem dados pessoais com a serventia.

A revisão dos contratos[31] deve incluir cláusulas que obriguem os empregados a respeitar integralmente as normas de privacidade e proteção de dados, bem como a desempenhar suas atividades em conformidade com as orientações do responsável pela serventia, adotando as medidas necessárias para prevenir qualquer violação de dados pessoais.

Por outro lado, é necessário revisar as minutas de contratos e convênios externos que envolvam o tratamento de dados pessoais. Na prática, a adequação contratual é a inclusão de cláusulas sobre proteção de dados nos instrumentos jurídicos da serventia. Para todos os contratos externos, o conteúdo mínimo deve abranger:

31 Essa adequação estende-se a todos os demais instrumentos de normatização internos, tais como código de ética, manuais de conduta, procedimentos operacionais, dentre outros.

- delimitação dos dados tratados, a finalidade do tratamento e a base legal que o autoriza ou referência às políticas onde o tema foi abordado;
- duração do tratamento e o dever de eliminação de dados (descarte);
- deveres de confidencialidade e requisitos mínimos de segurança da informação exigidos;
- autorização (ou não) para a contratação de suboperadores;
- dever de comunicação de incidente de segurança;
- dever de cooperação para atendimento de solicitações dos titulares de dados e de órgãos fiscalizadores (corregedorias e ANPD); e
- delimitações de responsabilidade civil e administrativa (e trabalhista, se for o caso).

Embora seja o mais comum, a adequação contratual não necessariamente precisa ser feita por meio de aditivos. Com efeito, a serventia pode se valer de instrumentos autônomos, os chamados Termos de Tratamento de Dados Pessoais para assinatura com os operadores. Os termos, que podem ser tanto documentos impressos, quanto eletrônicos, devem possuir um conteúdo similar ao aditivo, com as devidas adaptações de um instrumento autônomo.

De igual modo, é preciso exigir conformidade das pessoas naturais ou jurídicas que tratam dados dos cartórios de maneira externa. Esses destinatários de dados são denominados "terceiros". O art. 84, VIII, do CNN prescreve que a serventia deve "zelar para que terceiros contratados estejam em conformidade com a LGPD", fazendo isso de duas formas diferentes: (i) revisando cláusulas de contratação (adequação contratual) e (ii) questionando-os sobre sua adequação (gestão de terceiros).

A gestão de terceiros envolve a criação de procedimentos internos para governança de dados, cujo conteúdo deve ser definido pelo responsável da serventia, de acordo com riscos mapeados. Em caráter mínimo, o CNN exige que orientações e procedimentos sejam elaborados para as contratações futuras, além de atividades periódicas de auditoria.

A auditoria é a verificação do cumprimento das normas de privacidade e proteção de dados pelos terceiros que tratam os dados pessoais da serventia ou em seu nome. Uma das formas mais básicas de auditoria é a solicitação de evidências de adequação, que vão além da simples declaração formal de estar adequado. Isso significa pedir que o fornecedor envie provas concretas da realização da implementação, tais como certificados de treinamento, cópias de políticas internas, cópia de aditivos contratuais assinados com colaboradores e fornecedores etc.

Por fim, fornecedores de tecnologia, automação e armazenamento deverão comprovar a adequação dos sistemas e programas internos de gestão de dados às exigências da LGPD, garantindo segurança e conformidade.

É nesse sentido que o art. 87 do CNN afirma que os responsáveis pelas serventias extrajudiciais deverão exigir de seus fornecedores de tecnologia, de automação e de armazenamento a adequação às exigências da LGPD quanto aos sistemas e programas de gestão de dados internos utilizados. Logo, o contrato sobre o tratamento de dados realizado por tais empresas deve ser firmado com atenção aos riscos envolvidos.

DIRETRIZES ESPECÍFICAS APLICÁVEIS AOS CARTÓRIOS

As serventias extrajudiciais possuem especificidades próprias que impactam a relação entre suas atividades e a proteção de dados pessoais. Assim, este tópico apresenta diretrizes específicas para cada especialidade, conforme o Código Nacional de Normas da Corregedoria Nacional de Justiça (CNN/CNJ), observando suas peculiaridades no tratamento de dados.

TABELIONATO DE NOTAS

A Seção XI do CNN detalha a harmonização das atividades dos Tabelionatos de Notas com a proteção de dados pessoais. Dentre as recomendações específicas por tipo de documento estão:

- **Emissão de certidões de ficha de firma e documentos depositados**: ocorre apenas mediante solicitação do titular, representantes legais, mandatários com poderes específicos ou decisão judicial.
- O provimento fixa que o fornecimento de certidões para os solicitantes legitimados pode ocorrer por meio de cópia reprográfica.
- **Ata notarial para menores de 12 anos:** o pedido de lavratura de ata notarial realizado por um dos pais ou pelo responsável legal envolvendo dados de menor de 12 anos é considerado consentimento específico e em destaque para tratamento de dados da criança. Ressalte-se que se o responsável legal pretender retirar o consentimento em momento posterior, os dados não poderão ser eliminados de livros e arquivos, conforme o art. 16, da LGPD.
- **Condição de pessoa politicamente exposta:** não haverá necessidade de inserção da condição de pessoa exposta politicamente nos atos protocolares e nas escrituras públicas.
- **Certidão de testamento:** a certidão será fornecida ao testador ou por ordem judicial, sendo que, após o falecimento, a certidão poderá ser fornecida a terceiros com certidão de óbito.
- **Qualificação das partes em atos notariais:** o ato notarial deve incluir (i) nome completo, (ii) CPF, (iii) documento de identificação ou, na sua falta, a filiação, (iv) nacionalidade, (v) estado civil, (vi) existência de união estável, (vii) profissão e (viii) domicílio. Não é necessário incluir endereço eletrônico ou telefone.

Nessa especialidade, a Comissão de Proteção de Dados (CPD/CN) publicou a Diretriz 5/2023 (CPD/CN, 11ª Sessão Ordinária, Processos 06604/2023 e 0002485-94.2023.2.00.0000, j. 23/11/2023) estabelecendo que o pedido de certidão notarial deve ser, preferencialmente, feito em formato digital, com identificação do solicitante e a motivação, exceto quando o requerente for o titular dos dados. O cartório deve manter um prontuário dessas informações por 1 ano, conforme o Provimento CNJ n. 50/2015.

Na referida diretriz, ficou consignado que quando a certidão for solicitada por terceiros, o tabelião deve informar a presença de dados sensíveis, podendo emitir a certidão com tarja no dado sensível quando não for essencial à finalidade do requerente. A certidão deverá conter a indicação de que é cópia fiel do ato, com exceção do dado sensível. Para certidões na modalidade de cópia reprográfica, os mesmos critérios são aplicados. O tabelião deve evitar incluir dados sensíveis nos instrumentos notariais, salvo quando imprescindível para a constituição do ato.

REGISTRO CIVIL DE PESSOAS NATURAIS

A Seção XIII do CNN detalha as atividades do Registro Civil de Pessoas Naturais, equilibrando transparência e proteção de dados. Dentre as recomendações específicas por tipo de documento estão:

- **Certidões de breve relato:** é livre o acesso a certidões de breve relato, independentemente de autorização do juiz corregedor permanente. Caso a emissão da certidão for requerida por terceiros e a certidão contiver dados sensíveis, somente será feita a expedição mediante a autorização do juízo competente. Se o titular for falecido, as certidões poderão ser fornecidas aos parentes em linha reta, independentemente de autorização judicial.
- **Certidões por quesito:** as solicitações de certidões por quesitos ou informações solicitadas, independentemente da expedição de certidões, receberão o mesmo tratamento destinado às certidões solicitadas em inteiro teor quando os dados solicitados forem restritos, sensíveis ou sigilosos.
    - Dados restritos: previstos no art. 45 e art. 95 da Lei n. 6.015/1973, no art. 6.º e seus parágrafos da Lei n. 8.560/1992, nas normas de alteração de nome ou sexo no caso de pessoa transgênero ou outros, desde que previstos em legislação específica.
    - Dados sensíveis: previstos no inciso II do art. 5.º da LGPD ou outros, desde que previstos em legislação específica.
    - Dados sigilosos: previstos no parágrafo 7.º do artigo 57 da Lei n. 6.015/1973 ou outros, desde que previstos em legislação específica.

- **Certidões de inteiro teor**
  - A emissão da certidão depende de requerimento escrito com firma reconhecida do requerente ou com assinatura digital nos padrões ICP-Brasil, no padrão do sistema gov.br ou com assinatura confrontada com o documento de identidade original.
  - O reconhecimento de firma será dispensado quando o requerimento for firmado na presença do oficial ou de preposto.
  - Os requerimentos poderão ser recepcionados por e-mail ou por meio da Central de Informações do Registro Civil (CRC), desde que assinados digitalmente, nos padrões da ICP-Brasil, cuja autenticidade e integridade serão conferidas no verificador de conformidade do Instituto Nacional de Tecnologia da Informação (ITI), por meio do sistema de assinatura gov.br ou com assinatura confrontada com o documento de identidade original.
  - O requerimento deverá conter a identificação do requerente, o motivo em virtude do qual se requer a certidão sob a forma de inteiro teor e o grau de parentesco com o registrado, caso exista, bem como o fato de ser este falecido ou não.

- **Certidão de óbito:** não é necessário requerimento ou autorização judicial para emissão de certidão de óbito em nenhuma de suas modalidades.

A respeito da emissão e do fornecimento de certidão sobre procedimentos preparatórios ou documentos apresentados para a realização de atos no Registro Civil das Pessoas Naturais, o CNN determina que a solicitação dessa certidão somente poderá ser realizada a pedido do próprio interessado ou do titular do documento, seus representantes legais e mandatários com poderes especiais ou mediante autorização judicial ou, ainda, quando o documento solicitado for público com publicidade geral e irrestrita. Após o falecimento do titular, essa certidão poderá ser fornecida ao solicitante que apresentar a certidão de óbito.

Nesse sentido, a Comissão de Proteção de Dados (CPD/CN) publicou a Diretriz n. 4/2023 (CPD/CN, 10ª Sessão Ordinária, Processos 06604/2023 e 0002485-94.2023.2.00.0000, j. 09/11/2023), que orienta que o pedido de certidão de inteiro teor no Registro Civil das Pessoas Naturais deve ser feito, preferencialmente, em formato digital, contendo identificação e motivação do solicitante, exceto quando for o próprio titular dos dados. O cartório deverá manter esse requerimento por 1 ano, conforme o Provimento CNJ n. 50/2015.

Ainda, qualquer interessado, independentemente de justificação ou de requerimento, pode realizar buscas nos índices dos Registros Civis das Pessoas Naturais, respeitados os emolumentos estabelecidos pelas legislações estaduais. A realização de buscas com base em outras fontes, além dos índices de registros dos livros do cartório, somente será autorizada mediante requerimento escrito fundamentado, sujeito à análise de finalidade

pelo oficial do registro civil das pessoas naturais, de cuja decisão, em caso de indeferimento, caberá revisão pelo juiz competente.

A respeito do edital de proclamas, este conterá tão somente o nome, o estado civil, a filiação, a cidade e a circunscrição do domicílio dos noivos. Quando os nubentes residirem em circunscrições diferentes, basta a publicação do edital de proclamas eletrônico na serventia onde tramita o processo de habilitação de casamento.

REGISTRO DE TÍTULOS E DOCUMENTOS E CIVIL DE PESSOAS JURÍDICAS

Em relação aos registros de títulos e documentos e civil de pessoas jurídicas, a seção XII do CNN apenas delimita que as notificações que contenham dados pessoais tratados devem ser feitas, preferencialmente, pelo Registro de Títulos e Documentos da circunscrição do destinatário. Quando assim não ocorrer, a notificação deverá ser enviada junto à folha adicional informativa com os dados tratados do notificado.

REGISTRO DE IMÓVEIS

A seção XIV do CNN, na especialidade de registro de imóveis, deu especial destaque ao processo de emissão de certidão. Dentre as recomendações específicas por tipo de documento estão:

- **Pedidos de certidão de registros em sentido estrito, averbações, matrículas, transcrições ou inscrições específicas, expedidas em qualquer modalidade**: esses pedidos dependem de identificação do requerente e independem de indicação da finalidade.
- **Pedidos de certidão de documentos arquivados**: dependem de identificação do requerente e independem de indicação da finalidade os pedidos de certidão de documentos arquivados no cartório, desde que haja previsão legal ou normativa específica de seu arquivamento no registro. Pedidos de certidão de documentos arquivados em cartório para a qual não haja previsão legal específica de expedição dependem de identificação do requerente e indicação da finalidade.
    - Caso seja caracterizada tentativa de tratamento de dados em desacordo com as finalidades do Registro de Imóveis e com os princípios da LGPD, poderá o oficial recusar o fornecimento em nota fundamentada do que caberá revisão pelo juízo competente.
- **Pedidos de certidão, de busca e de informações apresentados em bloco**: ainda que instruídos com a numeração dos atos a serem certificados, esses pedidos depen-

dem de identificação do requerente e indicação da finalidade. Caso seja caracterizada tentativa de tratamento de dados em desacordo com as finalidades do Registro de Imóveis e com os princípios da LGPD, poderá o oficial recusar o fornecimento em nota fundamentada do que caberá revisão pelo juízo competente.

- **Matrícula eletrônica**: as certidões dos imóveis que já forem objeto de matrícula eletrônica, após a "primeira qualificação eletrônica", serão expedidas, independentemente de indicação de finalidade, em formato nato-digital estruturado, contendo a situação jurídica atual do imóvel, ou seja, a sua descrição, a titularidade e os ônus reais não cancelados. A expedição de certidão de atos anteriores da cadeia filiatória do imóvel depende de identificação segura do requerente e de indicação da finalidade.
- **Buscas fundadas exclusivamente no indicador pessoal ou real**: o atendimento a requisições desses tipos de busca pressupõe a identificação segura do solicitante, bem como a indicação da finalidade, mantendo-se o registro em meio físico ou virtual.

O CNN dispõe que não serão expedidas certidões cujo conteúdo envolva informações sobre dados pessoais extraídos de mais de uma matrícula, assentamento do registro auxiliar, transcrição ou inscrição, ressalvadas as hipóteses que tenham previsão legal ou normativa expressa, como as certidões de filiação de imóveis, de propriedade com negativa de ônus e alienações ou outras compatíveis com as finalidades dos registros de imóveis e com os princípios da LGPD.

O fornecimento, pelo registrador, por qualquer meio, de informações sobre o registro não veiculadas por certidão dependerá da segura identificação do solicitante e da indicação da sua finalidade, exceto nos casos em que o solicitante figure no registro em questão.

Além disso, o CNN indica que serão formados prontuários físicos ou digitais contendo os dados de identificação e indicação de finalidade em todas as hipóteses em que essas informações tenham sido exigidas. O titular dos dados pessoais solicitados terá direito a requisitar as informações contidas nos prontuários formados em virtude de buscas ou pedidos de informações e certidões para os quais foi exigida a identificação do solicitante e a indicação de finalidade.

PROTESTO DE TÍTULOS E DOCUMENTOS

A Seção XV do CNN dispõe sobre as certidões de protestos de títulos tratando os temas de emissão de certidão e coleta de dados. Dentre as recomendações específicas por tipo de documento estão:

- **Certidões individuais de protesto:** deverão constar, sempre que disponíveis, dados como nome, CPF ou CNPJ, entre outros, mas não deve constar o endereço completo, endereço eletrônico e telefone do devedor.
- **Certidões em forma de relação sobre inadimplementos por pessoas naturais**: essas certidões serão elaboradas pelo nome e CPF dos devedores, devidamente identificados, devendo abranger protestos por falta de pagamento, de aceite ou de devolução, vedada exclusão ou omissão, espécie do título ou documento de dívida, data do vencimento da dívida, data do protesto da dívida e valor protestado.
- **Informações complementares requeridas em lote:** nesses casos, poderão constar CPF dos devedores, espécie do título ou documento de dívida, número do título ou documento de dívida, data da emissão e data do vencimento da dívida, valor protestado, protocolo e data do protocolo, livro e folha do registro de protesto, data do protesto, nome e endereço do cartório.
- **Documentos arquivados**: o fornecimento de cópias ou certidões de documentos arquivados na serventia se limita ao documento protestado propriamente dito, nos termos do art. 22 da Lei n. 9.492/1997, enquanto perdurar o protesto, e dentro do prazo máximo de 10 anos, nos termos do art. 30 Lei n. 9.492/1997, não devendo ser fornecidas cópias dos demais documentos, salvo para as partes ou com autorização judicial. Se o documento arquivado for de identificação pessoal, a cópia arquivada somente deve ser fornecida ao próprio titular.

No caso da apresentação de dados desnecessários para a atividade objetivada, o tabelião de protesto poderá devolver ou eliminar documentos apresentados para protesto ou para cancelamento que forem considerados desnecessários à prática do ato almejado, após adequada qualificação. Ainda, o documento cujo original não precise ser guardado por imposição legal deve ser eliminado de maneira segura quando for digitalizado, evitando-se a duplicidade.

O CNN autoriza o tabelião de protesto a eliminar o documento após o término do prazo da tabela de temporalidade prevista no Provimento 50, da Corregedoria Nacional de Justiça, ou superada a necessidade de sua guarda por outras circunstâncias, tais como prescrição civil, tributária e penal. Essas determinações estão alinhadas com os princípios de necessidade e adequação, já que limitam o tratamento de dados ao estritamente neces-

sário, exigem descarte seguro e consciente de documentos e estão alinhadas à lógica de minimização de dados e governança responsável.

Quanto ao processo de intimação do devedor, antes da expedição do edital para intimação do devedor, o tabelião poderá buscar outros endereços em sua base de dados, nos endereços em que outros tabeliães realizaram a intimação, desde que na mesma base da sua competência territorial ou nos endereços eletrônicos a serem compartilhados por meio da Cenprot, bem como nos endereços constantes de bases de natureza jurídica pública e de acesso livre e disponível ao tabelião. A Cenprot deverá compartilhar entre os tabeliães os endereços em que foi possível a realização da intimação de devedores, acompanhado do CNPJ ou CPF do intimado, bem como da data de efetivação.

Ainda, a declaração eletrônica de anuência para fins de cancelamento de protesto, recebida na forma eletrônica, poderá ser comunicada ao interessado por meio dos Correios, das empresas especializadas, do portador do próprio tabelião ou de correspondência eletrônica, pela internet ou por qualquer outro aplicativo de mensagem, ficando autorizado o encaminhamento de boleto bancário, outro meio de pagamento ou instruções para pagamento dos emolumentos e das despesas relativas ao cancelamento do protesto.

CONCLUSÃO

A aplicação da LGPD às serventias extrajudiciais representa um marco significativo na consolidação de uma cultura de proteção à privacidade e ao tratamento ético de dados no setor notarial e registral. Como delegatários de serviços públicos, os cartórios exercem funções de grande relevância para a sociedade e, por isso, a conformidade com a LGPD deve ser entendida não apenas como uma obrigação legal, mas como um compromisso institucional com o direito fundamental à proteção de dados, com a segurança jurídica e com a confiança estabelecida entre o cidadão e a serventia.

Este Manual buscou apresentar, de forma estruturada e prática, os principais conceitos da legislação de proteção de dados adaptados ao contexto das serventias extrajudiciais, esclarecendo o papel dos agentes de tratamento, as bases legais aplicáveis às diversas operações cartorárias e os instrumentos normativos que regulam a atuação dos cartórios nesse campo. Além disso, foram propostas diretrizes para orientar a implementação de políticas de governança e segurança da informação, a capacitação das equipes e o relacionamento com terceiros, sempre com foco na mitigação de riscos e na garantia dos direitos dos titulares de dados.

Reconhecendo a complexidade das atividades desenvolvidas pelas diferentes especialidades, como Tabelionato de Notas, Registro Civil de Pessoas Naturais, Registro de Títulos e Documentos e Civil de Pessoas Jurídicas, Registro de Imóveis e Protesto de Títulos e Documentos, este Manual também oferece recomendações específicas por atribuição, de modo a assegurar que a adequação à LGPD respeite as particularidades legais e operacionais de cada área.

Diante dessas peculiaridades, apesar da LGPD ser a norma de referência à conformidade com a proteção de dados, a proteção de dados no ambiente cartorário deve ser interpretada em conjunto com outras normas complementares, de caráter setorial, que conformam o regime jurídico próprio das atividades notariais e registrais.

Destacam-se, nesse sentido, o Código de Normas da Corregedoria Nacional de Justiça (CNN), os provimentos da Corregedoria Nacional de Justiça, em especial o Provimento n. 134/2022, que trata da implementação de medidas de conformidade com a LGPD nas serventias, e o Provimento n. 50/2015, que dispõe sobre a gestão documental, fixando regras de temporalidade e eliminação de documentos. No plano institucional, é importante ainda considerar as normas estaduais e os acordos, convênios e regulamentos internos firmados com as Centrais de Serviços Compartilhados e os Operadores Nacionais de Registro, que também atuam como controladores de dados no compartilhamento interinstitucional de informações.

A adequação das serventias extrajudiciais à LGPD requer planejamento, diagnóstico e implementação progressiva de ações técnicas, organizacionais e jurídicas. Dada a sensibilidade e o volume das informações manipuladas pelos cartórios, a conformidade com a legislação de proteção de dados deve ser estruturada em torno de prioridades estratégicas, visando à minimização de riscos jurídicos e reputacionais, bem como à melhoria contínua dos serviços prestados.

Uma das prioridades é a realização de um mapeamento completo das operações de tratamento de dados pessoais, com identificação das entradas e saídas de dados, suas respectivas finalidades, formas de armazenamento, compartilhamentos e riscos envolvidos. A partir desse mapeamento, o cartório poderá elaborar um registro de operações de tratamento que sirva de base para as demais ações de conformidade. A partir desse mapeamento, é essencial a identificação das bases legais aplicáveis, uma vez que, embora os cartórios atuem por imposição legal ou normativa em muitas de suas atribuições, outras atividades exigem uma análise cuidadosa do fundamento jurídico que autoriza o tratamento.

A indicação de um encarregado (DPO) é outra medida recomendada. Ainda que a LGPD não exija expressamente a nomeação do encarregado por cartórios, de acordo com o Provimento n. 134/2022, essa nomeação pode ser conjunta entre serventias ou individual. Esse profissional atuará como canal de comunicação com os titulares e a ANPD, além de apoiar a governança em proteção de dados. Outras prioridades incluem a definição clara dos papéis dos agentes de tratamento (controlador, operador ou cocontrolador), a implementação de uma política interna de proteção de dados, o estabelecimento de processos para atendimento aos direitos dos titulares, a capacitação contínua das equipes e a revisão contratual com fornecedores e parceiros terceirizados.

Por fim, é essencial que os cartórios adotem medidas técnicas e administrativas robustas para garantir a segurança da informação, com políticas de backup, controle de acesso, criptografia, eliminação segura de documentos e planos de resposta a incidentes. Essas prioridades devem ser entendidas como etapas complementares de um processo contínuo de conformidade, e não como um checklist pontual. A maturidade em proteção de dados será construída ao longo do tempo, com base na experiência, na supervisão regulatória e no compromisso institucional das serventias com a integridade, a legalidade e a confiança pública.

A adoção de medidas para proteção de dados deve ser entendida como um processo contínuo de aprimoramento institucional. A cada nova tecnologia incorporada, a cada novo serviço oferecido, os cartórios são convidados a revisitar seus fluxos, contratos e procedimentos, sempre com vistas à transparência, à responsabilidade e à proteção da privacidade dos cidadãos. Com a adoção efetiva das práticas aqui descritas, as serventias não apenas atendem às exigências legais, mas também reafirmam seu papel como instituições confiáveis, modernas e alinhadas aos princípios constitucionais da administração pública e da cidadania digital.

Acesse também a versão digital:

CONSELHO NACIONAL DE JUSTIÇA