

CARTILHA LGPD

**LEI GERAL
DE PROTEÇÃO DE DADOS PESSOAIS**



UNIDADE DE TRATAMENTO DE DADOS PESSOAIS

Marcus Vinícius Sousa Ventura
Encarregado de Tratamento de Dados Pessoais

Thaderson Diorge Silva Duarte
Técnico Administrativo Substituto do Encarregado de
Tratamento de Dados Pessoais

ESCOLA SUPERIOR DA DEFENSORIA PÚBLICA

Diretor da Escola Superior da Defensoria Pública de Mato
Grosso
Fernando Antunes Soubhia

PROJETO GRÁFICO E DIAGRAMAÇÃO

Alessandro Moura Batista
Estagiário de Comunicação Social Habilitado em Publicidade
e propaganda da Escola Superior da Defensoria Pública de
Mato Grosso

Supervisora de Estágio
Damaris Lara da Costa
Secretária da Escola Superior da Defensoria Pública de Mato Grosso

Su má rio

07

Abrangência
e Aplicabilidade
da LGPD

04

Apresentação

10

Conceitos Importantes
da LGPD

06

Quais as principais leis
que se comunicam com
a LGPD?

40

Quais os Princípios da
LGPD?

42

E os dados pessoais sobre crianças, adolescentes e idosos?

43

O que é o Inventário de Dados Pessoais (IDP)?

44

O que é o Relatório de Impacto à Proteção de Dados Pessoais (RIPD)?

46

O que é Incidente de Segurança?

47

Quanto à Lei de Acesso à Informação (LAI) e LGPD?

50

O que é a Agência Nacional de Proteção de Dados – ANPD?

57

Referências Bibliográficas

Apresentação

O advento da Lei Geral de Proteção de Dados - LGPD, Lei nº 13.709, de 14 de agosto de 2018, tendo o seu pleno vigor a partir de 1º de agosto de 2021, representou um marco em proteção de dados pessoais no Brasil, haja vista que até então existiam algumas normas fragmentadas (Lei Nº 12.965 de 23 de abril de 2014 – Marco Civil da Internet e Lei Nº 8.078 de 11 de setembro de 1990 – Código de Defesa do Consumidor).

Nota-se que esse tema vem cada vez mais se tornando relevante e impactando a vida das pessoas e das organizações públicas e privadas no Brasil e internacionalmente.

São **objetivos** da “Cartilha LGPD”:

- a) introduzir, no âmbito da Defensoria Pública do Estado de Mato Grosso, o assunto de forma simplificada, clara e didática;
- b) elucidar as principais bases legais e fundamentos norteadores da Lei Geral de Proteção de Dados Pessoais Brasileira;
- c) esclarecer sobre a abrangência e aplicabilidade da LGPD;

- d) informar os conceitos principais, a fim de nortear a atuação de todos os que realizam tratamento de dados;
- e) informar sobre os princípios da LGPD;
- f) informar sobre o tratamento de dados pessoais de crianças, adolescentes e idosos;
- g) esclarecer o processo de inventariar dados pessoais e indicar os agentes envolvidos e o ciclo de vida dos dados pessoais;
- h) explicar a aplicação do Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
- i) elucidar o que é incidente de segurança;
- j) esclarecer sobre a Lei de Acesso à Informação e LGPD;
- k) explicar sobre as competências da Agência Nacional de Proteção de Dados;
- l) fortalecer a cultura de privacidade e proteção de dados na DPEMT;
- m) incentivar ações de governança e boas práticas em privacidade e proteção de dados na DPEMT.

Quais as principais leis que se comunicam com a LGPD?

Algumas das principais bases legais que interagem no escopo da privacidade e proteção de dados pessoais no âmbito brasileiro são:

- a) Constituição Federal de 1988 – especialmente o art. 5º, X e LXXIX;
- b) Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) – especialmente os arts. 6º, III; e 31;
- c) Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor) – especialmente os arts. 43, § 1º, § 2º, § 3º, § 6º; e 54-D, II;
- d) Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet no Brasil) – especialmente os arts. 3º, II e III; 8º; 11; e 16, II;
- e) Lei nº 15.211, de 17 de setembro de 2025 (Estatuto Digital da Criança e do Adolescente) – especialmente os arts. 3º; 7º; 13; 16; 22; e 26.



[Clique Aqui](#)

LGPD



[Clique Aqui](#)

Constituição Federal



[Clique Aqui](#)

Lei de Acesso à Informação



[Clique Aqui](#)

Código de Defesa do Consumidor



[Clique Aqui](#)

Marco Civil da Internet no Brasil



[Clique Aqui](#)

Estatuto Digital da Criança e do Adolescente

Abrangência e Aplicabilidade da LGPD

2.1 Quando se aplica a LGPD?

Segundo o seu art. 3º, a LGPD se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

1. a operação de tratamento seja realizada no território nacional;
2. a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
3. os dados pessoais objeto do tratamento tenha sido coletados no território nacional.

Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Exemplos Práticos de Aplicação (Art. 3º)

Dispositivo Legal	Hipótese / Exemplo Prático	Por que se aplica?
Inciso I (Tratamento no Brasil)	Uma padaria em Belo Horizonte que coleta nome e CPF de clientes para um programa de fidelidade.	A operação de tratamento (coleta e armazenamento) ocorre fisicamente em território nacional.
Inciso II (Oferta de bens ou serviços)	Uma plataforma de streaming sediada nos EUA que oferece assinaturas em Reais (R\$) e tem interface em português para o público brasileiro.	Mesmo sem sede no Brasil, a empresa visa claramente o mercado nacional e oferece serviços a residentes locais.
Inciso II (Tratamento de indivíduos no Brasil)	Uma empresa de publicidade europeia que rastreia o comportamento de navegação de usuários que estão em Curitiba para exibir anúncios direcionados.	O objetivo é tratar dados de indivíduos que estão localizados no Brasil no momento do tratamento.
Inciso III (Coleta em território nacional)	Um turista francês visitando o Rio de Janeiro que baixa um aplicativo de guia turístico e faz um cadastro enquanto caminha por Copacabana.	Conforme o § 1º, os dados são considerados coletados no Brasil porque o titular estava aqui no momento da coleta.

(Fonte: Gemini. Revisado e Adaptado em 30/01/2026)

2.2 Quando Não se aplica a LGPD?

ALGPD não se aplica ao tratamento de dados pessoais (art. 4º da LGPD):

1. realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

2. realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a este os arts. 7º e 11 da LGPD (hipóteses de tratamento acerca de dado pessoal comum e sensível);

3. realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

4. provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

Atenção! A LGPD não se aplica à dados de pessoas jurídicas (de forma direta), nem a dados anonimizados[1] de pessoas naturais.

Categoria / Inciso	O que diz a regra?	Exemplos Práticos
1. Particular e Não Econômico (I)	Uso pessoal, sem fins lucrativos ou comerciais.	<ul style="list-style-type: none"> • Agenda de contatos no celular. • Fotos de família em redes sociais privadas. • Lista de convidados para aniversário.
2. Jornalístico e Artístico (II, a)	Proteção à liberdade de expressão e de imprensa.	<ul style="list-style-type: none"> • Matéria sobre corrupção política. • Produção de documentários ou filmes. • Escrita de biografias autorizadas ou não.
3. Fins Acadêmicos (II, b)	Pesquisa científica e acadêmica (deve-se buscar a anonimização).	<ul style="list-style-type: none"> • Entrevistas para TCC ou Teses. • Estudos estatísticos universitários sobre a população.
4. Segurança e Defesa (III)	Atividades de repressão criminal e soberania nacional.	<ul style="list-style-type: none"> • Reconhecimento facial policial. • Inteligência militar para defesa nacional. • Acesso policial a dados cadastrais bancários.
5. Dados de Origem Estrangeira (IV)	Dados que apenas "transitam" ou são processados no Brasil sem uso nacional.	<ul style="list-style-type: none"> • Empresa estrangeira que usa servidor no Brasil para dados de clientes que não vivem aqui.

(Fonte: Gemini. Revisado e Adaptado em 30/01/2026)

[1] quando o titular não pode ser identificado, após a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento

Conceitos Importantes da LGPD

3.1 O que é dado pessoal?

Informação relacionada a pessoa natural identificada ou identificável (art. 5º, I, da LGPD).

3.1.1 E os 04 (quatro) pilares do dado pessoal?

Segundo o Guia de Boas Práticas LGPD da Administração Pública Federal (2020), o conceito de dado pessoal é composto por 04 (quatro) pilares, vejamos:

a) Informação:

Pode ter natureza objetiva (ex. idade) ou subjetiva (ex. o devedor X é confiável).

b) Relacionada a:

Um dado pode ser considerado relacionado a um indivíduo se ele diz respeito a um dos seguintes critérios:

- i) se relaciona a um conteúdo sobre o indivíduo;
- ii) tem a finalidade de avaliar um indivíduo ou seu comportamento; ou
- iii) tem um impacto sobre interesses ou direitos do indivíduo.



c) Pessoa natural:

Para ser pessoal, a informação deve estar relacionada a um indivíduo humano vivo.

d) Identificada ou identificável:

i) identificada: significa que a ligação ao indivíduo é feita de forma direta, como pelo tratamento de seu nome completo, fotografia, biometria, entre outros

ii) identificável: a ligação é indireta, e um processo de cruzamento de dados pode ser necessário para a identificação. Isto contudo não elimina a caracterização do dado como dado pessoal. É o caso de identificadores como: RG, CPF, endereço e telefone de uma pessoa natural.

3.1.2 São exemplos de dados pessoais:

Nome, sobrenome;
Número de documentos de identificação pessoal (RG, CPF, título de eleitor,
CNH, matrícula etc.);
Endereço residencial e telefone celular pessoal ou residencial;
Carteira funcional, passaporte;
Estado civil, data de nascimento e e-mail pessoal;
Informação financeira e patrimonial pessoal;
Placa de automóvel (quando relacionado a uma pessoa natural);
Cookie/Log (endereço IP + hora de acesso);
Internet Protocol (IP);
Hábito de navegação isolado;
Conjunto de Hábitos de navegação;
Posição geolocacional;
Conjunto de características pessoais;
Interesses, preferências, formação do perfil comportamental;
E-mail corporativo;
Entre outros.

Atenção! Importante frisar que a lista acima destacada trata de um rol exemplificativo, e não taxativo. Portanto, outros dados podem ser relacionados a pessoa natural de maneira direta ou indireta, e dessa forma serem classificados como dados pessoais.

Os dados pessoais tornados manifestamente públicos pela própria pessoa natural não deixam de ser protegidos pela LGPD. O tratamento desses dados deve respeitar os direitos e as legítimas expectativas da pessoa titular, além de observar os princípios previstos na LGPD, tais como finalidade, adequação, necessidade e transparência.

3.2 O que é dado pessoal sensível?

Dado relacionado a pessoa natural 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 (art. 5º, II, da LGPD).

Essa classificação se justifica, pois os dados pessoais sensíveis implicam em riscos, prejuízos e vulnerabilidades maiores aos direitos e liberdades fundamentais dos titulares, no caso de tratamentos indevidos, em razão do maior potencial discriminatório ou do nível de criticidade (identificação inequívoca do indivíduo).

A partir de uma interpretação literal e isolada do art. 5º, inciso II, da LGPD, entende-se que o rol (lista) dos dados pessoais sensíveis é taxativo (restritivo). Ou seja, a lei estabeleceu uma lista determinada, sem margem para ampliações desse conceito. Assim, só seria considerado dado pessoal sensível aquele que estiver inserido na relação. Esse posicionamento, permite mais clareza e limites bem definidos para a interpretação e aplicação da lei.

Atenção! Existem correntes doutrinárias que consideram que os dados pessoais sensíveis classificados no art. 5º, II, da LGPD, podem ser interpretados de maneira extensiva. Ou seja, não restrita ao rol descrito no dispositivo legal supracitado. Esse entendimento se fundamenta no art. 11, §1º, da LGPD: “dado que possa representar algum tipo de discriminação, vulnerabilidade ou revelar dado sensível, deve ser tratado como dado sensível”. Assim essa interpretação classifica como sensíveis todos os dados pessoais que de alguma forma possam discriminar, vulnerabilizar ou revelar dados sensíveis do titular desses dados.

Nesse sentido, citamos: “diante dos fundamentos da categoria dos dados sensíveis, da proteção de dados pessoais ser considerada um direito da personalidade e de sua natureza relacionada diretamente a aspectos existenciais da pessoa humana, entende-se que o rol de dados sensíveis na LGPD deve ser considerado exemplificativo, sendo tutelado de forma ampla e contextualizada” (TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. Indaiatuba: Foco, 2022. p. 67. Resenha de: FALEIROS JÚNIOR, José Luiz de Moura. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 32, n. 2, p. 331-339, abr./jun. 2023.).

3.2.1 São exemplos de dados pessoais sensíveis:

a) Clarice (nome fictício) é portadora do RG de número 0000000-0, é cristã, de origem espanhola, mora em Cuiabá e gosta de jogar xadrez.

Nesse caso hipotético, o fato de ser **cristã** e de origem **espanhola** é o que caracteriza “dados pessoais sensíveis” pela Lei Geral de Proteção de Dados Pessoais – LGPD.

CATEGORIA	Exemplo Prático do Dia a Dia
Saúde	O prontuário médico em um hospita, uma receita de remédio controlado ou um atestado médico ou laudo médico.
Biometria	A sua digital para bater o ponto no trabalho ou o reconhecimento facial para desbloquear o aplicativo do banco.
Vida Sexual	A informação de que um paciente faz uso de algum tipo de medicamento de prevenção ao HIV ou dados de orientação sexual em uma pesquisa de RH.
Origem Racial/Étnica	A autodeclaração de cor/raça em um formulário de matrícula escolar ou em uma pesquisa de Rh.
Opinião Política	O registro de filiação a um partido político ou a participação oficial em um movimento de militância.
Convicção Religiosa	O registro de pagamento de dízimo em uma igreja ou a declaração de que não trabalha aos sábados por motivos religiosos.
Dados genéticos	O resultado de um teste de ancestralidade ou exame de DNA

3.3 O que é Dado Anonimizado?

É o dado relativo ao titular que **não possa ser identificado**, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (art. 5º, III, da LGPD).

O objetivo da anonimização é afetar os identificadores presentes em um dado ou conjunto de dados, de modo que se perca a possibilidade de associação direta ou indireta a um determinado indivíduo.

Os dados anonimizados não serão considerados dados pessoais para os fins da LGPD, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido (art. 12, da LGPD).

Atenção! Anonimização é a utilização 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 (art. 5º, XI, da LGPD).

Imagine um conjunto de dados de prontuários médicos para uma pesquisa sobre diabetes:

<u>Nome Completo</u>	<u>Data de Nascimento</u>	<u>Cidade</u>	<u>Tipo Sanguíneo</u>	<u>Diagnóstico</u>
João Carlos Pereira	15/05/1982	Cuiabá	A+	Diabetes Tipo 2
Ana Beatriz Lima	23/09/1995	Várzea Grande	O-	Diabetes Tipo 1
Ricardo Souza	07/01/1984	Rondonópolis	B+	Diabetes Tipo 2

Para anonimizar esses dados, poderíamos aplicar as seguintes técnicas:

1. **Generalização:** Em vez de dados específicos, usamos categorias mais amplas.

A data de nascimento vira uma faixa etária (ex: 35-45 anos).

A cidade específica vira uma região (ex: Microrregião de Cuiabá).

2. **Supressão ou Remoção:** Informações diretamente identificadoras são completamente removidas.

O Nome Completo é totalmente apagado.

3. **Randomização ou Perturbação:** Adicionamos um "ruído" estatístico aos dados para que eles não sejam exatos, mas ainda úteis para análises agregadas.

Poderíamos alterar levemente a data exata do diagnóstico, mantendo o mês e o ano, para dificultar o cruzamento com outras bases de dados.

O resultado anonimizado seria algo assim:

<i>Faixa Etária</i>	<i>Região</i>	<i>Tipo Sanguíneo</i>	<i>Diagnóstico</i>
40-50 anos	Microrregião de Cuiabá	A+	Diabetes Tipo 2
25-35 anos	Microrregião de Cuiabá	O-	Diabetes Tipo 1
40-50 anos	Microrregião de Rondonópolis	B+	Diabetes Tipo 2

Neste novo formato, é praticamente impossível saber que a primeira linha se refere a João Carlos Pereira. O dado se tornou estatístico e perdeu seu caráter pessoal.

Atenção! Não confunda a técnica de anonimização com o mascaramento (tarjamento de parte do número do CPF, por exemplo).

As técnicas de mascaramento, nas quais apenas partes dos dados são ocultadas (ex: 4999-XXXX-XXXX-9999) não são suficientes para a anonimização, pois ainda podem permitir a reidentificação ou o "single out" (isolar um indivíduo no conjunto de dados). O mascaramento é uma técnica de ofuscação ("data obfuscation"), distinta da anonimização formal. Por sua natureza potencialmente reversível e por manter a estrutura original, o mascaramento não se adequa ao conceito legal de anonimização. Portanto, um dado mascarado ainda é um dado pessoal sob o olhar da LGPD.

Assim, podemos concluir que o mascaramento de dados é uma ferramenta de segurança para reduzir riscos, enquanto a anonimização é um processo de transformação de dados para eliminar a identidade pessoal de forma permanente. Dessa forma, o mascaramento está mais próximo da pseudonimização, do que de uma efetiva anonimização.

3.3.2 O que é Pseudonimização?

A pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, **senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro** (art. 13, § 4º, da LGPD).

É um conceito próximo ao de anonimização de dados, mas com ele não se confunde. Em ambos os casos ocorre a desidentificação (ação que consiste na perda da identidade) de identificadores diretos. Na pseudonimização, o controlador mantém um banco de dados separado e em ambiente seguro, no qual existem informações adicionais, que possibilitam a identificação direta ou indireta do indivíduo. Nesse contexto, banco de dados é entendido como um conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Em outras palavras, a pseudonimização é uma técnica de segurança que embaralha os dados de alguém para que não seja possível saber de quem são apenas olhando para eles. É como dar um apelido secreto aos dados. Você só descobre o "nome verdadeiro" se tiver a lista que liga o apelido ao nome, e essa lista fica muito bem protegida.

Imagine que você tem uma lista com nomes e idades de pessoas (exemplo: João Silva, 23 anos). Com a pseudonimização, o nome "João Silva" poderia virar um código, como "ABC123". Nessa situação, o dado principal ("ABC123") não revela quem é a pessoa. Para descobrir que "ABC123" é o João Silva, você precisaria de uma "chave" ou informação extra. Essa "chave" fica guardada em um lugar separado e seguro, para que ninguém consiga fazer a ligação facilmente.

Assim, como na pseudonimização não há uma anonimização de fato, o dado pseudonimizado ainda é considerado um dado pessoal e se mantém sob a proteção da LGPD.

3.4 Quem é o Titular de Dados Pessoais?

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, V, da LGPD).

Na DPEMT, os titulares podem ser **cidadãos** (assistidos e público externo em geral) que utilizam os serviços da Defensoria. Os dados pessoais deles são tratados pela área finalística (Núcleos da DPEMT) para que as petições iniciais sejam elaboradas, por exemplo.

Os titulares, na Defensoria, também podem ser os **prestadores de serviços contratados** (terceirizados), **membros, servidores e estagiários**. Os dados deles são tratados, por exemplo, pelas áreas de licitação, contratos, gestão de pessoas, financeiro, etc.

3.4.1 Quais são os direitos dos Titulares?

Entre os direitos dos titulares previstos pela LGPD, destacam-se (art. 18):

1. o direito de ter acesso aos próprios dados pessoais;
2. de ter a confirmação pelo controlador da existência de tratamento dos dados pessoais;
3. correção de dados pessoais incompletos, inexatos ou desatualizados;
4. anonimização, bloqueio ou eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a Lei;
5. portabilidade dos dados pessoais;
6. eliminação dos dados pessoais;
7. informação das entidades públicas e privadas que realizaram o compartilhamento de dados pessoais;
8. informação sobre a possibilidade de o titular não fornecer consentimento e as consequências dessa negativa, e
9. a possibilidade de revogação do consentimento.

3.5 Quem é o Controlador?

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI, da LGPD).

Importante frisar que o controlador possui autonomia decisória quanto a fins (finalidade) e meios (forma) de tratamento.

Na maioria das vezes, o controlador será uma pessoa jurídica, seja de direito privado, seja de direito público. É o que ocorre, por exemplo, quando sociedades empresárias ou entidades públicas tomam as principais decisões a respeito do armazenamento, da eliminação ou do compartilhamento de informações que integram um banco de dados pessoais que é gerido no âmbito da organização.

A título de exemplificação, no caso da DPEMT, o controlador é o Estado de Mato Grosso. Todavia, a DPEMT representa o Controlador dos dados pessoais tratados na realização de suas atividades legais e constitucionais, seja nas áreas administrativa ou finalística. O art. 20 da Política de Privacidade e Proteção de Dados Pessoais (PPPD) da DPEMT (Resolução nº 17/2025/DPG) formaliza essa definição.

Atenção! Não são controladoras as pessoas naturais que atuam como profissionais subordinados a pessoa jurídica. Ou seja, na DPEMT, os membros, servidores e estagiários não são controladores de dados pessoais. A definição de controlador não deve ser entendida como uma norma de distribuição interna de competências e responsabilidades.



3.5.1 E as Responsabilidades do Controlador?

Essas são algumas das responsabilidades do controlador delineadas na LGPD:

- a) Definir a base legal de tratamento (arts. 7º e 11);
- b) Manter registro das operações de tratamento (art. 37);
- c) Informar e prestar contas; garantir a portabilidade (arts. 9º; 18 e 20);
- d) Garantir a transparência no tratamento de dados baseado em legítimo interesse (art. 10, § 2º);
- e) Elaborar relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, com observância dos segredos comercial e industrial (arts. 10, § 3º, e 38);
- f) Verificar o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, quando o tratamento de dados pessoais de crianças for baseado no consentimento (art. 14, § 5º);
- g) Eliminar os dados após o tratamento (art. 16);
- h) Estabelecer mecanismos e salvaguardas nas transferências de dados;
- i) Indicar o encarregado pelo tratamento de dados (art. 41);
- j) Reparar danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de dados pessoais (art. 42);
- k) Comunicar à Agência Nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48);
- l) Salvaguardar os direitos dos titulares: responder as requisições, a adoção de providências, divulgação do fato em meios de comunicação; medidas para reverter ou mitigar os efeitos do incidente (arts. 18, e 48, § 2º);
- m) Observar as boas práticas e padrões de governança (art. 50).

O art. 23 da Resolução nº 017/2025/DPG (PPPD da DPEMT) também apresenta um rol de competências da DPEMT, enquanto controladora de dados pessoais: I. observar os fundamentos, princípios de privacidade e proteção de dados pessoais e os deveres impostos pela LGPD e por normativos correlatos da ANPD que disciplinam o tratamento e a governança dos dados pessoais; II. considerar o preconizado pelos art. 7º, art. 11 e art. 23 antes de realizar o tratamento de dados pessoais; III. cumprir o previsto pelos art. 46 e art. 50 da LGPD buscando a proteção de dados pessoais e sua governança; IV. indicar formalmente um encarregado e seu substituto pelo tratamento de dados pessoais, divulgando as identidades e as informações de contato de forma clara e objetiva, preferencialmente no sítio institucional; V. elaborar o inventário de dados pessoais (IDP) a fim de manter registros das operações de tratamento de dados pessoais; VI. elaborar, quando couber, o Relatório de Impacto de Proteção de Dados Pessoais (RIPD) relacionados às operações de tratamento, e atualizá-lo quando necessário; VII. reter dados pessoais somente pelo período necessário para o cumprimento da hipótese legal e finalidade utilizadas como justificativa para o tratamento de dados pessoais; VIII. criar e manter atualizados a políticas ou avisos de privacidade, que informarão sobre os tratamentos de dados pessoais realizados em cada ambiente físico ou virtual, e sobre as medidas de proteção de dados adotadas para salvaguardar esses dados pessoais; IX. requerer do titular a ciência com o termo de uso para cada serviço ofertado, informatizado ou não, que trate dados pessoais; X. assegurar aos titulares meios céleres, eficazes e adequados para viabilizar a comunicação com o encarregado e o exercício de direitos assegurados pela LGPD e normativos correlatos; XI. estabelecer, no sítio eletrônico da DPEMT, um portal destinado à LGPD, no qual serão divulgados esta Política, os canais de contato do encarregado, os avisos de privacidade e demais normas e documentos correlatos;



XII. requisitar, a qualquer tempo, informações a respeito do tratamento dos dados pessoais confiados a fornecedores de produtos, prestadores de serviços ou parceiros da DPEMT, respeitando-se o sigilo empresarial e as demais proteções legais; XIII. prover os meios necessários para o exercício das atribuições do encarregado, neles compreendidos, entre outros, recursos humanos, técnicos e administrativos; XIV. solicitar assistência e orientação do encarregado quando da realização de atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais; XV. garantir ao encarregado a autonomia técnica necessária para cumprir suas atividades, livre de interferências indevidas, especialmente na orientação a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; XVI. garantir ao encarregado acesso direto às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afetem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização.

3.6 Quem é o Operador?

É a pessoa natural ou jurídica, de direito público ou privado, que **realiza o tratamento de dados pessoais em nome do controlador** (art. 5º, VII, da LGPD).

O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria (art. 39, da LGPD).

A principal diferença entre o controlador e operador é o poder de decisão. O operador só pode agir no limite das finalidades determinadas pelo controlador.

Conforme previsto no parágrafo único do art. 24 da Resolução nº 17/2025/DPG, quaisquer fornecedores de produtos, prestadores de serviços e outros parceiros que realizarem tratamento de dados pessoais a eles confiados pela DPEMT são considerados operadores e devem seguir as diretrizes estabelecidas nesta política, na LGPD e nos regulamentos da ANPD. Assim, em regra, todas as empresas contratadas pela DPEMT para realizar algum tratamento de dado pessoal serão consideradas operadoras de dados pessoais.

Atenção! Os membros, servidores e estagiários da DPEMT não são operadores. Os empregados, administradores e outras pessoas naturais que integram a empresas contratadas pela DPEMT também não são considerados operadores. Ou seja, não é operador aquela pessoa natural que atua como profissional subordinado ao órgão controlador ou à empresa operadora.

3.6.1 E a Responsabilidade do Operador?

O controlador ou o operador que em razão do exercício de atividade de tratamento de dados pessoais, causar a outro dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (art. 42, da LGPD).

O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 da LGPD (art. 42, § 1º, I, da LGPD).

Desse modo, o operador só poderá tratar os dados para a finalidade previamente estabelecida pelo controlador. Isso demonstra a principal diferença entre o controlador e operador: o poder de decisão. **O operador só pode agir no limite das finalidades determinadas pelo controlador.**

Cabe destacar ainda, algumas das obrigações do operador:

- a) **seguir as instruções do controlador;**
- b) **firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador;**
- c) **dar ciência ao controlador em caso de contrato com suboperador.**

Os pontos que podem ser definidos contratualmente entre controlador e operador são o objeto, a duração, a natureza e a finalidade do tratamento dos dados, os tipos de dados pessoais envolvidos e os direitos e obrigações e responsabilidades relacionados ao cumprimento da LGPD.

Nesse sentido, dentro do seu escopo de atuação, o operador pode definir elementos não essenciais do tratamento, como medidas técnicas.

Dessa forma, o operador caracteriza-se como a pessoa natural ou jurídica, de direito público ou privado, externa ao quadro funcional da DPEMT, que realiza o tratamento de dados pessoais em nome desta, em todas as suas instâncias, especialmente no âmbito de contratos ou instrumentos congêneres com ele firmados (escopo eminentemente executório).

A título de exemplo, operadores são os fornecedores contratados pela DPEMT para tratar os dados dos assistidos, membros, servidores ou estagiários na execução de um contrato ou similar.

O art. 25 da RESOLUÇÃO Nº 017/2025/DPG (Política de Privacidade e Proteção de Dados Pessoais da DPEMT) determina que compete ao operador: I. aderir à PPPD da DPEMT; II. cumprir fielmente os deveres legais e contratuais, bem como as diretrizes e instruções estabelecidas pela DPEMT; III. assinar contrato ou termo de compromisso com cláusulas específicas sobre proteção de dados pessoais definidas pela DPEMT; IV. observar os princípios estabelecidos no art. 6º da LGPD, ao realizar tratamento de dados pessoais; V. antes de efetuar o tratamento, verificar se as diretrizes estabelecidas cumprem os requisitos legais presentes nos art. 7º, art. 11 e art. 23 da LGPD; VI. apresentar, sempre que solicitado, evidências e garantias suficientes de que aplica medidas técnicas e administrativas adequadas de segurança para a proteção dos dados pessoais, nos termos definidos na legislação, em normas administrativas da DPEMT e nos instrumentos contratuais; VII. facultar acesso a dados pessoais somente para o pessoal autorizado, que tenha estrita necessidade, e que tenha assumido compromisso formal de preservar a confidencialidade e segurança de tais dados, devendo a prova do compromisso estar disponível em caráter permanente para exibição à DPEMT, mediante solicitação; VIII. auxiliar, sempre que demandado pelo controlador, no atendimento pela DPEMT de obrigações perante titulares de dados pessoais, autoridades competentes ou quaisquer outros legítimos interessados;



IX. comunicar formalmente e de imediato à DPEMT a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa acarretar comprometimento ou dano potencial ou efetivo a titular de dados pessoais; X. descartar de forma irrecuperável ou devolver para a DPEMT, todos os dados pessoais e as cópias existentes, após a satisfação da finalidade respectiva ou o encerramento do tratamento por decurso de prazo ou por extinção de vínculo legal ou contratual; XI. manter os registros de tratamento de dados pessoais que realizar em nome da DPEMT, com condições de rastreabilidade e de fornecer evidências a qualquer tempo; e XII. permitir a realização de auditorias, incluindo inspeções pela DPEMT ou por ente por ela autorizado, e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações estabelecidas.

3.7 Quem é o Encarregado?

É a 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) (art. 5º, VIII, da LGPD).

O tratamento de dados pessoais pelo poder público (pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei de Acesso à Informação – LAI), além de ser realizado para o atendimento de finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, dependerá da indicação de um encarregado (art. 23, III, da LGPD).

Essa obrigatoriedade é reforçada no art. 41 da LGPD: “o controlador deverá indicar encarregado pelo tratamento de dados pessoais”.

Dessa forma, fica clara a obrigatoriedade, imposta pela LGPD, da necessidade de indicação de um encarregado para que o poder público possa tratar dados pessoais.

3.7.1 E as atribuições do Encarregado?

São atividades do Encarregado (art. 41, § 2º, da LGPD):

- 1 - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências cabíveis;
- 2 - receber comunicações da ANPD e adotar providências;
- 3 - 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
- 4 - executar as demais atribuições determinadas pelo agente de tratamento ou estabelecidas em normas complementares.

Conforme previsto na Resolução CD/ANPD Nº 18/2024, cabe ainda ao encarregado, prestar assistência e orientação ao agente de tratamento (Controlador e Operador) na elaboração, definição e implementação de:



- a) registro e comunicação de incidente de segurança;
- b) registro das operações de tratamento de dados pessoais;
- c) relatório de impacto à proteção de dados pessoais;
- d) mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais;
- e) medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito;
- f) processos e políticas internas que assegurem o cumprimento da LGPD, e dos regulamentos e orientações da ANPD;
- g) instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais;
- h) transferências internacionais de dados;
- i) regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da LGPD;

j) produtos e serviços que adotem padrões de design compatíveis com os princípios previstos na LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades; e

k) outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.

No âmbito da DPEMT, a Política de Privacidade e Proteção de Dados Pessoais (Resolução nº 17/2025/DPG, artigos 28 e 29) prevê que são atribuições do encarregado: I. receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II. receber comunicações e requisições da ANPD e adotar providências; III. orientar o público interno e contratados da DPEMT a respeito das normas, medidas e práticas a serem tomadas em relação à proteção de dados pessoais; IV. exercer outras atribuições correlatas e complementares; V. prestar assistência e orientação ao controlador na elaboração, definição, e implementação de: i. registro e comunicação de incidente de segurança; ii. registro das operações de tratamento de dados pessoais; iii. relatório de impacto à proteção de dados pessoais; iv. mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais;

v. medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito; vi. processos e políticas internas que assegurem o cumprimento da LGPD, e dos regulamentos e orientações da ANPD; vii. instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais; viii. transferências internacionais de dados; ix. regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da LGPD; X. produtos e serviços que adotem padrões de projetos compatíveis com os princípios previstos na LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades; e xi. outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.

3.8 Quem são os Agentes de Tratamento?

São agentes de tratamento o controlador e o operador (art. 5º, IX, da LGPD).

Os agentes de tratamento devem ser definidos a partir de seu caráter institucional. Não são considerados controladores (autônomos ou conjuntos) ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento.

No contexto de uma pessoa jurídica, a organização é o agente de tratamento para os fins da LGPD, já que é esta que estabelece as regras para o tratamento de dados pessoais, a serem executadas por seus representantes ou prepostos.

Todavia, as pessoas naturais podem ser consideradas controladoras ou operadoras de dados pessoais. Serão controladoras quando atuarem de acordo com os próprios interesses, com poder de decisão sobre as finalidades e os elementos essenciais de tratamento. Serão operadoras quando atuarem de acordo com os interesses do controlador, sendo-lhes facultada apenas a definição de elementos não essenciais à finalidade do tratamento.

O operador deve ser uma entidade distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos.

Por outro lado, os funcionários/servidores atuarão em subordinação às decisões do controlador, não se confundindo, portanto, com os operadores de dados pessoais.

A título exemplificativo, suponhamos que a DPEMT decida contratar uma empresa objetivando a aquisição de um sistema administrativo para execução e gerenciamento da folha de pagamento do órgão, com a finalidade de centralizar e operacionalizar todo o fluxo processual acerca do pagamento de membros, servidores e estagiários.

A Defensoria informará todos os requisitos para operacionalização e gerenciamento do sistema, tais como: público-alvo, requisitos mínimos de segurança, funcionalidades, layout (aparência), interface, entre outros. Nesse sentido, a empresa contratada tratará dados pessoais para fornecer, manter e gerenciar o funcionamento do sistema.

Nesse exemplo a Defensoria atua como controlador, ao determinar o tratamento de dados e definir os seus elementos essenciais. Enquanto que a empresa contratada atua como operadora, ao tratar dados conforme a finalidade do tratamento definido pelo controlador, ao fornecer, manter e gerenciar o funcionamento do sistema.

Necessário pontuar, que além da **finalidade** (realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular), o controlador é o responsável por estabelecer outros elementos essenciais relativos ao tratamento. É o caso da definição da **natureza dos dados pessoais tratados** (classificação de dados pessoais em gerais ou sensíveis) e da **duração do tratamento** (período durante o qual será realizada a operação, incluindo o estabelecimento de prazo para a eliminação dos dados). Vale ressaltar que outros elementos podem ser considerados essenciais a depender do contexto e das peculiaridades do caso concreto.

Atenção! Importante ressaltar que o servidor público que infrinja a LGPD, por dolo ou erro grosseiro, também é passível de responsabilização administrativa pessoal e autônoma, conforme prevê o art. 28, do Decreto Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às normas do Direito Brasileiro – LINDB).

3.9 O que é Tratamento?

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 (art. 5º, X, da LGPD).

O Guia de Boas Práticas da Lei Geral De Proteção De Dados (LGPD) do Governo Federal pontua e detalha algumas das operações supracitadas. Vejamos:

- a) acesso: possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo, etc., visando receber, fornecer, ou eliminar dados;
- b) armazenamento: ação ou resultado de manter ou conservar em repositório um dado;
- c) arquivamento: ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência;
- d) avaliação: ato ou efeito de calcular valor sobre um ou mais dados;
- e) classificação: maneira de ordenar os dados conforme algum critério estabelecido;
- f) coleta: recolhimento de dados com finalidade específica;

- g) comunicação: transmitir informações pertinentes a políticas de ação sobre os dados;
- h) controle: ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
- i) difusão: ato ou efeito de divulgação, propagação, multiplicação dos dados;
- j) distribuição: ato ou efeito de dispor de dados de acordo com algum critério estabelecido
- k) eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- l) extração: ato de copiar ou retirar dados do repositório em que se encontrava;
- m) modificação: ato ou efeito de alteração do dado;
- n) processamento: ato ou efeito de processar dados;
- o) produção: criação de bens e de serviços a partir do tratamento de dados;
- p) recepção: ato de receber os dados ao final da transmissão;
- q) reprodução: cópia de dado preexistente obtido por meio de qualquer processo;
- r) transferência: mudança de dados de uma área de armazenamento para outra, ou para terceiro;

s) transmissão: movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.;

t) utilização: ato ou efeito do aproveitamento dos dados.

Atenção! O tratamento de dados pessoais deve ser pautado pela **boa-fé**, além de observar aos seguintes **princípios**: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (art. 6º, da LGPD).

04

Quais os Princípios da LGPD?

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios (art. 6º, da LGPD):

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - 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;

IV - 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;

V - 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;

VI - 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;

VII - 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;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - 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.

Atenção! Ao considerar os princípios estabelecidos pela lei, a organização demonstrará que os dados pessoais coletados são necessários, mínimos, corretos, de qualidade e atendem uma finalidade de negócio válida.

05

E os dados pessoais sobre crianças, adolescentes e idosos?

O tratamento de dados pessoais de crianças e de adolescentes **deverá ser realizado no seu melhor interesse**, nos termos deste artigo e da legislação pertinente (art. 14, da LGPD).

Na mesma linha, o Enunciado CD/ANPD nº 01/2023, esclareceu que 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 (bases legais de tratamento de dados pessoais), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da referida Lei.



Atenção! O controlador deve comunicar à ANPD e ao titular qualquer incidente de segurança que possa acarretar risco ou dano relevante aos titulares dos dados (art. 48 da LGPD e art. 4º do Anexo da Resolução CD/ANPD nº 15/2024). A Agência Nacional de Proteção de Dados entende que o incidente de segurança que possa acarretar risco ou dano relevante aos titulares está caracterizado quando for capaz de afetar significativamente os interesses e direitos fundamentais dos titulares e, cumulativamente, envolver dados de crianças, adolescentes ou idosos (art. 5º, caput e inciso II, do Anexo da Resolução CD/ANPD nº 15/2024). Assim, o controlador deve comunicar à ANPD e aos titulares todo incidente de segurança que, cumulativamente, possa afetar significativamente interesses e direitos fundamentais dos titulares e envolva dados de crianças, adolescentes ou idosos.

Sobre essas categorias de titulares de dados pessoais, percebe-se que a lei e regulamentos emitidos pela ANPD as separa e evidencia. Assim, nota-se um nível de proteção adicional para o seu tratamento, haja vista as vulnerabilidades inerentes aos respectivos públicos.

06

O que é o Inventário de Dados Pessoais (IDP)?

O controlador e o operador devem manter **registro das operações de tratamento de dados pessoais que realizarem**, especialmente quando baseado no legítimo interesse (art. 37 da LGPD). O IDP consiste na materialização deste registro das operações de tratamento de dados pessoais realizado por um órgão.

O IDP representa um documento importante de **governança de dados pessoais e de subsídio para avaliação de impacto à proteção de dados pessoais** com vistas a verificar a conformidade da instituição ao preconizado pela LGPD. Ele proporciona uma espécie de “fotografia” do atual cenário do tratamento de dados pessoais do serviço/processo de negócio. (Guia de Elaboração do Inventário de Dados Pessoais do Ministério da Gestão e da Inovação em Serviços Públicos. Versão 2.0. março/2023).


Para maiores informações sobre o IDP, acesse o Manual de Inventário de Dados Pessoais da DPEMT disponível no portal da LGPD.


07

O que é o Relatório de Impacto à Proteção de Dados Pessoais (RIPD)?

É a 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 (art. 5º, XVII, da LGPD).

A Agência Nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (art. 10, §3º, da LGPD).

 [Clique Aqui](#) Guia de Elaboração de IDP

 [Clique Aqui](#) Portal da LGPD

A Agência Nacional poderá ainda determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial (art. 38, da LGPD).

O RIPD deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados (art. 38, parágrafo único, da LGPD).

Assim, o RIPD representa um documento fundamental a fim de demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados (Guia de Boas Práticas LGPD do Comitê Central de Governança de Dados do Governo Federal - versão 2.0. ago/2020).

Para maiores informações sobre o RIPD, acesse o Manual de elaboração do Relatório de Impacto à Proteção de Dados Pessoais da DPEMT disponível no portal da LGPD.



[Clique
Aqui](#)

Guia de Boas
Práticas



[Clique
Aqui](#)

Portal da
LGPD

O que é Incidente de Segurança?

No âmbito regulamentar da Agência Nacional de Proteção de Dados, o incidente de segurança é qualquer evento adverso confirmado, relacionado à violação das propriedades de **confidencialidade, integridade, disponibilidade e autenticidade** da segurança de dados pessoais (art. 3º, XII, do Anexo da Resolução CD/ANPD Nº 15, de 24 de abril de 2024).

Para maiores informações sobre o Incidente de Segurança, acesse o Manual de Registro de Incidente de Segurança envolvendo Dados Pessoais da DPEMT disponível no portal da LGPD.



[Clique
Aqui](#)

Portal da LGPD



[Clique
Aqui](#)

Resolução
CD/ANPD nº
15/2024

Quanto à Lei de Acesso à Informação (LAI) e LGPD?

A Lei de Acesso à Informação (LAI) – Lei Federal nº 12.527, de 18 de novembro de 2011 (art. 4º, IV), conceitua informação pessoal como aquela relacionada à pessoa natural identificada ou identificável. Já o art. 31 dessa lei estabelece que algumas informações pessoais possuem um regime específico de proteção.

Assim, apenas a informação pessoal com potencial de vulnerar os direitos de personalidade, tais como definidos no art. 5º, X, da Constituição Federal (inviolabilidade da intimidade, a vida privada, a honra e a imagem das pessoas), estaria sob uma proteção especial. No núcleo desse conjunto de dados, estaria o que se denominou, com amparo na doutrina existente, a informação pessoal sensível. Ou seja, aquela informação que viola o direito de autodeterminação da imagem ou que possa levar a que terceiros adotem ações discriminatórias contra o titular daquele dado. A existência de gradações desta natureza mostrou-se bastante importante ao longo dos últimos anos, pois passou a indicar limites à mitigação da expectativa de privacidade no caso em que os titulares dos dados eram os próprios agentes públicos. Esse é o entendimento esboçado no Guia de Boas Práticas LGPD do Comitê Central de Governança de Dados do Governo Federal - versão 2.0. ago/2020.

A LGPD, além de manter o conceito de dado pessoal apresentado de início pela LAI (art. 4º, IV), inovou ao positivar o conceito de dado pessoal sensível (art. 5º, II, da LGPD).



[Clique
Aqui](#)

Lei Federal nº
12.527/2011



[Clique
Aqui](#)

Guia de Boas
Práticas

Entretanto, diferentemente da LAI, os direitos e salvaguardas sobre dados pessoais da LGPD incidem sobre todos os tipos de dados pessoais, observadas as legislações existentes, inclusive os regimes existentes de transparência e acesso à informação. Ou seja, conforme ensina o Guia de Boas Práticas LGPD do CCGD, a tutela da lei se estende não mais apenas aos dados pessoais sensíveis ou diretamente relacionados aos direitos de personalidade, mas, em maior ou menor medida, a todos os dados pessoais.

Sobre o relacionamento complementar entre LAI e LGPD, transcrevemos trecho da conclusão da Cartilha do Ministério Público de Contas do Paraná – MPC Explica para você: LAI X LGPD:

Ocorre que não existe conflito aparente entre as Leis, ou seja, elas não se sobrepõem entre si. Pelo contrário, as Leis se complementam dando mais poder ao cidadão no exercício do controle social, enfatizando o desenvolvimento da transparência na Administração Pública e no controle dos seus próprios dados pessoais, além de fortalecer a privacidade, a autodeterminação informativa e os direitos dos titulares de dados pessoais.

Enquanto a LAI aumenta a transparência da Administração Pública, direta e indireta, em todas as esferas governamentais – municipais, estaduais e federais – ao disponibilizar para qualquer pessoa (física ou jurídica), informações de caráter público sem exigir motivação para o pedido, a LGPD influencia nessa transparência pública no que diz respeito à coleta e análise de dados privados. Ou seja, o Estado deverá deixar mais claro a maneira como fará o tratamento dos dados do cidadão e seguir as regras de anonimização e preservação da privacidade, o que irá contribuir não somente para a transparência, mas também para a segurança.

Além disso, vale mencionar que o escopo regulatório da LGPD está muito próximo do compliance e da cultura de gestão de riscos, assim como dos sistemas de segurança da informação, em que planejar e prevenir é sempre melhor do que remediar. Portanto, as contribuições normativas trazidas pela LGPD não se resumem apenas à letra de lei, mas sim a um contexto regulatório embasado nas evoluções tecnológicas que, acima de tudo, não esqueceram da importância do fator humano.



[Clique
Aqui](#)

MPC Explica
para você

O que é a Agência Nacional de Proteção de Dados – ANPD?

É uma entidade da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional (art. 5º, XIX, da LGPD).

A Agência Nacional de Proteção de Dados é autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública. Com a publicação da Medida Provisória nº 1.317, de 17 de setembro de 2025 (convertida na Lei nº 15.352, de 25 de fevereiro de 2026), a ANPD recebeu o status de agência reguladora (art. 2º, XII da Lei Federal nº 13.848/2019) e foi dotada de autonomia funcional, técnica, decisória, administrativa e financeira, com patrimônio próprio e com sede e foro no Distrito Federal (nova redação do art. 55-A da LGPD).

A ANPD é o órgão central na arquitetura da Lei Geral de Proteção de Dados, atuando como a principal entidade reguladora, fiscalizadora e educativa em matéria de proteção de dados pessoais no Brasil. Dessa maneira, a ANPD tem um papel fundamental na garantia dos direitos fundamentais à privacidade e à proteção dos dados pessoais.

Sua criação representa um passo significativo para o Brasil na adaptação às tendências globais de proteção de dados, alinhando-se a regulamentações internacionais como o GDPR (Regulamento Geral sobre a Proteção de Dados) da União Europeia. Recentemente, o conselho de diretor da ANPD, por meio da resolução 32/2026 considerou a união europeia como organismo internacional que proporciona grau de proteção de dados pessoais adequado ao previsto na LGPD, para fins de transferência internacional de dados.



10.1 Quais as funções e as competências da ANPD?

As competências e funções da ANPD estão detalhadas principalmente no artigo 55-J da LGPD e podem ser agrupadas em quatro grandes eixos: Normatização e Regulamentação; Fiscalização e Aplicação de Sanções; Promoção e Educação; e Atuação Colaborativa e Mediadora de Conflitos.

a) Normatização e Regulamentação: A ANPD detém a responsabilidade primária de dar clareza e detalhamento à LGPD, que, por vezes, apresenta conceitos abertos. Neste âmbito, suas principais atribuições são:

Edição de Normas e Procedimentos: A Agência é responsável por elaborar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, preenchendo lacunas e orientando a aplicação da lei em situações concretas. Isso inclui a definição de padrões técnicos mínimos de segurança e a regulamentação de temas como a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD).

Elaboração de Diretrizes: Compete à ANPD criar as diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, um instrumento estratégico para a efetivação da cultura de proteção de dados no país.

Interpretação da Lei: A ANPD tem a prerrogativa de interpretar a LGPD, garantindo segurança jurídica tanto para os titulares dos dados quanto para as organizações, sejam elas públicas ou privadas.

b) Promoção e Educação: A ANPD possui um papel crucial na disseminação da cultura de proteção de dados e na conscientização da sociedade sobre seus direitos e deveres. Suas atribuições nesta área são:

Promover o Conhecimento: É função da ANPD promover junto à população o conhecimento sobre as normas e as políticas públicas de proteção de dados, bem como sobre as medidas de segurança da informação.

Orientar Agentes de Tratamento: A Agência deve orientar empresas e órgãos públicos sobre as melhores práticas para se adequarem e cumprirem a LGPD.

Elaborar Estudos: A ANPD deve promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade, buscando o aprimoramento contínuo da legislação e de sua aplicação.

c) **Atuação Colaborativa e Mediadora de Conflitos:** Além de suas funções impositivas, a ANPD atua de forma a mediar conflitos e a colaborar com outras entidades, visando a resolução administrativa de questões e a proteção dos direitos dos titulares. Neste sentido, compete à Agência:

Apreciar Petições de Titulares: A ANPD atua como uma instância de recurso para os titulares de dados, apreciando suas petições contra os controladores após a tentativa de solução direta não ter sido bem-sucedida no prazo estabelecido.

Atuar na Prevenção de Infrações: A Agência busca resolver conflitos de forma administrativa, prevenindo a judicialização de questões relacionadas à proteção de dados.

Estimular a Adoção de Padrões: A ANPD deve incentivar a adoção de padrões para serviços e produtos que facilitem o exercício do controle dos titulares sobre seus dados pessoais, levando em conta as especificidades de cada setor.

Cooperação Internacional: A Agência deve promover ações de cooperação com autoridades de proteção de dados de outros países, alinhando as práticas brasileiras aos padrões globais.

Portanto, a atuação da ANPD é multidimensional e suas competências são projetadas para criar um ambiente seguro e confiável para o tratamento de dados pessoais no Brasil.

10.2 A ANPD tem poder sancionador?

A LGPD estabelece uma série de sanções para organizações que falharem na proteção dos dados pessoais conforme requerido pela legislação. A aplicação dessas sanções é de competência exclusiva da ANPD (art. 55-K da LGPD).

A ANPD é o órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para sua implementação (parágrafo único do art. 55-K da LGPD). Assim, como a competência da ANPD prevalece sobre as competências correlatas de outros órgãos da administração pública, no que se refere ao tema da proteção de dados pessoais, cabe a ela articular sua atuação com outras entidades e órgãos com competências sancionatórias e normativas no campo da proteção de dados pessoais.

As penalidades foram desenhadas para assegurar que as organizações tratem a proteção de dados pessoais com a máxima seriedade, enfatizando a importância de aderir às práticas de segurança e privacidade estabelecidas. As sanções podem variar de acordo com a gravidade da infração e incluem (art. 52 da LGPD):

- I - advertência, com indicação de prazo para adoção de medidas corretivas;
- II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- III - multa diária, observado o limite total a que se refere o inciso II;
- IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- VI - eliminação dos dados pessoais a que se refere a infração;
- X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
- XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Importante frisar, que **somente poderá ser aplicado às entidades e aos órgãos públicos as sanções dispostas** nos incisos I, IV, V, VI, X, XI e XII.

Nesse sentido, percebe-se que as sanções podem representar prejuízos de grande impacto e consequências as organizações em caso de não conformidade com a LGPD.

Referências Bibliográficas



DEFENSORIA PÚBLICA
DO ESTADO DE MATO GROSSO



Escola Superior da
Defensoria Pública de Mato Grosso

Governo Federal. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19/11/2025.

ANPD. Enunciado CD/ANPD Nº 1, de 22 de maio de 2023. Disponível em: <https://www.in.gov.br/en/web/dou/-/enunciado-cd/anpd-n-1-de-22-de-maio-de-2023-485306934>. Acesso em: 10/03/2025.

ANPD. Resolução CD/ANPD Nº 15, de 24 de abril de 2024. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>. Acesso em: 10/03/2025.

ANPD. Resolução CD/ANPD Nº 2, de 27 de janeiro de 2022. Disponível em: https://www.gov.br/anpd/pt-br/aceso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 16/09/2025.

Ministério da Gestão e da Inovação em Serviços Públicos. Guia de Elaboração de Inventário de Dados Pessoais. Brasília, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_inventario_dados_pessoais.pdf. Acesso em: 10/03/2025.

Comitê Central de Governança de Dados do Governo Federal. Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD). 2020. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 12/03/2025.

Governo Federal. Página Participa + Brasil: Tomada de Subsídios: Tratamento de Dados Pessoais de Crianças e Adolescentes. Disponível em: <https://www.gov.br/participamaisbrasil/tscriancaeadolescente>. Acesso em: 10/03/2025.

Referências Bibliográficas



DEFENSORIA PÚBLICA
DO ESTADO DE MATO GROSSO



Escola Superior da
Defensoria Pública de Mato Grosso

Data Privay Brasil. Curso Privacidade e Proteção de Dados - turma 47, disciplina dados sensíveis e proteção de dados de criança e adolescente, 2024.

Governo Federal. Lei nº 8.159, de 8 de janeiro de 1991 (Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8159.htm. Acesso em 14/03/2025.

Governo Federal. Constituição Federal de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14/03/2025.

Governo Federal. Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 14/03/2025.

Governo Federal. Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 14/03/2025.

Governo Federal. Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14/03/2025.

Governo Federal. Lei Federal nº 14.133/2021 (art. 18, I, e §1º). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm. Acesso em: 24/03/2025.

Governo de Mato Grosso. Decreto Estadual nº 1.525/2022 (art. 35). Disponível em: <https://leisestaduais.com.br/mt/decreto-n-1525-2022-mato-grosso-regulamenta-a-lei-federal-no-14-133-de-1o-de-abril-de-2021-no-ambito-da-administracao-publica-estadual-direta-autarquica-e-fundacional-do-estado-de-mato-grosso?q=1525>. Acesso em: 24/03/2025.

Referências Bibliográficas



Ministério da Gestão e da Inovação em Serviços Públicos. Guia/Modelo de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais. Disponível em <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos>. Acesso em: 16/09/2025.

Ministério da Gestão e da Inovação em Serviços Públicos. Guia de Resposta a Incidentes de Segurança. Disponível em https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_resposta_incidentes.pdf. Acesso em: 16/09/2025.

Ministério Público de Contas do Paraná. Cartilha LAI X LGPD. Disponível em: https://www.mpc.pr.gov.br/wp-content/uploads/2021/10/MPC_EXPLICA_PARA_VOCE-__LAI_x_LGPD_-_2-1.pdf. Acesso em 16/09/2025.

ANPD. Glossário ANPD. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd>. Acesso em: 24/03/2025.

DICIO. Dicionário Online de Português. Disponível em: <https://www.dicio.com.br/>. Acesso em: 24/03/2025.

Associação Brasileira de Normas Técnicas – ABNT. ABNT NBR ISO 31000:2018 (Gestão de riscos — Diretrizes). ANPD. Resolução Nº 32, de 26 de janeiro de 2026. Disponível em: <https://www.in.gov.br/web/dou/-/resolucao-n-32-de-26-de-janeiro-de-2026-683334547>. Acesso em: 03/02/2026.

DPEMT. Resolução nº 017/2025 (Institui a Política de Privacidade e Proteção de Dados Pessoais (PPPD) no âmbito da Defensoria Pública do Estado de Mato Grosso). Disponível em: https://www.iomat.mt.gov.br/apifront/portal/edicoes/imprimir_materia/1724271/18538. Acesso em: 12/03/2026.

Referências Bibliográficas



Governo Federal. Lei nº 15.211, de 17 de setembro de 2025 (Estatuto Digital da Criança e do Adolescente). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Acesso em: 12/03/2026.

ANPD. Resolução Nº 32, de 26 de janeiro de 2026 (Reconhecimento da União Europeia como organismo internacional com grau de proteção de dados pessoais adequado ao previsto na LGPD, para fins de transferência internacional de dados). Disponível em: <https://www.in.gov.br/web/dou/-/resolucao-n-32-de-26-de-janeiro-de-2026-683334547>. Acesso em 12/03/2026.