

ANOREG|MA

Associação dos Notários e Registradores do Estado do Maranhão

GUIA DE CONFORMIDADE COM
A LGPD PARA ASSOCIADOS
ANOREG



ST•A | SOTÃO
ADVOCACIA

Apresentação

A LGPD, Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados, entrou em vigor em setembro de 2020 e estabelece as regras para o tratamento de dados pessoais, aplicando-se tanto ao indivíduos quanto às instituições de direito público ou privado, em ambientes físicos e digitais.

Atento à importância da LGPD para a rotina das serventias extrajudiciais, em agosto de 2022 o Conselho Nacional de Justiça editou o Provimento nº 134/2022 que trouxe, detalhadamente, quais medidas devem ser implementadas nos cartórios para adequação às exigências da lei e proteção dos direitos dos titulares, além das sanções para casos de descumprimento.

Assim, este guia educativo foi especialmente elaborado para os associados da ANOREG/MA, com o propósito de auxiliá-los na compreensão e efetiva conformidade com a LGPD.

PARA QUE FALAR EM LGPD?

A LGPD traz importantes impactos para as serventias extrajudiciais, tanto para o fomento ética e proteção dos direitos dos cidadãos, como para o cumprimento e conformidade legal. A adequação às exigências da LGPD fortalece a credibilidade das organizações, evita implicações negativas e mantém a integridade das serventias, respeitando a privacidade e minimizando riscos legais.



QUAL É O OBJETIVO DA LGPD?

A LGPD tem como objetivo principal proteger os direitos fundamentais de liberdade e privacidade das pessoas naturais que são titulares de dados pessoais.

Por isso, tenha sempre em mente que a preocupação da LGPD é PROTEGER O TITULAR!

Em seu texto, a LGPD regulamenta práticas relacionadas à coleta, uso, armazenamento, compartilhamento e controle de dados pessoais, preocupando-se com a garantia da privacidade através da rastreabilidade e do controle de acesso aos dados pessoais, construindo um ambiente ético, legalmente compatível e de alta credibilidade nas serventias extrajudiciais.

QUEM SÃO OS AGENTES DE TRATAMENTO?

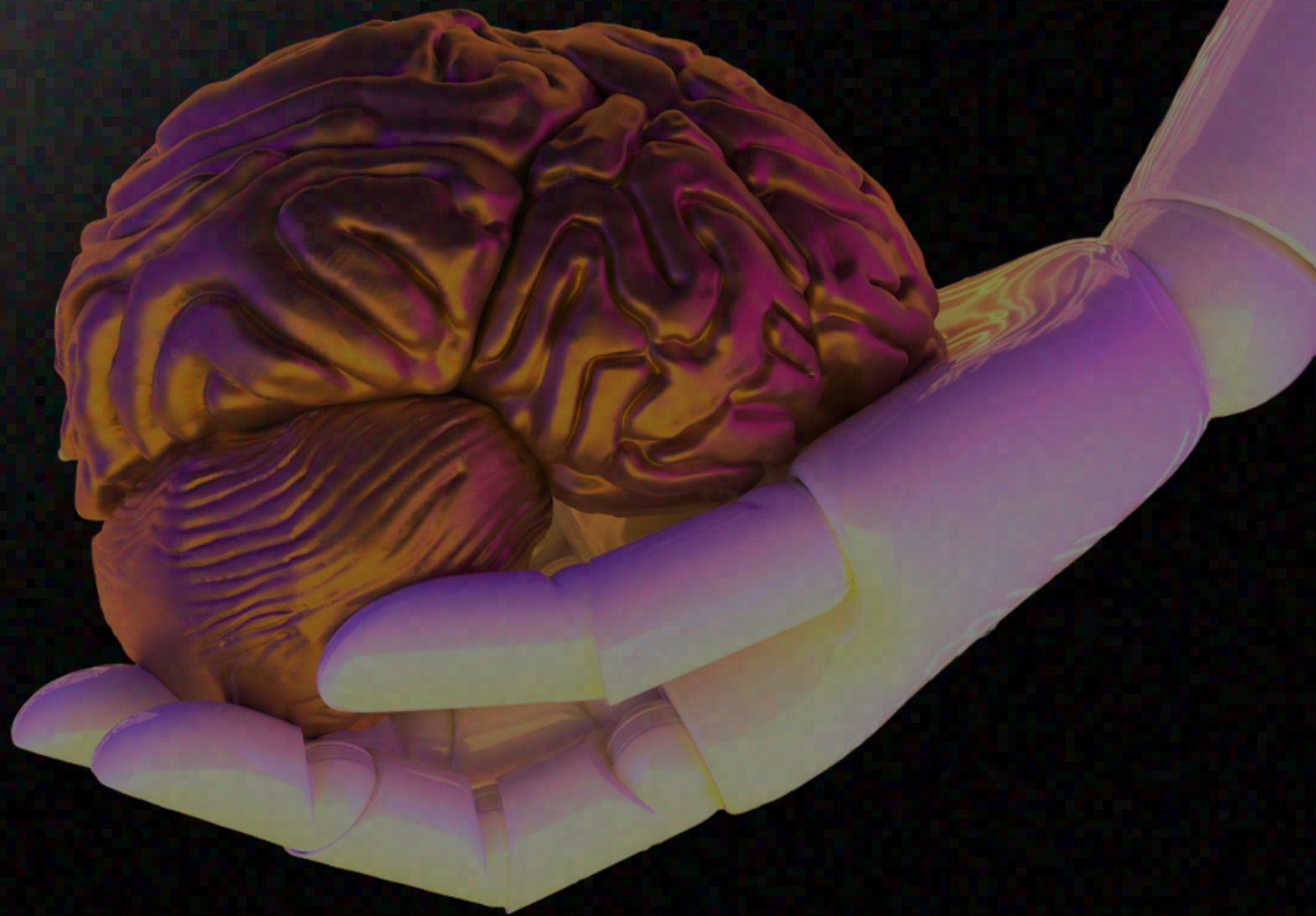
Na LGPD é importante identificarmos os agentes de tratamento, para então definirmos responsabilidades e atribuições, fundamentais à segurança jurídica da serventia.

São agentes de tratamento de dados o controlador e o operador.

1

Controlador de dados:

Pessoa física ou jurídica a quem compete as decisões referentes ao tratamento de dados. No caso das serventias o tabelião titular sempre será o controlador, mas também é possível que hajam outros controladores nas atividades de tratamento realizadas na serventia - o que seria o equivalente a uma responsabilidade conjunta pelo tratamento de dados pessoais, em co-controladoria, a depender do caso concreto.



2

Operador de dados:

pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Os operadores da serventia poderão ser integrantes ou não integrantes do seu quadro de prepostos, desde que na qualidade de prestadores terceirizados de serviços técnico. Assim, funcionários não são considerados operadores de dados, mas também precisam estar sob as regras estabelecidas pelo controlador – o que se faz pelos termos e políticas construídos na serventia.

3

Encarregado de Dados (DPO):

agente de tratamento de obrigatória indicação pelo controlador (art 41 da LGPD), cujas atribuições são:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. fomentar e disseminar a cultura da proteção de dados pessoais na serventia, recebendo as solicitações de titulares e da autoridade nacional (ANPD) e adotando providências quando for necessário. Ainda dentre as atribuições do DPO, temos a realização de treinamentos e orientações aos funcionários e contratados a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

PARA SEGURANÇA DA SERVENTIA, ENTENDA OS PRINCÍPIOS

Princípios sobre legitimação do tratamento:

I. Princípio da Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma diversa ou incompatível com essas finalidades.

II. Princípio da Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

III. Princípio da Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Princípios sobre a postura do agente de tratamento:

I. Princípio da Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

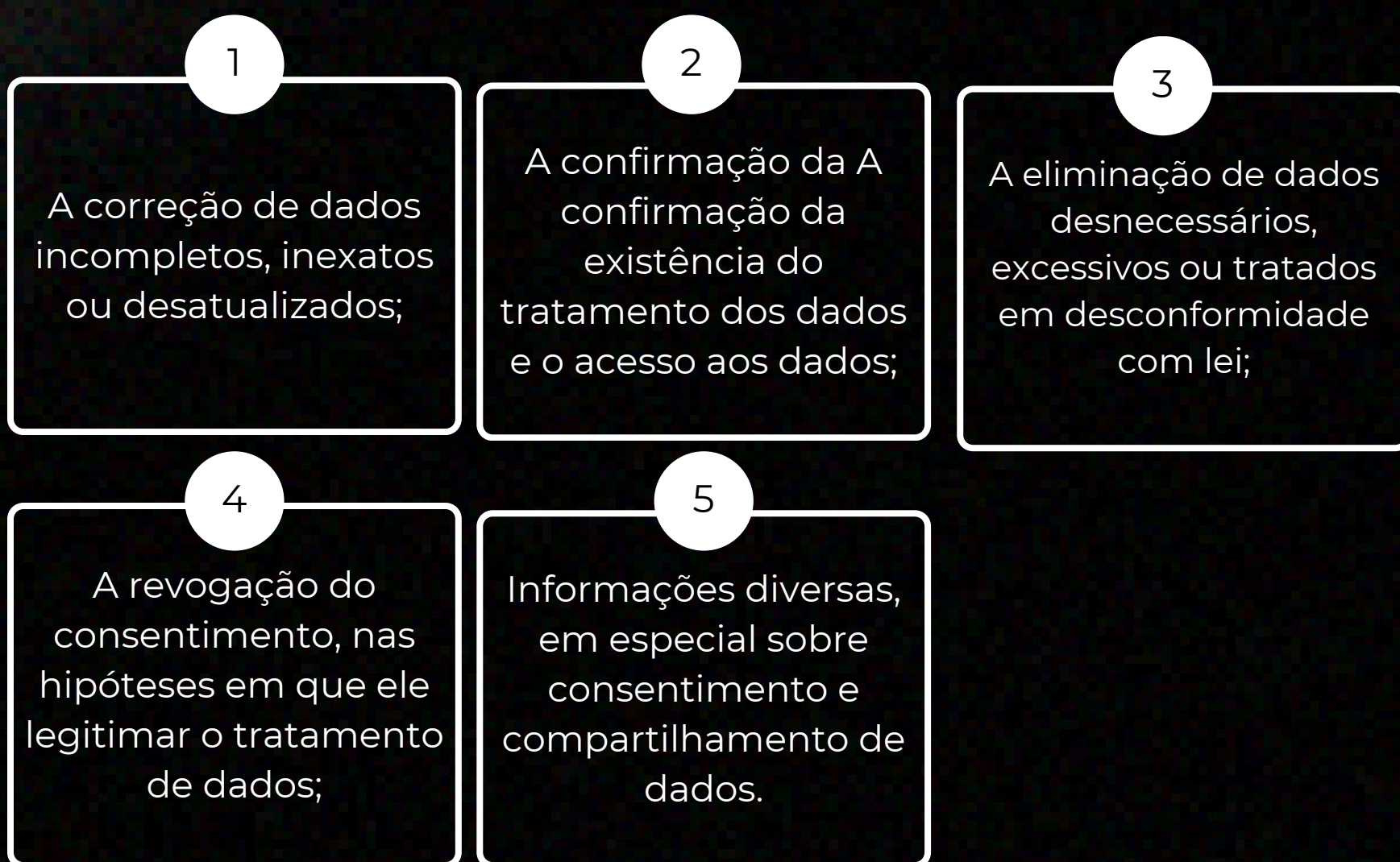
II. Princípio da Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

III. Princípio da prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

IV. Princípio da responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

DIREITOS DO TITULAR

Todos os usuários que possuam alguma informação utilizada pela serventia (clientes, funcionários, etc) são titulares de dados e podem requerer os seguintes direitos:



Para garantir a segurança e a proteção dos dados pessoais, o exercício desses direitos deve ser realizado mediante solicitação expressa, com a devida confirmação da identidade do titular, através do canal de exercício de direitos do titular.

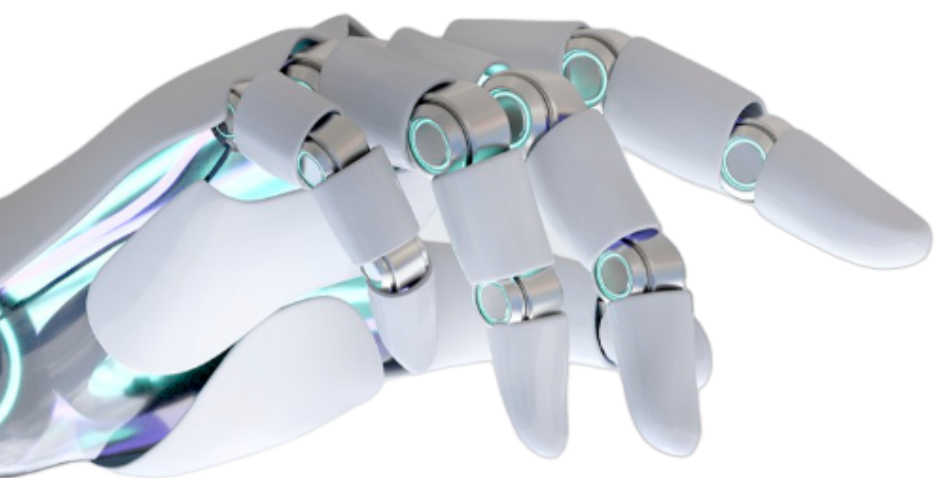
Levando em consideração a natureza dos serviços prestados pelos cartórios, é importante ressaltar que:

- **Certidões:** As informações obtidas por meio do exercício do direito de acesso não têm o valor de certidão oficial.
- **Gratuidade do Acesso:** A gratuidade do acesso é limitada aos dados pessoais constantes nos sistemas administrativos do cartório e não se aplica aos atos próprios da atividade registral, incluindo a emissão de certidões.
- **Correção de Dados Oficiais:** A correção de dados registrados em documentos oficiais do cartório, como matrículas de imóveis ou certidões de nascimento, deve seguir os procedimentos previstos na legislação ou normas específicas, seja de forma extrajudicial ou judicial.
- **Exclusão de Dados:** Dados podem ser apagados a pedido do usuário, desde que não existam obrigações legais ou regulatórias, execução de contratos ou outras circunstâncias que legitimem sua retenção.
- **Portabilidade de Dados:** Os cartórios extrajudiciais não se equiparam a prestadores de serviços no que se refere à portabilidade de dados pessoais.

PARA ADEQUAR A SUA SERVENTIA, SAIBA QUAIS MEDIDAS PRECISAM SEREM ADOTADAS

Nas serventias extrajudiciais, a segurança e gestão de dados são prioridades.

A implementação de medidas eficazes é fundamental para proteger as informações, especialmente os dados pessoais. Abaixo, seguem as ações que as serventias extrajudiciais devem adotar:



1. TREINAMENTO

As serventias extrajudiciais devem proporcionar treinamentos e sensibilização dos seus prepostos sobre a legislação de proteção de dados pessoais, incluindo debates e discussões apropriados. Essa medida é uma das mais importantes pois, além de promover alterações práticas, promove a coerência entre os documentos de evidência existentes e a rotina da serventia.

2. SEGURANÇA DA INFORMAÇÃO

As serventias devem empenhar seus melhores esforços na proteção da informação, com ênfase nos dados pessoais.

Devem ser aplicadas medidas de proteção administrativas, físicas e técnicas, exigindo dos fornecedores um nível aceitável de segurança da informação, com base em cláusulas contratuais e responsabilizações.

Tão importante quanto implementar as medidas de segurança da informação é ter como evidenciar todas as medidas adotadas, através de documentos, contratos e políticas internas.

3. MAPEAMENTO DE DADOS E DOCUMENTOS

Cada serventia deve realizar uma análise abrangente do percurso dos dados pessoais, desde o momento da coleta até a conclusão do tratamento e a elaboração da documentação deve refletir fielmente a realidade e as operações da serventia.

Com um mapeamento bem feito, a serventia comprova medidas de governança e a adequação do seu programa interno de privacidade.

4. CONTRATOS

As serventias devem revisar e adequar todos os contratos que envolvam atividades de tratamento de dados pessoais. Além disso, é importante comunicar aos prestadores de serviços sobre o processo de adequação à LGPD que a serventia está conduzindo e estabelecer obrigações conexas e específicas a cada um deles.

5. BASE DE DADOS

A serventia é responsável pela guarda da base de dados e do acervo, garantindo que o armazenamento aconteça em um ambiente seguro e controlado. O uso dos dados deve ser restrito aos fins estabelecidos na política de privacidade, com acesso limitado a profissionais e fornecedores autorizados.

6. MEDIDAS DE SEGURANÇA

De acordo com o Provimento nº 74/2018 do CNJ, a serventia deve implementar medidas técnicas e administrativas de segurança da informação, as quais incluem a utilização de firewall, antivírus, antissequestro e filtro de conteúdo.

Além disso, é fundamental realizar backups de forma regular. A serventia também deve contar com armazenamento em servidores próprios e em nuvem, fornecendo orientações documentadas sobre procedimentos de manutenção da segurança.

7. ARMAZENAMENTO E DESCARTE

De acordo com o Provimento nº 74/2018 do CNJ, a serventia deve implementar medidas técnicas e administrativas de segurança da informação, as quais incluem a utilização de firewall, antivírus, antissequestro e filtro de conteúdo.

Além disso, é fundamental realizar backups de forma regular. A serventia também deve contar com armazenamento em servidores próprios e em nuvem, fornecendo orientações documentadas sobre procedimentos de manutenção da segurança.

CONSIDERAÇÕES FINAIS

Este guia foi elaborado para oferecer uma visão abrangente da Lei Geral de Proteção de Dados Pessoais (LGPD) a todos os associados da Anoreg/MA.

Nosso objetivo é tornar os conceitos fundamentais da LGPD mais acessíveis, esclarecer quais são os direitos dos titulares de dados e fornecer informações cruciais sobre as principais medidas necessárias para criar uma cultura de conscientização entre todos os envolvidos.

Juntos, estamos preparados para enfrentar os desafios da LGPD e promover a proteção de dados pessoais em nossas operações diárias.

As exigências da LGPD são uma obrigação legal para todos e a adequação às novas regras traz consigo ganhos secundários como aprimoramento da qualidade dos serviços, fortalecimento de imagem e posicionamento de mercado.

A ANOREG/MA, com o intuito de promover a adequação das serventias às exigências da LGPD, firmou convênio com o escritório SOTÃO ADVOCACIA e está disponibilizando gratuitamente aos associados o serviço de Encarregado de Dados (DPO), a ser realizado pela Dra Rayana Sotão. Entre em contato e entenda melhor como utilizar o benefício!

ST • A | SOTÃO
ADVOCACIA

ANOREG|MA

Associação dos Notários e Registradores do Estado do Maranhão



Esse guia foi elaborado por:

Rayana Pereira Sotão

Advogada, Sócia fundadora do Sotão
Advocacia
Encarregada de Dados (DPO)
Consultora em Proteção de Dados - EXIN
Foundation e EXIN Essentials
Membro do Comitê Jurídico da
Associação Nacional dos Profissionais de
Privacidade de Dados - APDADOS
Professora Universitária
Mestre em Direito pela Universidade
Federal do Maranhão