# LGPD NA CODEMGE/ CODEMIG

## A Lei Geral de Proteção de Dados Pessoais e os agentes públicos

Belo Horizonte, Agosto de 2026

## ORGANIZAÇÃO

Comissão Interna de Privacidade (CIP)
Codemge/Codemig

**Composição da CIP:**

Patrícia Sanglard Fadlallah – Encarregada/*Data Protect on Officer* (DPO)
Érica Rosália de Jesus Parreiras – Coordenadora
Cláudia Patrocínio Veloso
Denise Lobato de Almeida
Juliana Lúcia Mascarenhas Gomes Ferreira
Marcello Pereira Machado
Ronaldo José Madureira
Suellen Silva de Almeida

**Diagramação e produção visual:**

Gerência de Comunicação (Gerco)
Codemge/Codemig

# SUMÁRIO

# 1. APRESENTAÇÃO

A Lei nº 13.709/2018 é conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Passou a vigorar em setembro de 2020 e surgiu em um contexto de intensa circulação de dados pela internet. Com os avanços tecnológicos recentes, o uso de redes sociais e a virtualização de diversos aspectos vida cotidiana, os dados pessoais chegam a ser considerados hoje como o "novo petróleo".

Nesse contexto, o desenvolvimento da sociedade de rede e a expansão das tecnologias de informação e comunicação (TICs) geram oportunidades e desafios. De um lado, podem agilizar a comunicação, permitir reuniões à distância, gerar economia de recursos e reduzir deslocamentos físicos. Por outro lado, podem elevar a exposição, a vulnerabilidade, o monitoramento e a vigilância.

Diante disso, várias leis buscando a proteção dos dados pessoais têm sido implementadas pelo mundo. Crescem também as discussões sobre a privacidade e a possibilidade de o indivíduo participar do processamento de seus dados pessoais e controlar o uso de suas informações.

No Brasil, a proteção de dados na Administração Pública está relacionada com a Constituição Federal de 1988, a Lei de Acesso à Informação (LAI, Lei nº 12.527/2011) e o Marco Civil da Internet (Lei nº 12.965/2014). Por sua vez, a LGPD veio proteger os dados pessoais do cidadão, guardando estreita relação com o direito à liberdade, à privacidade e à não discriminação, para exemplificar.

Nesta cartilha temática, a Comissão Interna de Privacidade (CIP) esclarece conceitos gerais e dissemina informações pertinentes à LGPD para agentes públicos e privados, além de oferecer orientações importantes sobre a prote-ção de dados pessoais no âmbito das Companhias. A peça foi desenvolvida em parceria com a Gerência de Comuni-cação (Gerco) da Empresa, especialmente para o público externo, incluindo fornecedores e prestadores de serviço, por exemplo. Leia e consulte este documento sempre que precisar.

## Objetivos da cartilha

- Apresentar o assunto, para o público externo, de forma simplificada, clara e didática;
- Informar os conceitos, fundamentos e princípios da LGPD, a fim de orientar a atuação de todos os que realizam tratamento de dados pessoais;
- Esclarecer os direitos dos titulares de dados;
- Fomentar a disseminação da cultura de proteção de dados nas Companhias e junto aos seus públicos externos.

O CIP permanece à disposição – e-mail: privacidade@codemge.com.br. Boa leitura!

# 2. BREVE LINHA DO TEMPO DAS REGULAÇÕES NO BRASIL

## 2010

A proteção de dados pessoais recebe as primeiras discussões mais aprofundadas no Brasil, mediante Consulta Pública do Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais

## 2011

É publicada a Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI) –, que regula o acesso à informação disposto na Constituição Federal de 1988 e a transparência dos dados pessoais pelo poder público

## 2014

Entra em vigor o Marco Civil da Internet, pela Lei nº 12.965, estabelecendo princípios, garantias, direitos e deveres para o uso da rede mundial de computadores no Brasil

## 2018

É promulgada a LGPD, em agosto, por meio da Lei nº 13.709, com o prazo de dois anos para vigorar

## 2020

Entra em vigência a LGPD, no mês de setembro

## 2021

LGPD adquire vigência plena, em agosto, de modo que descumprimentos passam a ser passíveis de judicialização e sanções administrativas

## 3. O QUE É A LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD), de nº 13.709/2018, prevê regras para que os dados das pessoas sejam protegidos de uso indevido. Foi promulgada, portanto, para regulamentar o tratamento dessas informações e preservar os direitos fundamentais de liberdade e de privacidade, bem como a livre formação da personalidade e a dignidade de cada indivíduo.

A Lei abarca o tratamento de dados pessoais, dispostos em meio físico ou digital, por pessoa física ou jurídica de direito público ou privado. Engloba, assim, um amplo conjunto de operações que podem ocorrer em meios manuais ou eletrônicos.

Trata-se de um avanço na disciplina da proteção de dados pessoais no Brasil, uma vez que, antes dela, havia apenas normas esparsas, genéricas e fragmentadas sobre o assunto. Seguindo a tendência mundial, o País editou essa legislação contemporânea de proteção de dados, indo além da proteção da privacidade, ao promover também a liberdade e a autonomia das pessoas, bem como a confidencialidade e a integridade dos sistemas técnico-informacionais.

**Impedir ou disciplinar?**

A LGPD não pretende impedir nem restringir totalmente o tratamento de dados pessoais, hoje indispensável tanto para empresas privadas quanto para entes públicos. O objetivo é orientar e disciplinar o modo como pode e deve ser realizado, a fim de proteger as pessoas envolvidas.

Com isso, a LGPD traz, por um lado, segurança jurídica para os agentes de tratamento de dados e, por outro, protege o titular dos dados pessoais.

Aliás, a proteção de dados pessoais foi elevada ao status de direito fundamental, previsto no artigo 5º da Constituição Federal, com a promulgação da Emenda Constitucional nº 115, em 10/2/2022. Isso demonstra a importância conferida a essa temática no País, constituindo um marco significativo para todos os cidadãos brasileiros.

# 4. O QUE MUDA COM A LGPD

Para estarem em conformidade com a LGPD, tanto o poder público e como os entes privados precisam considerar alguma das hipóteses que justifiquem o tratamento de dados pessoais (bases legais, detalhadas no capítulo 9 desta cartilha). Além disso, devem adotar uma série de medidas de adequação, conformidade e cuidado, como eliminação de dados desnecessários, transparência e uso da segurança e da gestão de riscos para evitar vazamentos.

A LGPD inaugura e sistematiza um verdadeiro catálogo de direitos ao titular dos dados, que devem ser cumpridos e promovidos. Além da base legal, só será considerado justificado o tratamento de dados pessoais que atenda aos princípios estabelecidos no artigo 6º da LGPD: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. O capítulo 7 desta cartilha detalha esses princípios.

**O que muda na vida do cidadão**

Com a LGPD, o cidadão ganhou uma legislação específica para a proteção de seus dados pessoais. Isso é importante especialmente na era tecnológica atual, em que meros fragmentos ou vestígios isolados, apa-

rentemente insignificantes, podem revelar um quadro completo da personalidade de cada indivíduo, quando esses dados são associados, cruzados e processados com apoio de tecnologias ou sistemas computacionais. Nesse sentido, a LGPD busca evitar que essas informações sejam usadas de forma ilícita ou deturpada, para fins de discriminação ou exploração, por exemplo.

Além de disciplinar em quais situações os dados poderão ser usados, a lei confere uma série de direitos e ferramentas aos indivíduos, colocando-os como protagonistas nesse novo paradigma. Certamente, de compras on-line a redes sociais, de hospitais a bancos, de escolas a teatros, de hotéis a órgãos públicos, da publicidade à tecnologia, a LGPD afeta diferentes setores e serviços.

## 5. GLOSSÁRIO DA LGPD: CONCEITOS IMPORTANTES

### *DADO PESSOAL*

Informação relacionada a pessoa natural identificada ou identificável. Exemplos: nome, sobrenome, CPF, RG, CNH, título de eleitor, matrícula profissional, data de nascimento, e-mail, endereço, telefone.

### *DADO PESSOAL SENSÍVEL*

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Por terem potencial discriminatório, colocando os titulares em situação de maior vulnerabilidade, devem ser tratados com ainda mais cuidado, conforme regras da LGPD. Exemplos: tipo sanguíneo, religião, nome social, dado biométrico, filiação partidária.

### *DADO ANONIMIZADO*

Dado relativo a titular que não possa ser identificado, considerando o uso de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

***BANCO DE DADOS***

Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

***TITULAR DOS DADOS***

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Nesse sentido, os titulares podem ser, por exemplo, cidadãos que interajam com as Companhias, fornecedores, contratados e os próprios empregados.

***CONTROLADOR***

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Por exemplo, a Codemge/Codemig é o ente controlador dos dados tratados na realização das suas atividades.

***OPERADOR***

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Operadores são, por exemplo, os fornecedo-

res contratados pelo poder público que venham a tratar os dados do cidadão na execução de um contrato.

## *ENCARREGADO/DPO*

Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD). Em inglês, a função é chamada de *Data Protect on Officer* (DPO). A LGPD atribuiu ain-da outras funções ao Encarregado, como as de aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da ANPD 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. A Codemig designou, entre os empregados, uma pessoa para atuar como Encarregada – atualmente, Patrícia Sanglard Fadlallah.

## *AGENTES DE TRATAMENTO*

O controlador e o operador.

## *TRATAMENTO DE DADOS*

Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

## *ANONIMIZAÇÃO*

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

## *CONSENTIMENTO*

Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

## *BASE LEGAL*

Autorização legal que respalda o tratamento de dados pessoais e está prevista nos artigos 7º e 11 da LGPD.

## *PRINCÍPIOS*

Conforme o artigo 6º da Lei, as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas – veja o detalhamento no capítulo 7 desta cartilha.

## *BLOQUEIO*

Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

## *ELIMINAÇÃO*

Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

## *TRANSFERÊNCIA INTERNACIONAL DE DADOS*

Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

## *USO COMPARTILHADO DE DADOS*

Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

## *RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS*

Documentação do controlador que contém a descrição dos processos de tratamento de
dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

## *ÓRGÃO DE PESQUISA*

Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

## *AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD)*

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

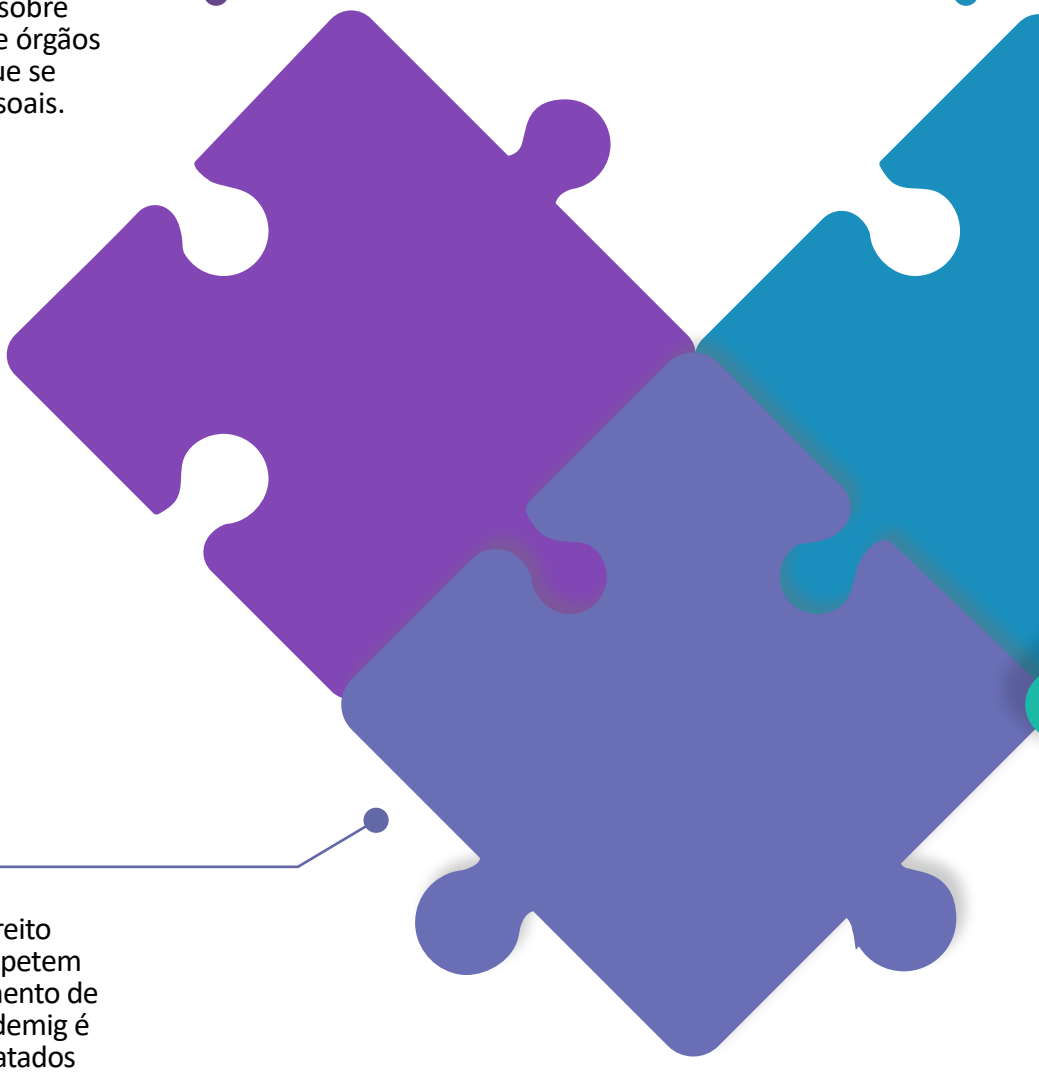
# 6. PRINCIPAIS ATORES

## ANPD

Agência Nacional de Proteção de Dados, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no território nacional. Trata-se do ente central de interpretação dessa Lei e sobre as suas próprias competências e casos omissos. Detém competência exclusiva para aplicar as sanções administrativas previstas na LGPD, com prevalência de suas competências sobre outras correlatas de entidades e órgãos da administração pública, no que se refere à proteção de dados pessoais.

## TITULAR

Pessoa natural a quem pertencem os dados pessoais. Nesse caso, os titulares podem ser, por exemplo, cidadãos que interajam com as Companhias, fornecedores, contratados e os próprios empregados.

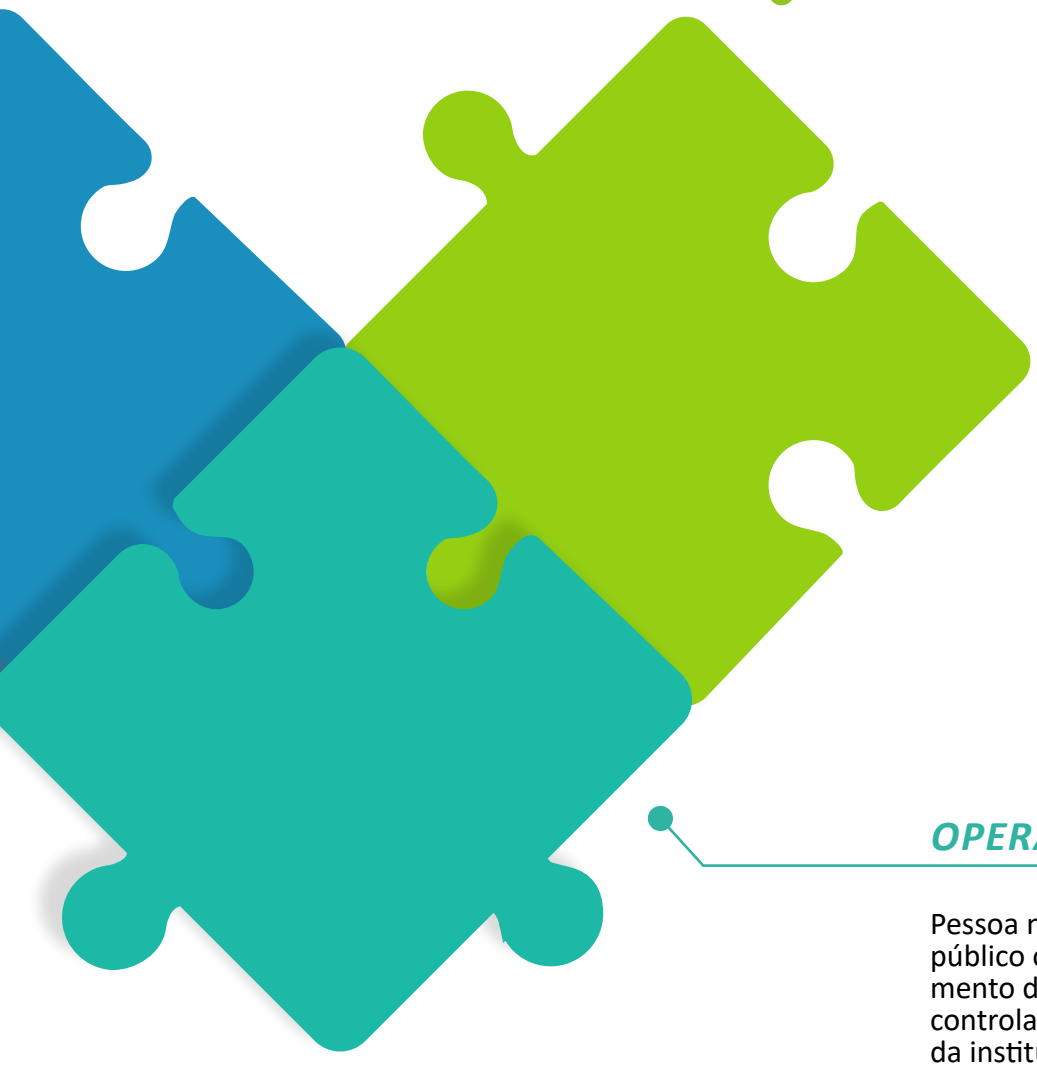


## CONTROLADOR

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. A Codemge/Codemig é o ente controlador dos dados tratados na realização das suas atividades.

## *Encarregado/DPO*

Pessoa indicada pelo controlador para atuar como canal de comunicação entre ele, os titulares dos dados e a ANPD. Em inglês, a função é chamada de Data Protection Officer (DPO). A Codemig designou, entre os empregados, uma pessoa para atuar como Encarregada – atualmente,  Patrícia Sanglard Fadlallah.



## *OPERADOR*

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador não faz parte da instituição; ao contrário, é externo a ela e contratado para uma finalidade específica, agindo conforme diretrizes definidas pelo controlador. Ex.: empresa contratada para realizar o armazenamento de dados em “nuvem”.

Importante: no âmbito das Companhias, empregados, estagiários e terceirizados atuam sob o poder diretivo do controlador e também são responsáveis pelo cumprimento da LGPD.

# 7. OS PRINCÍPIOS DA LGPD

A observância dos princípios da LGPD (art. 6º) constitui parte essencial do tratamento de dados pessoais. A Lei tem os seguintes princípios:


***FINALIDADE***

Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

***ADEQUAÇÃO***

Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo
com o contexto do tratamento.

***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. O princípio da necessidade impõe, assim, que a coleta se atenha à menor quantidade possível de dados para o alcance da finalidade proposta. Os entes públicos e privados devem verificar se informações usualmente coletadas de cidadãos (como cópias de documentos de identidade ou de dados solicitados em formulários) ou de contratados (a exemplo de estado civil e endereço residencial) são, efetivamente, necessárias, não se admitindo a coleta indistinta de dados pessoais, em particular de dados para os quais não se tenha identificado uma finalidade específica e legítima para o tratamento.

***LIVRE ACESSO***

Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do
tratamento, bem como sobre a integralidade de seus dados pessoais. Esse princípio enfatiza a necessidade de o agente de tratamento disponibilizar mecanismos efetivos para que o titular possa solicitar e ter acesso a determinadas informações referentes ao tratamento de seus dados pessoais.

***QUALIDADE DOS DADOS***

Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

***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. Esse princípio impõe obrigações de cunho geral e que demandam uma postura ativa do agente de tratamento, o qual tem o dever de disponibilizar as informações exigidas pela Lei, independentemente de solicitação do titular.

***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.

***PREVENÇÃO***

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

***NÃO DISCRIMINAÇÃO***

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

***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.

# 8. TRATAMENTO DE DADOS

O tratamento de dados pessoais abarca toda operação efetuada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação/controle da informação, modificação, comunicação, transferência, difusão ou extração.

O tratamento pode ocorrer apenas quando o titular ou o responsável legal consentir, de maneira específica e destacada, para finalidades determinadas, ou sem o consentimento para situações previstas no artigo 7º da Lei Geral de Proteção de Dados Pessoais.

No caso de dados pessoais sensíveis, o tratamento pode se dar somente quando o titular ou o responsável legal consentir, de maneira específica e destacada, para finalidades determinadas, ou sem o consentimento para certas situações previstas no artigo 11, inciso II, da LGPD.

**Atenção! O tratamento de dados pessoais pelo poder público deve estar sempre associado a uma finalidade pública, que seja:**

• legítima, isto é, lícita e compatível com o ordenamento jurídico, além de amparada em uma base legal, que autorize o tratamento;

• específica, de forma que a partir da finalidade seja possível delimitar o escopo do tratamento e estabelecer as garantias necessárias para a proteção dos dados pessoais;

• explícita, ou seja, expressa de uma maneira clara e precisa;

• informada, isto é, disponibilizada em linguagem simples e de fácil compreensão e acesso ao titular dos dados.

Dessa forma, o tratamento de dados pessoais pelo poder público, incluindo a divulgação pública de dados pessoais, deve ser realizado em conformidade com as disposições da LGPD. Devem ser observadas as normas que garantem a proteção integral dos dados pessoais, a autodeterminação informativa e o respeito à privacidade dos titulares durante todo o ciclo do tratamento. Além de observar os princípios previstos na Lei e verificar a base legal aplicável ao tratamento, é preciso assegurar os direitos dos titulares e adotar medidas de prevenção e segurança, a fim de evitar a ocorrência de incidentes.

# FUNDAMENTOS


**Importante: são destinatárias da proteção da LGPD exclusivamente pessoas naturais titulares dos dados pessoais. Contudo, a lei se aplica e deve ser observada por todo aquele que realize o tratamento de dados, seja *online* e/ou *offline*, por pessoa física ou jurídica, com finalidade econômica, pública ou privada.**

**Atenção! O tratamento de dados pessoais é um processo com duração definida, após o qual, em regra, eles devem ser eliminados, observados os prazos e condições previstos em normas específicas que regem a gestão de documentos e arquivos. A LGPD estabelece, em seu artigo 16, hipóteses gerais em que é autorizada a conservação de dados pessoais para as seguintes finalidades:**

• cumprimento de obrigação legal ou regulatória pelo controlador;

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

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

• uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

**No contexto das Companhias:**

O tratamento de dados pessoais é um processo com duração definida, após o qual, em regra, eles devem ser eliminados, observados os prazos e condições em normas específicas. Nas Companhias, como empresa estatal, há necessidade de prestação de contas anual para o Tribunal de Contas do Estado de Minas Gerais e demais órgãos de controle; por essa razão, orienta-se que a eliminação de dados pessoais ocorra em consonância com a Tabela de Temporalidade e Destinação de Documentos de Arquivo (TTDDA).

O dado pessoal deve seguir a mesma lógica de descarte do suporte que o contenha (documento físico ou digital). Essa orientação mitiga o risco de descarte de informações e documentos essenciais para fins de prestação de contas e demais ações de controle.

# 9. BASE LEGAL

Nos termos da LGPD, o tratamento de dados pessoais só poderá ser realizado se houver autorização legal, chamada de “base legal”. Está prevista nos artigos 7º e 11 da Lei.

O tratamento de dados pessoais pode ser realizado somente nas seguintes condições:

1. Mediante o consentimento pelo titular;

2. Para o cumprimento de obrigação legal ou regulatória pelo controlador;

3. Pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da LGPD;

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

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

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

7. Para a proteção da vida ou da incolumidade física do titular ou de terceiro;

8. Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

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

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

## Bases legais da LGPD


**No contexto das Companhias:**

Considerando o contexto das Companhias e as atividades por ela desenvolvidas, as hipóteses autorizativas do tratamento de dados pessoais mais utilizadas para o tratamento são:
• cumprimento de obrigação legal;
• legítimo interesse;
• execução de contrato ou de procedimentos preliminares relacionados;
• exercício regular de direitos em processo judicial, administrativo ou arbitral.

Já no caso das exceções para manutenção de dados pessoais após o término do tratamento, a base legal mais utilizada pela Companhia é o cumprimento de obrigação legal ou regulatória.

**Importante:**

**> Consentimento**

• O consentimento poderá eventualmente ser admitido como base legal para o tratamento de dados pessoais pelo poder público. Para tanto, a utilização dos dados não deve ser compulsória, e a atuação estatal não deve, em regra, basear-se no exercício de prerrogativas estatais típicas, que decorrem do cumprimento de obrigações e atribuições legais.

• É dispensada a exigência do consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos na LGPD.

**> Legítimo interesse**

• A base legal do legítimo interesse autoriza o tratamento de dados pessoais de natureza não sensível quando necessário ao atendimento de interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Trata-se, portanto, de base legal não aplicável ao tratamento de dados pessoais sensíveis.

• Por ser uma base legal mais frágil, sua adoção deve ser precedida de uma avaliação em que seja demonstrada a proporcionalidade entre, de um lado, os interesses do controlador ou de terceiro para a utilização do dado pessoal e, de outro, os direitos e as legítimas expectativas do titular.

• É preciso considerar também que o titular tem o direito de se opor ao tratamento realizado com base no legítimo interesse, em caso de descumprimento dos requisitos previstos na LGPD.

• No setor público, de forma similar ao que ocorre com o consentimento, a aplicação do legítimo interesse é limitada. Seu uso não é apropriado quando o tratamento de dados pessoais é realizado de forma compulsória ou quando for necessário para o cumprimento de obrigações e atribuições legais.

• A ANPD recomenda que, em geral, órgãos e entidades públicos evitem recorrer ao legítimo interesse, preferindo outras bases legais, a exemplo de execução de políticas públicas e cumprimento de obrigação legal, para fundamentar os tratamentos de dados pessoais que realizam nessas condições.

**No contexto das Companhias:**

Considerando a fragilidade do uso do legítimo interesse, a Codemge/Codemig desenvolveu um teste de proporcionalidade para verificar a adequada utilização dessa base legal. Nesse teste, são avaliadas a legitimidade e a necessidade do uso, bem como aplicada a regra de balanceamento e verificação de atendimento às salvaguardas.

**> Execução de políticas públicas**

• O conceito de políticas públicas não é definido na LGPD. A ANPD recomenda que ele seja interpretado de forma ampla, abrangendo qualquer programa/ação governamental, definido em instrumento formal (lei, regulamento ou ajuste contratual como contrato, convênio e instrumentos congêneres), cujo conteúdo inclui, em regra, objetivos, metas, prazos e meios de execução.

• No caso de envolver dados sensíveis, a base legal é mais restrita, sendo limitada a políticas públicas previstas em "leis e regulamentos".

• Deve-se observar o art. 23 da LGPD, em especial a exigência de que o tratamento seja realizado para o atendimento da finalidade pública, na persecução do interesse coletivo, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

**O tratamento de dados pessoais sensíveis poderá ser realizado quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.**

**Sem fornecimento de consentimento do titular, poderá ocorrer nas hipóteses em que for indispensável para:**

• cumprimento de obrigação legal ou regulatória pelo controlador;

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

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

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

• proteção da vida ou da incolumidade física do titular ou de terceiro;

• tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

• garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no artigo 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

## 10. DADOS DE CRIANÇA E DE ADOLESCENTE

Existe um regramento especial no caso de tratamento de dados pessoais de crianças e adolescentes. Esse tratamento deverá ser realizado em seu melhor interesse, observadas as proteções legais.

**Atenção!**

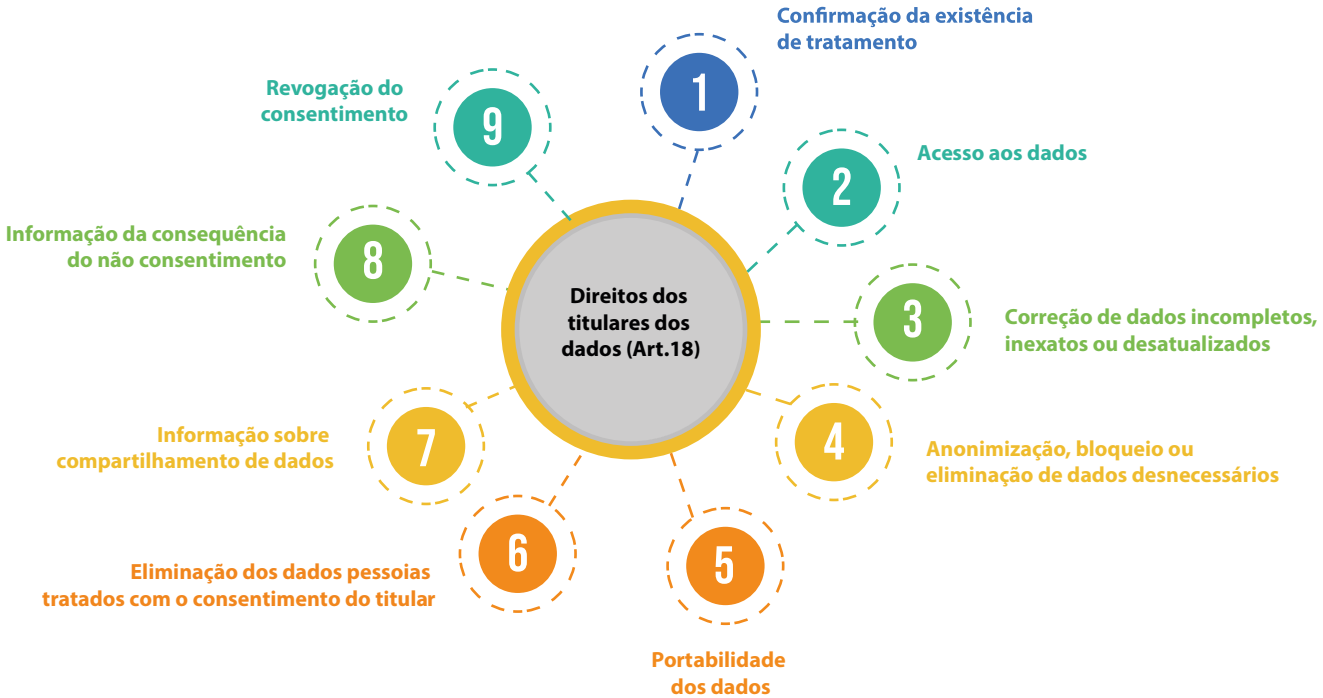
**O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.**

**Entretanto, poderão ser coletados dados pessoais de crianças sem esse consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento.**

# 11. DIREITOS DO TITULAR

Os direitos dos titulares de dados pessoais constam do artigo 18 da LGPD. Segundo a Lei, eles têm o direito de:

• Confirmar a existência de tratamento de dados pessoais;
• Acessar os dados pessoais;
• Corrigir os dados incompletos, inexatos ou desatualizados;
• Anonimização, bloqueio ou eliminação de dados (desnecessários, excessivos ou tratados em desconformidade com a LGPD);
• Portabilidade de dados a outro fornecedor de serviço ou produto, por intermédio de requisição expressa, com base na regulamentação da Agência Nacional de Proteção de Dados (ANPD);
• Eliminação dos dados pessoais tratados com o consentimento do titular (com exceção do artigo 16);
• Informação das entidades públicas e privadas com as quais os dados foram compartilhados;
• Informação sobre a possibilidade de não fornecer o consentimento e quais as implicações da negativa;
• Revogação do consentimento a qualquer tempo.



**No contexto das Companhias:**

**Qualquer colaborador da Codemge/Codemig que receber pedido enviado por titular que diga respeito ao tratamento de dados pessoais deve encaminhá-lo imediatamente a Comissão Interna de Privacidade, pelo endereço privacidade@codemge.com.br, conforme detalhado na IN 057 – Resposta a Pedidos da LGPD. A partir do recebimento do e-mail, o CIP analisará a solicitação e dará início aos procedi-mentos de resposta à ocorrência.**

## 12. A LGPD NO SERVIÇO PÚBLICO

A LGPD aplica-se aos setores público e privado.

O termo “poder público” é definido pela LGPD de forma ampla e inclui órgãos ou entidades dos entes federativos (União, Estados, Distrito Federal e Municípios) e dos três Poderes (Executivo, Legislativo e Judiciário), inclusive das Cortes de Contas e do Ministério Público, além das empresas públicas e as sociedades de economia mista. Assim, os tratamentos de dados pessoais realizados por esses entes devem observar as disposições da LGPD, ressalvadas as exceções previstas no artigo 4º da Lei (ver box abaixo).

No que se refere ao setor público, a aplicabilidade alcança qualquer órgão ou entidade pública, sociedades de economia mista e empresas públicas, nos termos do artigo 3º, da LGPD.

Na Administração Pública, busca-se estabelecer um equilíbrio entre a proteção de dados pessoais dos cidadãos e a elaboração de políticas públicas, assim como a prestação de serviços públicos.

Conforme o art. 7º, II, da LGPD, o tratamento de dados pessoais pelo poder público poderá ser realizado "para o cumprimento de obrigação legal ou regulatória pelo controlador". A mesma hipótese está prevista no art. 11, II, "a", que rege o tratamento de dados sensíveis.

**• Realizados por pessoa natural para fins exclusivamente particulares e não econômicos**

**• Para fins exclusivamente jornalísticos, artísticos ou acadêmicos**

**• Exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais**

**• Oriundos de fora do território nacional e que não sejam objeto de comunicação ou uso compartilhado de dados com agentes de tratamento do Brasil, nem objeto de transferência internacional de dados com país diferente do de proveniência, contanto que o país de proveniência garanta grau de proteção de dados pessoais adequado à LGPD**

**Obs.: os casos de tratamento de dados de segurança pública, embora não façam parte do escopo da LGPD, devem respeitar limitações de tratamento de dados para essas finalidades, conforme artigo 4º da Lei.**

## Poder público, transparência e privacidade

A Administração Pública costuma lidar diariamente com vários dados pessoais dos cidadãos – informações que podem ser fundamentais para a execução e a implementação de políticas públicas. Considerando que a relação entre Estado e cidadão é diferente da relação

entre empresa e indivíduo, a LGPD destinou um capítulo próprio à esfera pública (artigos 23 a 30).

Na maior parte das vezes, o tratamento de dados feito pelo poder público decorre do cumprimento de seus deveres constitucionais e legais.

A aplicação da LGPD ao tratamento de dados pessoais realizado pelo poder público traz o desafio de conciliar as regras e os princípios dispostos na LGPD com os princípios aos quais a Administração Pública está submetida, tais como a eficiência, a publicidade e o interesse coletivo, por exemplo.

**LGPD e LAI: como harmonizar**

Torna-se necessária a harmonização entre a LGPD, que busca assegurar a privacidade dos dados pessoais (esfera privada dos cidadãos), e a Lei de Acesso à Informação (LAI, (LAI, Lei nº 12.527/2011), cujo objetivo é garantir a transparência da gestão pública. A base legal da LAI é o princípio da publicidade disposto no artigo 37 da Constituição Federal de 1988.

Ao invés de se contradizerem, a LGPD e a LAI se complementam. A primeira vem proteger a privacidade dos cidadãos, e a segunda preserva o direito de informação da sociedade.

As disposições da LAI reforçam os direitos dos titulares previstos na LGPD no que tange ao acesso e à transparência. Dessa forma, os titulares poderão obter acesso aos dados pertinentes à sua pessoa, tratados pelas instituições públicas, bem como todas as informações relacionadas ao tratamento dos seus dados, numa espécie de "prestação de contas" ou *accountability*.

Aliás, o próprio conceito de dado pessoal constante da LGPD foi previsto inicialmente na LAI e indicado como informação pessoal (artigo 4º, Inciso IV), definida como "aquela relacionada à pessoa natural identificada ou identificável". A LGPD inovou, por exemplo, ao definir dado pessoal sensível.

Portanto, é necessária a responsabilidade do poder público na harmonização da transparência e da prestação de contas, com a proteção dos dados pessoais. A LGPD e a LAI incidem sobre campos distintos e podem ampliar e fortalecer o acesso à informação. Ambas as leis são essenciais à preservação de direitos fundamentais e das garantias do Estado Democrático de Direito.

**No contexto das Companhias:**

**As Companhias adotam como prática, na coordenação que realiza a gestão do acesso à informação – quando do atendimento a demandas referentes à Lei 12.527/2011, à Ouvidoria e ao Canal de Denúncias – , a anonimização de dados pessoais cujo acesso é dispensável para o atendimento da finalidade proposta.**

## Tratamento de dados no serviço público

As organizações públicas são as maiores detentoras de bases de dados pessoais, já que a relação entre o Estado e os cidadãos tem início com o nascimento do indivíduo e se mantém, inclusive, após a morte. Com a LGPD, a administração pública deve ter um cuidado ainda maior com os dados que irá publicar ao promover a transparência passiva ou ativa. O que pode ou não ser publicado, em situações que envolvam dados pessoais, deverá ser avaliado no caso concreto e justificado à luz das normas e princípios aplicáveis.

Em seu Capítulo IV, a LGPD dispõe sobre o tratamento de dados pessoais realizado pelo poder público. O artigo 23 estabelece as regras específicas para tanto. O tratamento de dados pessoais realizado pelas pessoas jurídicas de direito público deve buscar alcançar a finalidade e o interesse públicos, com o objetivo de executar/cumprir as competências e atribuições legais.

As empresas públicas e as sociedades de economia mista, que atuam em regime de concorrência, sujeitas ao disposto no artigo 173 da Constituição Federal de 1988, receberão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares (artigo 24 da LGPD).

Por outro lado, as empresas públicas e as sociedades de economia mista, quando operacionalizarem ou

executarem políticas públicas, receberão o mesmo tratamento conferido aos órgãos e entidades da esfera governamental.

O compartilhamento de dados pessoais pelo poder público deve respeitar os princípios da LGPD e atender às finalidades para execução de políticas públicas e alcance do interesse coletivo.

No artigo 11, parágrafo 4º, a lei veda a comunicação ou o uso compartilhado entre os controladores de dados pessoais sensíveis relacionados à saúde, com o intuito de obter vantagem econômica, salvo nas hipóteses relacionadas à prestação de serviços de saúde e à assistência farmacêutica, incluídos os serviços auxiliares de diagnose e terapia, em prol dos interesses dos titulares.

Outro aspecto importante é a inserção de cláusulas e atribuições de deveres e de responsabilidade nos contratos firmados pela administração pública, quando esses envolvam o tratamento de dados pessoais. Também deverá ser exigido pela Administração que a contratada adote política de proteção de dados em conformidade com a LGPD, entre outras medidas.

**Importante: o agente público que infrinja a LGPD também é passível de responsabilização administrativa pessoal e autônoma, conforme o art. 28 do Decreto Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro). Dessa forma, tratar dados pessoais indevidamente, como, por exemplo, vendendo banco de dados, alterando ou suprimindo cadastros de forma inadequada ou usando dados pessoais para fins ilegítimos pode levar à responsabilização do agente público que praticou o ato ilegal.**

**Atenção! O uso compartilhado de dados é um mecanismo relevante para a execução de atividades típicas e rotineiras do poder público. A LGPD reconhece essa importância ao estabelecer, em seu artigo 25, que os dados devem ser mantidos "em formato interoperável e estruturado para o uso compartilhado", visando, entre outras finalidades, "à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral".**

O uso compartilhado de dados pessoais pelo poder público deve ser formalizado, por meio de contratos, convênios ou instrumentos congêneres firmados entre as partes, ou ainda por decisão administrativa da autoridade competente, autorizando o acesso aos dados e estabelecendo os requisitos definidos como condição para o compartilhamento.

A ANPD recomenda a instauração de processo administrativo, do qual constem os documentos e as informações pertinentes, incluindo análise técnica e jurídica, conforme o caso, que exponham a motivação para a realização do compartilhamento e a sua aderência à legislação em vigor. Os dados pessoais a serem compartilhados devem ser indicados de forma objetiva e detalhada, limitando-se ao que for estritamente necessário para as finalidades do tratamento, em conformidade com o princípio da necessidade. Além disso, a finalidade deve ser específica, com vistas à execução de políticas públicas e à atribuição legal por órgãos públicos, respeitados os princípios de proteção de dados pessoais elencados no artigo 6º da LGPD.

Também é necessário que o instrumento que autoriza ou formaliza o compartilhamento estabeleça, de forma expressa, o período de duração do uso compartilhado dos dados,

além de esclarecer, conforme o caso, se há a possibilidade de conservação ou se os dados devem ser eliminados após o término do tratamento.

Exemplo:

A ANPD traz, como exemplo, um caso hipotético em que uma entidade financeira privada solicitou ao setor de recursos humanos de uma autarquia os dados de contato dos servidores para oferecer empréstimo consignado. O pedido foi negado pela autoridade competente, com base em análise técnica e jurídica, que concluiu pela impossibilidade de realização do compartilhamento dos dados, tendo em vista:

• a incompatibilidade entre a finalidade original da coleta e a finalidade proposta para o compartilhamento;

• a inexistência de base legal válida a amparar o uso compartilhado dos dados, em particular a inexistência de consentimentos dos titulares, de obrigação legal ou de qualquer vínculo com a execução de políticas públicas na hipótese;

• a vedação prevista no artigo 26, § 1º, da LGPD (segundo o qual é vedado ao poder público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, com as exceções previstas na Lei);

• o não enquadramento do caso em uma das exceções previstas nos incisos do mesmo dispositivo citado no item anterior.

| CUIDADOS A SEREM OBSERVADOS NA DIVULGAÇÃO DE DADOS PESSOAIS PELO PODER PÚBLICO | |
|---|---|
| **Parâmetros** | **Recomendações** |
| A coleta do dado pessoal é necessária e adequada para a finalidade do tratamento? | - Verificar a possibilidade de dispensa da coleta ou de eliminação dos dados pessoais, tendo em vista a sua efetiva necessidade para o alcance das finalidades do tratamento<br><br>- Verificar se há formas de atingir a finalidade almejada sem o tratamento de dados pessoais e de maneira menos gravosa para o titular de dados |
| A divulgação envolve dados pessoais sensíveis? | Em caso positivo, o tratamento deve ser efetuado com maior cautela, observando-se normas específicas, como os dispositivos da LGPD relativos a estudos em saúde pública |
| Quais medidas de mitigação de risco para o titular de dados podem ser adotadas? | - Elaboração de relatório de impacto à proteção de dados pessoais, caso necessário<br><br>- Medidas de prevenção e segurança, a exemplo de anonimização dos dados pessoais, sempre que isso não comprometa o exercício do controle social<br><br>- Limitação da divulgação aos dados necessários para alcançar a finalidade pretendida, observados o contexto, a finalidade e as expectativas legítimas dos titulares<br><br>- Transparência do tratamento<br><br>- Garantia de direitos dos titulares |

*Fonte: ANPD (Guia orientativo: tratamento de dados pessoais pelo poder público)*

# 13. SANÇÕES

Em caso de infrações cometidas às normas previstas na LGPD, os agentes de tratamento de dados estão sujeitos às seguintes sanções administrativas aplicáveis pela ANPD:

• Advertência, com indicação de prazo para adoção de medidas corretivas;
• Multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada a R$ 50 milhões por infração;
• Multa diária;
• Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
• Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
• Eliminação dos dados pessoais a que se refere a infração;
• Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
• Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período;
• Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

**Importante: a LGPD garantiu ao poder público tratamento diferenciado, inclusive no momento de fiscalização e aplicação de sanções. No caso da Administração Pública, o foco não está em multas, mas em advertência, publicização da infração e bloqueio do acesso aos dados, entre outras sanções específicas.**

## 14. BOAS PRÁTICAS DE GOVERNANÇA EM PROTEÇÃO DE DADOS

A regularidade do tratamento de dados depende da adoção de medidas de segurança, bem como dos princípios trazidos pela Lei Geral de Proteção de Dados Pessoais, em seu artigo 6º. A adequação extrapola a simples execução de ações pontuais e isoladas. Afinal, é preciso que todos se comprometam com estratégias para o gerenciamento e o monitoramento constantes de seus processos, pessoas e tecnologias.

O dever constitucional para a Administração Pública implica dupla dimensão: não intervir ou agir com excesso em relação às liberdades individuais e, de forma reflexa, atuar para garantir que os direitos dos cidadãos (titulares) sejam protegidos.

No caso da proteção dos dados pessoais, deve-se atuar com a finalidade de evitar riscos para os cidadãos em geral, por meio da adoção de medidas de proteção/prevenção.

Desse modo, considerados a natureza, o escopo, a finalidade, a probabilidade, a gravidade dos riscos e os benefícios relacionados ao tratamento dos dados do titular, a LGPD dispõe, em seu artigo 50, parágrafo 1º, que os agentes de

tratamento poderão formular ou aderir a regras de boas práticas e governança que, dentre outros aspectos, estabeleçam as condições de organização, o regime de funcionamento e os procedimentos, incluindo reclamações e petições de titulares, normas de segurança, padrões técnicos, obrigações específicas, ações educativas, mecanismos de supervisão e de mitigação de riscos.

**Você sabia?**

**Para adequação à LGPD, algumas ações básicas são necessárias, como: mapeamento de dados, programa de governança em proteção de dados, avaliação dos riscos e disseminação da cultura de proteção de dados na entidade.**

## 15. LGPD NA PRÁTICA: 30 CONDUTAS DO AGENTE PÚBLICO RELACIONADAS À PROTEÇÃO DE DADOS

1. Ao tratar dados pessoais (independentemente de a quem pertençam, como foram obtidos ou onde são armazenados), observe as normas aplicáveis, bem como as políticas, normas, orientações e boas práticas adotadas pelas Companhias;

2. Use apenas meios seguros e legais ao tratar dados pessoais;

3. Certifique-se de tratar dados pessoais apenas para fins legítimos e restritos à finalidade pública e ao interesse público, ou seja, para cumprimento de competências legais, atribuições do serviço público ou de políticas públicas;

4. Busque usar dados pessoais com qualidade, ou seja, exatos e atualizados, protegendo-os com cuidado;

5. Não colete informações desnecessárias;

6. Trate dados apenas na medida necessária para realização do serviço de sua atribuição;

7. Reduza os riscos relacionados à segurança da informação;

8. Ao tomar ciência de uma falha de segurança, reporte ao setor competente;

9. Seja cuidadoso ao discutir assuntos que envolvam dados pessoais com indivíduos de fora da instituição;

10. Evite conversas em locais públicos ou de uso coletivo (elevadores, corredores, refeitórios, banheiros) que tenham como objeto dados pessoais;

11. Não use dados pessoais desatualizados ou inexatos;

12. Previna a perda acidental ou destruição de dados pes-soais;

13. Evite o acesso não autorizado aos dados controlados pela Codemge/Codemig;

14. Limite o acesso aos dados pessoais apenas aos agen-tes que necessitem deles para as atividades da administra-ção pública na Companhia;

15. Reporte a Comissão Interna de Privacidade a ocorrên-cia de violações à LGPD ou de incidentes envolvendo dados pessoais;

16. Não envie e-mails para pessoas ou grupos além do necessário e se atente para quem você irá enviar o e-mail ou cópia da mensagem quando houver dados pessoais;

17. Não deixe documentos com dados pessoais na im-pressora, na sua mesa ou em outro local onde outros pos-sam ver;

18. Não deixe a tela do seu computador aberta com da-dos pessoais quando você não o estiver utilizando;

19. Verifique a existência de salvaguardas quando for compartilhar dados com terceiros;

20. Não tire fotos nem filme documentos que contenham dados pessoais;

21. No desenvolvimento de novos sistemas, processos ou procedimentos que envolvam o tratamento de dados pessoais, adote medidas de proteção de dados desde a concepção até a execução;

22. Proceda à correção de dados pessoais que estejam imprecisos, incorretos ou incompletos;

23. Garanta que os titulares dos dados tenham a possibilidade de revisar e corrigir seus dados pessoais;

24. Em conformidade com normas específicas, guarde os dados apenas pelo tempo necessário e forneça explicações ao titular sobre a utilização dos dados, quando solicitado;

25. Elimine os dados pessoais que não tenham mais justificativa para serem mantidos e tratados pela Companhia, sempre observando as orientações da chefia imediata e do responsável pelo tratamento de dados, bem como as normas e os regulamentos internos;

26. Realize a troca periódica da sua senha de acesso, usando uma sequência forte e exclusiva para os sistemas da Companhia e tendo o cuidado de não a compartilhar;

27. Utilize a função de “bloqueio” quando se ausentar da sua estação de trabalho, de modo a não deixar a tela do computador aberta/exposta em sua ausência;

28. Não abra e-mails suspeitos, quando houver dúvida quanto à origem deles;

29. Não poste em redes sociais dados pessoais e sensíveis de terceiros;

30. Não forneça dados pessoais por e-mail, telefone ou outro canal inapropriado, de modo a limitar o acesso aos dados apenas para os agentes que necessitem deles para as atividades da administração pública.

**Importante: colete apenas as informações necessárias e realize o tratamento de dados na medida de suas atribuições. A rastreabilidade dos acessos indicará o responsável em caso de tratamento inadequado ou em desconformidade com a LGPD. Lembre-se de que, ao tratar os dados pessoais em conformidade com a LGPD, você está cumprindo o direito fundamental à proteção dessas informações.**

# 16. CODEMGE/CODEMIG E SUAS CONTRATADAS: JUNTAS NA PROTEÇÃO DE DADOS PESSOAIS

A Codemge/Codemig explicitam, junto a suas contratadas, diretrizes relacionadas à LGPD e à proteção de dados pessoais, as quais deverão ser aplicadas a toda e qualquer atividade que envolva a contratação e a execução do objeto contratado. Confira, a seguir, os principais pontos estabelecidos.

1. As partes se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais e se obrigam, sempre que cabível, a atuar no contrato em conformidade com a legislação vigente sobre proteção de dados pessoais e as determinações de órgãos reguladores/fiscalizadores.

2. Quando necessário para a execução do contrato, as partes poderão realizar tratamento de dados pessoais, desde que amparadas por uma das hipóteses legais previstas na LGPD. O tratamento será limitado às atividades necessárias às finalidades de execução do contrato e/ou do serviço con-tratado, sendo vedado o tratamento de forma incompatível com as finalidades e prazos acordados.

3. Os dados pessoais não poderão ser revelados a terceiros, direta ou indiretamente, nem mediante a distribuição de cópias, resumos, compilações, extratos, análises, estudos ou outros meios que contenham ou reflitam essas informações, com exceção da prévia autorização por escrito da Codemge/Codemig e das hipóteses permitidas pelo art. 7º da LGPD.

4. Caso a contratada seja obrigada, por determinação legal ou judicial, a fornecer dados pessoais a uma autoridade pública, deverá informar previamente à Codemge/ Codemig, para que a Companhia tome as medidas que julgar cabíveis.

5. Se estiver atuando como operadora de dados pessoais, a contratada realizará o tratamento dos dados transmitidos pela Companhia nos limites e na forma definidos em contrato, ressalvadas as hipóteses em que a contratada for co-controladora dos dados pessoais.

6. A contratada deverá guardar sigilo sobre os dados pessoais compartilhados pela Codemge/Codemig e não poderá realizar qualquer atividade de tratamento de dados em nome da Companhia, atuando como operadora, sem consentimento prévio e expresso.

7. Em caso de subcontratação, a subcontratada somente poderá realizar tratamento de dados em nome da Codemge/Codemig quando expressamente autorizado pela Companhia e em atendimento às finalidades determinadas.

8. Encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sensíveis ou não, a contratada interromperá o tratamento dos dados pessoais realizado no âmbito do contrato, em no máximo 30 dias, sob instruções e na medida do determinado pela Codemge/Codemig. Além disso, eliminará completamente os dados pessoais e todas as cópias porventura existentes (em formato digital ou físico), salvo quando a contratada tenha que manter os dados para cumprimento de dever legal ou outra hipótese da LGPD.

9. A contratada dará conhecimento formal aos seus empregados das obrigações e condições acordadas, inclusive

quanto à Política de Privacidade da Codemge/Codemig, cujos princípios deverão ser aplicados à coleta e ao tratamento dos dados pessoais.

10. A contratada cooperará no atendimento às obrigações referentes ao exercício dos direitos dos titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e no atendimento de requisições e determinações do Poder Judiciário, Ministério Público, Órgãos de controle administrativo.

11. A contratada deverá informar imediatamente à Companhia quando receber uma solicitação de titular sobre seus dados pessoais, bem como deverá abster-se de responder qualquer solicitação em relação aos dados pessoais do so-licitante, exceto nas instruções documentadas da Companhia ou conforme exigido pela LGPD e Leis e Regulamentos de Proteção de Dados em vigor.

12. A critério do encarregado de dados da Codemge/ Codemig, a contratada poderá ser provocada a colaborar no atendimento à solicitação de titular, conforme a sensibilidade e o risco inerente dos serviços objeto do contrato, no tocante a dados pessoais.

13. A Companhia terá o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade da contratada, diante das obrigações de operador, para a proteção de dados pes-soais referentes à execução do contrato.

14. Os contratos, em geral, não transferem a propriedade de quaisquer dados da Codemge/Codemig para a contratada.

15. As partes ficam obrigadas a indicar “encarregado” pela proteção de dados pessoais, ou preposto, para eventual

comunicação sobre os assuntos pertinentes à LGPD, que gerem impacto ao objeto e à vigência do contrato. O tratamento será limitado às atividades necessárias ao atingimento das finalidades de execução do contrato e/ou do serviço contratado.

16. O encarregado da contratada manterá contato formal com o encarregado da Codemge/Codemig, no prazo de 24 horas da ciência da ocorrência de qualquer incidente que implique violação ou risco de violação de dados pessoais e que gere impacto ao objeto e à vigência do contrato, a fim de que se adotem as providências devidas, na hipótese de questiona-mento das autoridades competentes.

17. A critério do encarregado de dados da Codemge/Codemig, a contratada poderá ser provocada a colaborar na elaboração do Relatório de Impacto à Proteção de Dados (RIPD ou, na sigla em inglês, DPIA – *Data Protect on Impact Assessment*), conforme a sensibilidade e o risco inerente dos serviços ob-jeto do contrato, no que se refere a dados pessoais.

18. Eventuais responsabilidades das partes serão apuradas conforme estabelecido no contrato e de acordo com o que dispõe a Seção III, Capítulo VI da LGPD.

# 17. CONSIDERAÇÕES FINAIS

De acordo com a ANPD, a coleta indiscriminada de dados pessoais é, muitas vezes, o ponto principal a ser considerado. Desse modo, ao invés de eventual e posterior atribuição de sigilo, a proteção será mais efetiva com a própria dispensa da coleta ou com a eliminação da informação desnecessária.

Há situações, porém, em que a coleta é necessária, e não é cabível a eliminação dos dados. Mesmo assim, é importante adotar medidas de mitigação de risco e prevenção de danos, tornando mais segura a possibilidade de divulgação dos dados pessoais e reduzindo o potencial lesivo aos direitos dos titulares. Tais medidas podem, inclusive, ser descritas em relatório de impacto à proteção de dados pessoais, documento do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

A ANPD destaca que uma possível salvaguarda a ser adotada é a limitação da divulgação aos dados efetivamente necessários para se alcançar os propósitos legítimos e específicos em causa, observados o contexto do tratamento e as expectativas legítimas dos titulares.

Nesse sentido, por exemplo, em cumprimento a uma decisão proferida pelo Supremo Tribunal Federal, a divulgação da remuneração individualizada de servidores públicos federais é realizada sem a apresentação completa de números como o CPF e a matrícula do servidor, bem como sem endereços residenciais. Segundo a ANPD, a restrição de acesso a essas informações mitiga os riscos aos titulares de dados pessoais, sem, contudo, comprometer a finalidade de garantia de transparência e de controle social sobre as despesas públicas. O contexto e as expectativas legítimas dos titulares também são relevantes, à medida que se entende, como uma decorrência natural do exercício da atividade pública, que determinadas informações pessoais dos servidores se submetam ao escrutínio da sociedade.

A ANPD salienta também a boa prática de realizar o tratamento de dados pessoais levando em conta a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados. Entre outras medidas, sempre que possível, os dados pessoais devem ser pseudonimizados ou anonimizados.

Concluindo, a LGPD veio estabelecer ampla proteção aos dados pessoais, inclusive para aqueles cujo acesso é público, seja por força de lei, seja por manifestação de vontade do titular.

# REFERÊNCIAS


ANPD. Guia orientativo: tratamento de dados pessoais pelo poder público (versão 1.0, jan. 2022). Disponível em: < https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 5 mai. 2023.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 11 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#art65>. Acesso em: 11 abr. 2023.

MINISTÉRIO PÚBLICO DO RIO GRANDE DO SUL. Cartilha LGPD MPRS. Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018. Disponível em: <https://www.mprs.mp.br/media/areas/lgpd/arquivos/cartilha_lgpd.pdf>. Acesso em: 11 abr. 2023.

PREFEITURA DE JUIZ DE FORA. Cartilha LGPD. Disponível em: <https://www.pjf.mg.gov.br/secretarias/cgm/lgpd/arquivos/cartilha-lgpd.pdf>. Acesso em: 11 abr. 2023.

PREFEITURA DE PORTO ALEGRE. O que muda no seu trabalho com a Lei Geral de Proteção de Dados. Disponível em: <https://prefeitura.poa.br/sites/default/files/usu_doc/cartadeservicos/Cartilha%20Lei%20Geral%20de%20Protec%CC%A7a%CC%83o%20de%20Dados%20-%20para%20distribuic%CC%A7a%CC%83o.pdf>. Acesso em: 11 abr. 2023.

Comissão Interna de Privacidade –
CIP privacidade@codemge.com.br

Facebook: /Codemge
Instagram: @codemge
LinkedIn: Codemge

www.codemge.com.br