

MANUAL

Modelos de cláusulas contratuais no contexto da Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo (Controle 14)

Portaria CGM/SP nº 27/2026

Programa de Governança em Privacidade
e Proteção de Dados Pessoais



PREFEITURA DE
SÃO PAULO

FICHA

Prefeitura do Município de São Paulo

Prefeito

Ricardo Nunes

Controladoria Geral do Município

Controlador Geral do Município

Daniel Falcão

Chefe de Gabinete

Marcos Augusto Carboni

Equipe da Coordenadoria de Proteção de Dados Pessoais

Coordenador

Edson Joaquim Raimundo de Araujo Júnior

Elaboração

Fábio Fernandes Libonati

João Francisco Resende

Thiago Ryuichi Hirata

Revisão

Alana Leite Catuzzati

Arte e Diagramação

Marília Miquelin de Oliveira

Versão 01

Junho de 2026

Este manual foi elaborado em cumprimento aos termos do Decreto Municipal nº 59.767, de 15 de setembro de 2020, que regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018, no âmbito do Poder Executivo do Município de São Paulo.

Controlador Geral do Município

Daniel Falcão

VERSÃO

Versão	Descrição	Data
1.0	Versão inicial	06/2026

Sumário

1. Apresentação	6
2. Metodologia	7
3. Conceitos iniciais	9
3.1. Verificação se o objeto do contrato envolve o tratamento de dados pessoais	9
3.2. Verificação da extensão geográfica do tratamento: nacional ou internacional	10
3.3. Verificação da existência de minuta padrão obrigatória com cláusulas de proteção de dados pessoais	12
3.4. Verificação do papel das partes: controlador ou operador	12
3.4.1. Controlador	14
3.4.2. Controlador conjunto	15
3.4.3. Operador	16
3.4.4. Suboperador	17
3.5. Escopo do modelo de cláusulas do presente manual	17
4. Modelos de cláusulas contratuais	19
4.1. Tratamento de dados pessoais	20
4.1.1. Descrição do tratamento	21
4.1.2. Finalidade do tratamento	23
4.1.3. Condições gerais do tratamento	24
4.1.4. Condições específicas do tratamento	25
4.1.5. Duração e término do tratamento	27
4.2. Segurança	28
4.2.1. Medidas de segurança	29
4.2.2. Comunicação de incidente de segurança	30
4.3. Direitos do titular	31
4.3.1. Requisições do titular	32
4.3.2. Transparência	33
4.4. Responsabilidade e documentação	34
4.4.1. Responsabilidade	35
4.4.2. Documentação	36
4.5. Compartilhamento posterior	37
5. Metodologia para implementação	38
5.1. Competências e responsabilidades	39
5.2. Formalização e aprovação	39
6. Referências	40
Apêndice I – Exemplos da atuação do controlador e do operador	43

1. Apresentação

Este manual foi elaborado com o objetivo de auxiliar os agentes públicos responsáveis por implementar os controles previstos na Portaria CGM nº 27/2026, que regulamenta o modelo de Programa de Governança em Privacidade e Proteção de Dados Pessoais da Administração Pública Municipal. O foco deste manual é a implementação do “*Controle 14 – Modelos de cláusulas contratuais*”.

A Lei Geral de Proteção de Dados Pessoais (LGPD) permite que órgãos públicos tratem e compartilhem dados pessoais quando isso for necessário para cumprir suas funções, como executar serviços e políticas públicas. Esse compartilhamento pode acontecer com base em contratos, convênios e acordos, desde que respeite os direitos dos titulares dos dados pessoais e siga regras claras. Dessa forma, cabe ao órgão ou entidade definir sobre as formas e limites do tratamento, assim como instruir e fiscalizar a empresa, organização, fornecedor ou prestador de serviço contratado ou parceiro. Para tanto, os instrumentos que estabeleçam a relação com terceiros devem conter cláusulas que disciplinem o tratamento de dados pessoais objeto da contratação. Para contratações específicas e rotineiras, caracteriza-se como boa prática a utilização de modelos de cláusulas contratuais.

Convém ressaltar que as cláusulas podem variar de acordo com o contexto das contratações ou parcerias. É possível que seja elaborado modelo de cláusulas para a aquisição ou contratação de determinados bens e materiais, que difere do modelo de cláusulas elaborado para a contratação de serviços, ou ainda do modelo de cláusulas para o estabelecimento de parcerias com diferentes finalidades. Os órgãos e entidades possuem autonomia técnica e devem considerar o contexto, o volume e o risco dos tratamentos de dados pessoais realizados na implementação deste controle. Dessa forma, o modelo apresentado neste manual não é de uso obrigatório. Ele tem caráter orientativo e deve ser ajustado às diferentes realidades, desde que essas adaptações sejam devidamente justificadas.

2. Metodologia

É importante esclarecer que o objetivo deste manual não é explicar ou interpretar conceitos teóricos relacionados à proteção de dados pessoais. Trata-se de um manual de aplicação prática, que busca sistematizar as orientações e o conhecimento já produzido pela Agência Nacional de Proteção de Dados (ANPD) e outras instituições de referência, visando auxiliar os gestores públicos da Administração Municipal na aplicação dos conceitos às suas diferentes realidades.

O manual tomou como referência instituições que elaboraram modelos e minutas de contratos, que devem ser consultados pelos gestores públicos para maiores informações:

- **Referência A:** REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. Guia para a Implementação de Cláusulas Contratuais Modelo Para a Transferência Internacional de Dados Pessoais.
- **Referência B:** MATO GROSSO DO SUL. Procuradoria-Geral do Estado. Pareceres Referências e Minutas-Padrão.
- **Referência C:** PERNAMBUCO. Procuradoria-Geral do Estado. Instrumentos Padronizados.
- **Referência D:** RIO DE JANEIRO (Cidade). Secretaria de Integridade, Transparência e Proteção de Dados (SMIT). Minuta de Termo Aditivo ao Contrato (ou Instrumento Congênere).
- **Referência E:** BRASIL. Advocacia-Geral da União. Modelos da Lei 14.133/2021. Modelo Contrato Serviços Sem Mão de Obra Lei 14.133 (setembro/2025).

Ademais, também foram utilizadas referências normativas e de boas práticas em proteção de dados pessoais, mencionadas a seguir:

- **Referência F:** ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27701:2020. Tecnologia de segurança – Extensão da ABNT NBR/IEC 27001

e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes. Rio de Janeiro: ABNT, 2024.

- **Referência G:** ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27001:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2022.
- **Referência H:** ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27002:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.
- **Referência I:** ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27557:2023. Segurança da Informação, segurança cibernética e proteção da privacidade – Aplicação da ABNT NBR ISO 31000:2018 para gestão de riscos de privacidade organizacional. Rio de Janeiro: ABNT, 2023.
- **Referência J:** BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).
- **Referência K:** BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança.
- **Referência L:** BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 19, de 23 de agosto de 2024. Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais.

A proposta do presente manual é apresentar diferentes tipos de cláusulas aplicáveis a contratos administrativos, termos de parceria, acordos de cooperação ou instrumentos congêneres que tenham como objeto ou envolvam tratamento de dados pessoais para sua execução. Espera-se que o manual seja útil para auxiliar os agentes públicos na elaboração de instrumentos contratuais que assegurem que o tratamento de dados pessoais seja realizado de forma legítima e segura. As referências foram elencadas de A-L para fins de citação no presente manual.

3. Conceitos iniciais

Inicialmente, é importante esclarecer qual o escopo de aplicação do presente manual. Nesse sentido, destaca-se que a sua utilização deve ocorrer em contexto específico, no qual cabe ao agente público avaliar os quatro critérios que serão explicados a seguir:

- Verificação se o objeto do contrato¹ envolve o tratamento de dados pessoais;
- Verificação da extensão geográfica do tratamento: nacional ou internacional;
- Verificação da existência de minutas padrão obrigatórias que já contenham cláusulas de proteção de dados pessoais; e
- Verificação do papel das partes: controlador ou operador.

3.1. Verificação se o objeto do contrato envolve o tratamento de dados pessoais

O primeiro passo da definição do escopo do presente manual é a verificação do objeto do contrato. Nesse sentido, o foco do modelo de cláusulas apresentado está relacionado a **contratações cujo objeto envolva diretamente o tratamento de dados pessoais**.

Para facilitar a compreensão, apresenta-se como exemplo de situação que integra o escopo deste manual os casos em que a execução do contrato exige um cadastro de usuários ou o compartilhamento de base de dados pessoais de indivíduos. Nota-se que, nesses casos, a execução do contrato depende diretamente do tratamento de dados pessoais.

Por outro lado, apresenta-se como exemplo de situação que não integra o escopo deste manual os casos em que os únicos dados pessoais tratados são referentes aos próprios contratantes. Nota-se que todos os contratos possuem esse tipo de informação, como os nomes das partes, seus documentos de identificação, endereços, dados bancários, entre outros dados pessoais que são indispensáveis para a formalização do contrato. Destaca-se que esses dados pessoais não estão relacionados diretamente com a execução do objeto do contrato.

¹ Para fins de simplificação do texto, o termo “contrato” será utilizado de forma abrangente para se referir a contratos administrativos destinados à aquisição de bens, materiais, serviços ou obras, assim como a termos de colaboração, termos de fomento, acordos de cooperação e contratos de gestão celebrados pela Administração Municipal com organizações da sociedade civil, com vistas à realização de objetivos de interesse público.

3.2.Verificação da extensão geográfica do tratamento: nacional ou internacional

O segundo passo da definição do escopo do presente manual é a verificação da extensão geográfica do tratamento de dados pessoais. Nesse sentido, o foco do modelo de cláusulas apresentado está relacionado a contratações cujo tratamento de dados pessoais possui abrangência nacional, ou seja, **não inclui a transferência internacional de dados pessoais**.

O tema da transferência internacional é tratado em capítulo específico da LGPD e possui regulamentação própria, considerando-se a relevância e a complexidade do assunto (vide Resolução CD/ANPD nº 19/2024, na seção “6. Referências” deste documento). Nota-se que a transferência internacional deve estar fundamentada em uma das hipóteses legais de tratamento previstas no Art. 7º ou 11 da LGPD e, ainda, estar amparada em um dos mecanismos válidos de transferência internacional de dados, previstos nos incisos I a IX do Art. 33 da LGPD.

Nota-se, portanto, que os contratos que prevejam a transferência internacional de dados pessoais devem observar regras e mecanismos específicos. Portanto, não se aplica o conteúdo do presente manual, sendo necessário seguir estritamente a legislação pertinente aplicável.

Para fins de contextualização, será apresentada na tabela a seguir breve explicação sobre o inciso II do Art. 33 da LGPD. Esse dispositivo legal apresenta mecanismo de transferência internacional no qual o controlador deve comprovar a adequação do tratamento por meio de: *a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; e d) selos, certificados e códigos de conduta regularmente emitidos*. É importante destacar que os termos citados possuem sentido próprio na LGPD, e não se confundem com os modelos de cláusulas apresentados neste manual.

Tabela 1: Mecanismos de transferência internacional do Art. 33, II da LGPD

Termo	Resolução CD/ANPD nº 19/2024	Glossário da ANPD
Cláusulas-Padrão Contratuais	Conforme Art. 15 da Resolução CD/ANPD nº 19/2024, as cláusulas-padrão contratuais são elaboradas e aprovadas pela própria ANPD. No momento da elaboração deste manual, elas foram aprovadas e constam no Anexo II da referida Resolução. Seu objetivo é garantir a adoção de garantias mínimas, salvaguardas e condições válidas para a realização de transferências internacionais de dados pessoais. A validade da transferência internacional de dados quando amparada nas cláusulas-padrão, pressupõe a adoção de seu texto integral e sem alteração, conforme disponibilizado no Anexo II da Resolução.	<i>“mecanismo de transferência internacional de dados que estabelece garantias mínimas e condições válidas para a realização de transferências internacionais de dados e que pressupõe a adoção integral e sem alteração de texto disponibilizado no Anexo II do Regulamento de Transferências Internacionais, aprovado pela Resolução nº 19, de 23 de agosto de 2024.”</i>
Cláusulas-Padrão Contratuais Equivalentes	Conforme Art. 18 da Resolução CD/ANPD nº 19/2024, as cláusulas-padrão contratuais equivalentes são elaboradas por outros países ou organismos internacionais e são reconhecidas pela própria ANPD como equivalentes às cláusulas previstas no Anexo II da Resolução. Nesse sentido, após o reconhecimento da equivalência, as cláusulas-padrão contratuais equivalentes são consideradas como mecanismo válido para a realização de transferências internacionais de dados.	<i>“cláusulas-padrão contratuais de outros países ou de organismos internacionais reconhecidas pela Autoridade Nacional de Proteção de Dados como equivalentes com as cláusulas previstas no Anexo II da Resolução CD/ANPD nº 19, de 23 de agosto de 2024”.</i>
Cláusulas Contratuais Específicas	Conforme Art. 21 da Resolução CD/ANPD nº 19/2024, as cláusulas contratuais específicas são elaboradas pelo próprio controlador e devem ser submetidas para aprovação pela ANPD. Nota-se que a utilização de cláusulas contratuais específicas só é permitida quando a transferência internacional de dados não puder ser realizada por meio das cláusulas-padrão contratuais, em razão de circunstâncias excepcionais, devidamente comprovadas pelo controlador.	<i>“mecanismo de transferência internacional de dado no qual o controlador solicita à Autoridade Nacional de Proteção de Dados a sua aprovação e que ofereçam e comprovem garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei nº 13.709, de 14 de agosto de 2018 e na Resolução CD/ANPD nº 19, de 23 de agosto de 2024 , desde que a transferência não possa ser realizada por meio das cláusulas-padrão contratuais, em razão de circunstâncias excepcionais de fato ou de direito, devidamente comprovadas pelo controlador”.</i>
Normas Corporativas Globais	Conforme Art. 25 da Resolução CD/ANPD nº 19/2024, as normas corporativas globais são destinadas às transferências internacionais de dados entre organizações do mesmo grupo ou conglomerado de empresas, possuindo caráter vinculante em relação aos membros do grupo. As normas corporativas globais devem ser submetidas à aprovação da ANPD.	<i>“Mecanismo destinado às transferências internacionais de dados entre organizações do mesmo grupo ou conglomerado de empresas, possuindo caráter vinculante em relação aos membros do grupo que as subscreverem.”</i>

Fonte: elaboração própria

3.3. Verificação da existência de minuta padrão obrigatória com cláusulas de proteção de dados pessoais

Outro critério a ser avaliado pelos órgãos e entidades na implantação desse controle é a não existência de minutas padrão de contratos de uso obrigatório na Administração Municipal que já contenham cláusulas específicas relacionadas à proteção de dados pessoais², aplicáveis ao objeto da contratação.

Conforme dispõe o Art. 114, III do Decreto Municipal nº 62.100/2022, que regulamenta a aplicação na Administração Municipal da Lei Federal nº 14.133/2021 (Lei de Licitações e Contratos Administrativos), os contratos deverão conter, quando aplicáveis, as cláusulas essenciais relacionadas à proteção de dados pessoais.

Dessa forma, quando o objeto da contratação estiver abrangido por minuta padrão de uso obrigatório, não se aplicam as recomendações deste manual, devendo o órgão ou entidade adotar integralmente o modelo aprovado e disponibilizado pela Procuradoria Geral do Município (PGM), conforme suas orientações e atualizações oficiais.

3.4. Verificação do papel das partes: controlador ou operador

O quarto passo da definição do escopo do presente manual é a verificação do papel das partes no tratamento dos dados pessoais: se exercem função de controlador ou de operador. É importante que os contratos prevejam a definição das partes como controlador ou operador, pois isso afeta o conteúdo do próprio contrato, como a definição das responsabilidades em relação à reparação por danos decorrentes de atos ilícitos.

De acordo com o “*Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*”, elaborado pela ANPD, o agente de tratamento pode assumir quatro papéis, esquematizados na tabela a seguir: controlador; operador; controlador conjunto; e suboperador.

² Conforme disponível na página da Procuradoria Geral do Município de São Paulo, Minutas-Padrão de Editais de Licitação e Contratos Administrativos, no endereço https://prefeitura.sp.gov.br/web/procuradoria_geral/w/minutas_padrao_de_editais_de_licitacao_e_contratos_administrativos. Acesso em 15/01/2026.

Tabela 2: Possibilidade de relação entre agentes de tratamento

Órgão ou entidade	Outra parte
Controlador	Operador
Controlador	Controlador conjunto
Operador	Suboperador
Operador	Controlador

Fonte: elaboração própria.

Observando as orientações da ANPD, também é importante esclarecer que a definição dos agentes de tratamento (controlador e operador) se baseia em seu caráter institucional, ou seja, não são considerados controladores ou operadores “(...) *os indivíduos subordinados, tais como funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento*”³.

Para fins deste manual e com o objetivo de maximizar a utilidade deste documento para os agentes públicos, **o órgão ou entidade será tratado como controlador**, uma vez que possuirá, em grande parte dos casos, competência para as decisões referentes ao tratamento de dados pessoais. Destaca-se que é possível que o órgão ou entidade seja operador em determinados casos, embora isso ocorra de maneira mais pontual, razão pela qual o presente manual não tratará desses casos. Consulte o Apêndice I para a visualização de situações exemplificativas da atuação como controlador ou operador.

Por sua vez, a identificação da outra parte como controlador ou operador deve ser realizada quando da elaboração dos contratos, dado que isso tem impacto significativo nesse processo. No âmbito do presente manual, será dado foco aos contratos em que a outra parte atue como operador. Entretanto, também serão apresentados alguns pontos de atenção para os casos em que a outra parte assuma o papel de controlador conjunto.

³ BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo. Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Maio de 2021. Brasília, DF. Disponível em: < https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf > Acesso em: 24/07/2025, p. 5.

3.4.1. Controlador

A LGPD, em seu art. 5º, define o controlador como *“pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”*.

De acordo com o *“Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado”*, elaborado pela ANPD, o conceito possui elevada importância prática, pois a LGPD atribui obrigações específicas ao controlador, como:

- A elaboração de relatório de impacto à proteção de dados pessoais (Art. 38);
- A comprovação de que o consentimento obtido do titular atende às exigências legais (Art. 8º, § 2º);
- O registro das operações de tratamento de dados pessoais (Art. 37);
- A adoção de medidas de segurança, técnicas e administrativas (Art. 46);
- A comunicação à ANPD da ocorrência de incidentes de segurança (Art. 48);
- A transparência sobre o tratamento dos dados pessoais e de informações do encarregado (Art. 23, I e 41); e
- O atendimento aos direitos dos titulares (Art. 18).

De acordo com o referido Guia da ANPD, o papel de controlador pode decorrer das obrigações pactuadas no contrato. Porém, a atividade desempenhada na prática é que irá determinar se o agente de tratamento de fato é um controlador ou não. Nesse sentido, a ANPD aponta dois elementos que auxiliam na caracterização do controlador:

- **Poder de decisão:** não é necessário que o tratamento de dados pessoais seja realizado diretamente pelo controlador, bastando que ele possua o poder de decisão sobre o tratamento. É possível, portanto, que o controlador forneça instruções para que um operador realize o tratamento em seu nome (Art. 39);
- **Elementos essenciais:** não é necessário que o controlador tome todas as decisões sobre o tratamento, bastando que ele mantenha sob a sua influência e controle as principais decisões. Entre os elementos essenciais das decisões, destacam-se:

- **Finalidade do tratamento:** o controlador é responsável por definir a finalidade do tratamento dos dados pessoais, ou seja, estipular os objetivos que justificam a realização do tratamento e a sua respectiva base legal;
- **Outros elementos essenciais:** o controlador também é responsável por estabelecer outros elementos essenciais, como a natureza dos dados pessoais tratados e a duração do tratamento.

3.4.2. Controlador conjunto

De acordo com o “*Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*”, elaborado pela ANPD, a depender do contexto, uma mesma operação de tratamento de dados pessoais pode envolver mais de um controlador. A identificação desse cenário é relevante, pois, conforme o Art. 42, §1º, II, da LGPD, os controladores conjuntos responderão de forma solidária.

Embora a LGPD não explicita o conceito de controladoria conjunta, infere-se que ele esteja contemplado no sistema jurídico de proteção de dados pessoais. De acordo com o Glossário da ANPD, o conceito de controladoria conjunta envolve “*determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD*”.

Em resumo, o já referido Guia da ANPD apresenta os três critérios que devem ser observados cumulativamente para que se configure a controladoria conjunta:

- “**Mais de um controlador possui poder de decisão sobre o tratamento de dados pessoais**”: decorrente do próprio conceito de controlador, já definido neste manual, a configuração da controladoria conjunta depende da existência de mais de um controlador, ou seja, agente de tratamento que possui poder de decisão sobre a finalidade e os elementos essenciais do tratamento de dados pessoais;
- “**Há interesse mútuo de dois ou mais controladores, com base em finalidades próprias, sobre um mesmo tratamento**”: o Guia da ANPD destaca que não se configura

a controladoria conjunta quando os objetivos do tratamento forem distintos entre os diversos controladores. Portanto, as finalidades devem ser comuns, convergentes ou complementares, configurando-se um interesse mútuo; e

- ***“Dois ou mais controladores tomam decisões comuns ou convergentes sobre as finalidades e elementos essenciais do tratamento”***: o conceito de decisões comuns está relacionado com a intenção comum e a tomada de decisões em conjunto sobre as finalidades e meios de tratamento. Por sua vez, o conceito de decisões convergentes está relacionado com decisões distintas, porém que se complementam de tal forma que o tratamento não seria possível sem a participação de ambos os controladores.

3.4.3. Operador

A LGPD, em seu art. 5º, define o operador como *“pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”*. No mesmo sentido, o Art. 39 dispõe que: *“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”*.

De acordo com o *“Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado”*, elaborado pela ANPD, o conceito possui elevada importância prática, pois a LGPD atribui obrigações específicas ao operador, como:

- Manter registro das operações de tratamento de dados pessoais (Art. 37);
- Seguir as instruções do controlador (Art. 39); e
- Adotar medidas de segurança, técnicas e administrativas (Art. 46).

O referido Guia da ANPD ainda destaca a boa prática de o operador dar ciência ao controlador em caso de contrato com suboperador, no caso de autorização prevista em contrato. Cabe ressaltar ainda que, em geral, tanto o controlador como o operador possuem a obrigação de reparação se causarem danos a terceiros, no âmbito de suas respectivas esferas de atuação. Assim, entende-se que o controlador, por exercer o poder decisório sobre o tratamento, responde de forma mais ampla, inclusive por atos praticados por operadores sob sua direção, desde que estes atuem de boa-fé e dentro dos limites das instruções recebidas. Todavia, há uma

exceção prevista no Art. 42, § 1º, I da LGPD, que estabelece a responsabilidade solidária do operador quando o dano decorrer de tratamento irregular de dados pessoais, isto é, quando houver descumprimento da legislação ou das instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador.

Nota-se que a diferença fundamental entre o controlador e o operador reside no poder de decisão quanto aos elementos essenciais do tratamento de dados pessoais. Dessa forma, se a outra parte puder realizar decisões sobre os elementos essenciais do tratamento de dados pessoais objeto da contratação, trata-se de controlador conjunto. Por outro lado, caso a outra parte realize o tratamento de dados pessoais unicamente a partir das diretrizes e orientações passadas pelo órgão ou entidade da Administração Pública municipal, ela caracteriza-se tão somente como operador.

3.4.4. Suboperador

Analogamente ao conceito de controladoria conjunta, a LGPD também não explicitou a definição de suboperador. De acordo com o Glossário da ANPD, o conceito de suboperador se refere a “*contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador*”. Em teoria, o suboperador possui relação direta com o operador, e não com o controlador. Porém, independentemente do acordo firmado entre o operador e o suboperador, ambos podem ser entendidos como operadores perante a LGPD.

De acordo com o “*Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*”, elaborado pela ANPD, a discussão ora apresentada possui relevância para a equiparação do suboperador ao operador perante a LGPD, em relação às atividades que foi contratado para executar. Isso implica na ampliação da cadeia de responsabilidade solidária dos operadores, prevista no Art. 42, §1º, I da LGPD.

3.5. Escopo do modelo de cláusulas do presente manual

Em suma, conclui-se que o **escopo do presente manual** apresenta modelo de cláusulas contratuais que poderão ser utilizadas pelos agentes públicos **nos casos de contratos**:

- Que tem como objeto ou envolva diretamente em seu objeto o tratamento de dados pessoais;
- Que não contemplem a transferência internacional de dados pessoais;
- Que não tenham aplicável minuta padrão obrigatória com cláusulas de proteção de dados pessoais; e
- Que tenham o órgão ou entidade como controlador.

Ressalta-se mais uma vez que o conteúdo deste manual é apenas um modelo, que deve ser adaptado de acordo com o contexto das contratações.

4. Modelos de cláusulas contratuais

A seguir, são apresentados os principais tópicos que costumam compor cláusulas contratuais relacionadas ao tratamento de dados pessoais. Esses itens foram extraídos de documentos de diversas instituições de referência e podem ser adaptados pelos órgãos e entidades de acordo com as particularidades de cada contratação⁴. Sua inclusão não é obrigatória, sendo possível selecionar apenas os tópicos mais relevantes ou ainda incluir outros, conforme a necessidade, cabendo ao gestor público realizar essa avaliação.

i) Tratamento de dados pessoais

- a. Descrição do tratamento
- b. Finalidade do tratamento
- c. Condições gerais do tratamento
- d. Condições específicas do tratamento
- e. Duração e término do tratamento

ii) Segurança

- a. Medidas de segurança
- b. Comunicação de incidente de segurança

iii) Direitos do titular

- a. Requisitos do titular
- b. Transparência

iv) Responsabilidade e documentação

⁴ A escolha dos tópicos também teve fundamento na minuta da ANPD sobre o futuro regulamento sobre o uso compartilhado de dados pessoais pelo Poder Público, especificamente o Art. 7º. Apesar de preliminar, o normativo traz indícios de eventuais exigências por parte da ANPD: “Art. 7º A decisão administrativa e os instrumentos referidos no art. 6º deverão apresentar de forma objetiva e detalhada os seguintes aspectos relacionados ao uso compartilhado de dados: I – a identificação dos agentes de tratamento envolvidos, incluindo informações de contato; II – a definição de responsabilidades de cada agente de tratamento, inclusive em relação aos direitos dos titulares; III – os dados pessoais do objeto do uso compartilhado; IV – a finalidade específica do uso compartilhado dos dados, na forma do art. 26, caput, da Lei nº 13.019, de 14 de agosto de 2018; V – a hipótese legal utilizada, nos termos do art. 7º ou do art. 11 da Lei nº 13.709, de 14 de agosto de 2018; VI – os meios e os procedimentos, inclusive recursos técnicos e tecnológicos, utilizados para realizar o compartilhamento; VII – a duração do uso compartilhado de dados, justificando o prazo e informando o período de conservação ou a necessidade de eliminação dos dados, quando for o caso; VIII – a indicação das medidas de segurança adotadas para proteger os dados pessoais; IX – a vedação das medidas de segurança adotadas para proteger os dados pessoais; X – a declaração de que foi realizada a avaliação de trata o art. 8º e verificada a compatibilidade entre a finalidade original para a qual os dados pessoais foram coletados e a finalidade do uso compartilhado. Parágrafo único. A definição de responsabilidades de que trata o inciso II do caput deste artigo incluirá as instruções e as condições a serem observadas para o tratamento dos dados pessoais pelo agente de tratamento receptor, quando atuar como operador, em conformidade com o disposto no art. 39 da Lei nº 13.709, de 14 de agosto de 2018.”

- a. Responsabilidade
- b. Documentação

v) Compartilhamento posterior

É importante destacar que a seleção dos tópicos também levou em consideração o Guia da ANPD sobre o “*Tratamento de Dados Pessoais pelo Poder Público*”, mais especificamente na seção sobre “*Compartilhamento de dados pessoais pelo Poder Público*” e “*Anexo I*”. Tal documento elenca os principais requisitos que devem ser observados nos processos de compartilhamento de dados pessoais pelo Poder Público. Trata-se de diretrizes gerais, que devem ser ajustadas ou complementadas de acordo com o contexto e as peculiaridades de cada caso concreto. Para mais informações, recomenda-se a leitura completa do referido material.

4.1. Tratamento de dados pessoais

O primeiro tópico que deve compor as cláusulas contratuais relaciona-se com as disposições referentes ao tratamento de dados pessoais realizado no âmbito do contrato. Isso decorre da própria definição de controlador, que é o responsável pela tomada de decisão a respeito de elementos essenciais do tratamento. Dessa forma, é importante que essas decisões sejam formalizadas em contrato, contemplando os principais aspectos do tratamento.

O presente manual identificou cinco aspectos-chave que devem ser detalhados em contrato, porém, os órgãos e entidades devem avaliar a existência de outros pontos que variam a depender do contexto da contratação. Cada um desses aspectos será explicado a seguir: descrição do tratamento, finalidade do tratamento, condições gerais do tratamento, condições específicas do tratamento, duração e término do tratamento.

Especificidades para contratos entre Controladores conjuntos
A LGPD confere ao controlador o dever de registrar as suas operações de tratamento (Art. 37). A definição sobre o tratamento de dados pessoais em contratos de controladoria conjunta possui a particularidade de que todos os controladores envolvidos tomam decisões em conjunto sobre as finalidades e os elementos essenciais do tratamento, havendo interesse mútuo. É importante estabelecer procedimento para a tomada de decisão a respeito do tratamento de dados pessoais e eventuais alterações necessárias.

4.1.1. Descrição do tratamento

O primeiro aspecto a ser detalhado é a descrição do tratamento, que deve especificar, de forma clara e objetiva, quais atividades serão realizadas com os dados pessoais no âmbito do contrato⁵. É importante que seja delimitado o escopo das operações de tratamento de dados pessoais do acordo que se pretenda celebrar. Nesse sentido, é fundamental descrever com clareza todas as especificidades do tratamento de dados pessoais realizado, como as operações autorizadas, as categorias de dados pessoais envolvidos, seus respectivos titulares e a forma de coleta dos dados. Também é importante reforçar que o operador deve seguir as instruções repassadas pelo controlador.

A descrição precisa permitir que todas as partes compreendam as etapas envolvidas no tratamento e se responsabilizem pelas medidas de segurança e conformidade aplicáveis a cada uma delas. O detalhamento dessas informações contribui para a transparência entre as partes e para o cumprimento das normas aplicáveis. Trata-se de um ponto essencial para a gestão dos riscos à privacidade, assegurando-se maior controle sobre o fluxo dos dados pessoais.

Recomenda-se que o órgão ou entidade realize a descrição dos dados pessoais objeto do uso compartilhado, com destaque para:

- A **natureza**⁶ dos dados pessoais compartilhados, classificando-os em:
 - **Gerais**⁷; ou
 - **Sensíveis**⁸.

⁵ Neste ponto, vale lembrar que a LGPD define em seu Art. 5º, inciso X como tratamento de dados pessoais, uma ampla variedade de atividades e operações, a título exemplificativo, tais como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

⁶ Resolução CD/ANPD nº 15, de 2024 “Art. 3º. (...) XV - *natureza dos dados pessoais: classificação de dados pessoais em gerais ou sensíveis*;”.

⁷ LGPD, “Art. 5º (...) I - *dado pessoal: informação relacionada a pessoa natural identificada ou identificável*;”.

⁸ LGPD, “Art. 5º (...) II - *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*”

- A **categoria**⁹ dos dados pessoais compartilhados, isto é, a classificação dos dados pessoais de acordo com o contexto de sua utilização, tais como:
 - Dados de identificação pessoal;
 - Dados de autenticação em sistemas;
 - Dados financeiros;
 - Entre outros¹⁰.
- Os **titulares** de dados pessoais envolvidos, com destaque para:
 - Dados pessoais de crianças e adolescentes¹¹; ou
 - Dados pessoais de idosos¹².

Nessa linha, o Guia da ANPD sobre o “*Tratamento de Dados Pessoais pelo Poder Público*” ressalta, em seu tópico “(b) Objeto e finalidade”, que é importante indicar de forma objetiva e detalhada os dados pessoais que serão compartilhados.

Mapeamento de cláusulas para contratos entre Controlador e Operador	Referências
Especificação das operações de tratamento de dados pessoais autorizadas e sua frequência, incluindo-se informações a respeito da fonte e metodologia de coleta dos dados	▪ A – Cláusula 4, Anexo B ▪ C – Cláusula 9, § 2º, V ▪ I – Item 6.4.2.2 ▪ J – Art. 37, 38, p. único ▪ L – Cláusula 2.1
Especificação da natureza e das categorias de dados pessoais objeto do tratamento	▪ A – Cláusula 4, Anexo B ▪ C – Cláusula 9, § 2º, V ▪ D – Anexo I, Cláusula 4.1 ▪ I – Item 6.4.2.2 ▪ J – Art. 37, 38, p. único ▪ L – Cláusula 2.1
Especificação das categorias de titulares cujos dados pessoais objeto do tratamento	▪ A – Cláusula 4, Anexo B ▪ I – Item 6.4.2.2 ▪ J – Art. 37
Obrigação do operador de realizar o tratamento de dados pessoais seguindo as instruções repassadas pelo controlador	▪ C – Cláusula 9, § 1º, I, § 2º, I ▪ J – Art. 39 ▪ L – Cláusula 10.1

⁹ Resolução CD/ANPD nº 15, de 2024 “Art. 3º. (...) III - categoria de dados pessoais: classificação dos dados pessoais de acordo com o contexto de sua utilização, tais como dados de identificação pessoal, dados de autenticação em sistemas, dados financeiros;”.

¹⁰ Para mais informações, vide o Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022, pp. 141-143. O guia exemplifica categorias de dados pessoais, tais como hábitos, lazer, consumo, finanças, residência, família, educação, trabalho, filiações, conflitos, entre outros.

¹¹ LGPD, “Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.”

¹² LGPD, “Art. 55-J (...) XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);”.

4.1.2. Finalidade do tratamento

Em seguida, deve-se explicitar a finalidade do tratamento, ou seja, para que os dados pessoais serão tratados no contexto da contratação. Recomenda-se que o órgão ou entidade especifiquem a finalidade do uso compartilhado, bem como a finalidade do tratamento de dados pessoais por cada uma das partes, de forma que seja possível avaliar sua adequação e compatibilidade.

A LGPD define o princípio da finalidade (Art. 6º, I) como a *“realização de tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”*. Relacionado ao tema, a LGPD também define o princípio da não discriminação (Art. 6º, IX), como a *“impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos”*. A finalidade precisa ser específica, legítima e informada, evitando usos genéricos ou que ultrapassem o escopo do contrato.

Dessa forma, é necessário formalizar a finalidade do tratamento de dados pessoais objeto do acordo que se pretenda celebrar, bem como estabelecer compromissos para adoção de medidas que possam assegurar que os tratamentos de dados pessoais sejam realizados conforme a finalidade apresentada. Isso é relevante para que se evite o uso posterior dos dados pessoais para finalidades incompatíveis, discriminatórias ou abusivas. Trata-se de importante medida para se garantir a conformidade com a legislação e a proteção dos direitos dos titulares.

O Guia da ANPD sobre o *“Tratamento de Dados Pessoais pelo Poder Público”* ressalta, em seu tópico *“(b) Objeto e finalidade”*, que é importante indicar a finalidade do tratamento, a qual deve ser específica, com a indicação precisa de qual política pública ou competência legal será atendida pelo compartilhamento dos dados pessoais. Nesse sentido, o documento destaca o Art. 26 da LGPD, segundo o qual *“o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei”*. **O Guia da ANPD ainda alerta que finalidades genéricas ou indeterminadas contrariam as disposições da LGPD.**

Por fim, o Guia da ANPD destaca, em seu tópico *“(c) Base legal”*, a necessidade de indicação da base legal do compartilhamento dos dados pessoais, conforme Art. 7º ou 11 da LGPD.

Mapeamento de cláusulas para contratos entre Controlador e Operador	Referências
Especificação das principais finalidades do tratamento dos dados pessoais	▪ A – Cláusula 4, 6.2, Anexo B ▪ C – Cláusula 9, § 2º, V ▪ D – Anexo I, Cláusula 5 ▪ E – Cláusula 10.2 ▪ F – Item 7.2.1 ▪ I – Item 6.4.2.2 ▪ J – Art. 26 ▪ L – Cláusula 2.1
Especificação das bases legais para o tratamento de dados pessoais	▪ B – Cláusula 2.1, p. único ▪ D – Anexo I, Cláusula 3 ▪ F – Item 7.2.2 ▪ J – Art. 7º, 11
Obrigação do operador de que os dados pessoais somente sejam tratados para as finalidades especificadas (incluindo eventual tratamento posterior), sendo vedado o tratamento para fins discriminatórios ou abusivos	▪ A – Cláusula 4, 6.2, 7.2, Anexo B ▪ B – Cláusula 2.2, § 1º ▪ C – Cláusula 9, § 1º, XIII ▪ E – Cláusula 10.3 ▪ J – Art. 7º, § 7º, Art. 8º, § 2º, 27 ▪ L – Cláusula 10.1
Vedação ao operador ao tratamento de dados pessoais sem consentimento específico do titular quando necessário	▪ A – Cláusula 4, 6.2, Anexo B ▪ B – Cláusula 2.2, § 2º ▪ C – Cláusula 9, § 1º, XII, § 2º, IV ▪ F – Item 7.2.3, 7.2.4 ▪ J – Art. 7º, § 5º

4.1.3. Condições gerais do tratamento

É importante definir em contrato as condições gerais do tratamento de dados pessoais, as quais incluem medidas que buscam garantir a compatibilidade com as finalidades declaradas. Nesse sentido, apresentam-se os conceitos de três outros princípios da LGPD:

- **Adequação (Art. 6º, II):** *“compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”.*
- **Necessidade (Art. 6º, III):** *“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”.*
- **Qualidade dos dados (Art. 6º, V):** *“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”.*

Dessa forma, ao se incorporar esses princípios no contrato, busca-se assegurar que o tratamento de dados pessoais seja realizado de maneira proporcional ao atingimento das finalidades declaradas, respeitando-se os direitos dos titulares e os limites legais. Isso contribui não apenas para a conformidade com a LGPD, mas também para a construção de uma relação de confiança entre as partes envolvidas, prevenindo riscos e promovendo boas práticas de governança de dados.

O Guia da ANPD sobre o “*Tratamento de Dados Pessoais pelo Poder Público*” ressalta, em seu tópico “(b) *Objeto e finalidade*”, que é importante limitar o compartilhamento aos dados pessoais que forem estritamente necessários para as finalidades do tratamento, em conformidade com o princípio da necessidade.

Mapeamento de cláusulas para contratos entre Controlador e Operador	Referências
Obrigação das partes em limitar o tratamento ao mínimo necessário para realização das finalidades previstas no acordo, tendo como objeto dados pertinentes, proporcionais e não excessivos	▪ A – Cláusula 6.4 ▪ F – Item 7.4.1, 7.4.2, 7.4.4 ▪ L – Cláusula 10.1
Obrigação das partes de garantir aos titulares exatidão, clareza, relevância e atualização dos dados pessoais, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento	▪ A – Cláusula 6.4 ▪ C – Cláusula 9, § 2º, IV ▪ F – Item 7.4.3 ▪ L – Cláusula 10.1
Obrigação das partes em informar, imediatamente, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados, a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que a comunicação seja comprovadamente impossível ou implique esforço desproporcional	▪ F – Item 7.3.7 ▪ J – Art. 18, § 6º ▪ L – Cláusula 15.5
Obrigação das partes em manter os dados em formato interoperável e estruturado	▪ C – Cláusula 9, § 1º, XX ▪ E – Cláusula 10.10.1 ▪ J – Art. 25

4.1.4. Condições específicas do tratamento

Para além das condições gerais, é importante verificar se o objeto do tratamento contempla temas que merecem atenção especial. Isso se justifica porque a LGPD elenca requisitos específicos para determinados tipos de tratamento de dados pessoais, que serão exemplificados a seguir:

- **Dado pessoal sensível (Seção II, do Capítulo II da LGPD):** a LGPD define dado pessoal sensível como (Art. 5º, II) “*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”. Nota-se que o normativo estabelece requisitos específicos para o tratamento de dados pessoais sensíveis.

- **Dado pessoal sensível de saúde:** a LGPD apresenta requisitos específicos relacionado ao tratamento de dados pessoais sensíveis referentes à saúde e em estudos em saúde pública (Art. 11, § 4º e 5º, Art. 13).
- **Dados pessoais de crianças e adolescentes (Seção III, do Capítulo II da LGPD):** a LGPD confere atenção especial ao tratamento de dados pessoais de crianças e adolescentes, disciplinando o assunto em seção específica, no Art. 14.
- **Dados pessoais de idosos (Art. 55-J, inc. XIX, da LGPD):** a LGPD estabelece como competência da ANPD a garantia de que o tratamento de dados de idosos *"seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso)"*;
- **Tratamento automatizado (Art. 20 da LGPD):** a LGPD dispõe sobre o tratamento automatizado em seu Art. 20, buscando-se garantir os direitos do titular ao se fornecer transparência sobre os critérios utilizados para a decisão automatizada, evitando-se a ocorrência de discriminação.

Portanto, na elaboração de contratos que envolvam o tratamento de dados pessoais, é essencial avaliar se há previsão de operações que exigem cuidados adicionais, tais como os dados pessoais sensíveis ou de crianças e adolescentes e idosos, além da existência de tratamento automatizado.

O Guia da ANPD sobre o “*Tratamento de Dados Pessoais pelo Poder Público*” ressalta, em seu tópico “*(f) Outros requisitos*”, que é importante que o Poder Público ainda cumpra com requisitos específicos para compartilhamento de dados pessoais com entidades privadas, de acordo com os Arts. 26, § 1º e 27, da LGPD.

Mapeamento de cláusulas para contratos entre Controlador e Operador	Referências
Obrigações das partes em adotar salvaguardas adicionais para o tratamento de dados pessoais sensíveis, como medidas de segurança específicas e proporcionais aos riscos da referida atividade de tratamento	▪ A – Cláusula 4, 6.8, Anexo B ▪ D – Anexo I, Cláusula 4.3 ▪ J – Art. 11, § 3º ▪ L – Cláusula 11, 21.2
Obrigações das partes em adotar salvaguardas adicionais para o tratamento de dados pessoais de crianças e adolescentes, bem como medidas que assegurem que o tratamento seja realizado no melhor interesse de tais titulares, nos termos da legislação aplicável	▪ A – Cláusula 6.8 ▪ D – Anexo I, Cláusula 4.2 ▪ J – Art. 14 ▪ L – Cláusula 12, 21.2
Obrigações das partes em adotar salvaguardas adicionais para o tratamento de dados pessoais relacionados à saúde ou estudo em saúde pública	▪ J – Art. 11, § 4º, § 5º, 13
Obrigações do controlador em fornecer ao titular, sempre que solicitado, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada	▪ A – Cláusula 7.2 ▪ F – Item 7.3.10 ▪ J – Art. 20, § 1º
Obrigações do controlador em seguir requisitos específicos para o compartilhamento de dados pessoais com entidades privadas, incluindo a comunicação dos acordos para a ANPD	▪ E – Cláusula 10.12 ▪ J – Arts. 26, § 1º e 27

4.1.5. Duração e término do tratamento

Dentre as consequências do princípio da necessidade, já explicado anteriormente, é a eliminação dos dados pessoais a partir do momento em que o tratamento de dados pessoais não seja mais necessário. A LGPD confere especial atenção ao tópico, tratado em seção específica (Seção IV), nos Arts. 15 e 16.

É importante que os contratantes formalizem em contrato a frequência e a duração do tratamento dos dados pessoais, pois o armazenamento de informações após o término da relação contratual pode implicar em riscos para os contratantes. Nesse sentido, torna-se essencial determinar a destinação final dos dados pessoais, prevendo requisitos relacionados à eliminação dos dados, a práticas de anonimização ou pseudonimização, entre outras possibilidades.

O Guia da ANPD sobre o “*Tratamento de Dados Pessoais pelo Poder Público*” ressalta, em seu tópico “(d) *Duração do tratamento*”, que é importante estabelecer de forma expressa o período de duração do uso compartilhado dos dados pessoais, além de se esclarecer se há a possibilidade de conservação (Art. 16 da LGPD) ou se os dados pessoais devem ser eliminados após o término do tratamento. Deve-se observar as condições e os prazos previstos em normas específicas que regem a gestão de documentos e arquivos na Administração Pública

Municipal¹³. Após o término do uso compartilhado, é adequado realizar reavaliações dos termos do contrato caso seja de interesse a sua renovação, adequando-os a novas disposições legais e regulamentares e a novas medidas de segurança, conforme as tecnologias disponíveis.

Mapeamento de cláusulas para contratos entre Controlador e Operador	Referências
Especificação do período de armazenamento dos dados pessoais	▪ A – Cláusula 4, 6.5, 13, Anexo B ▪ B – Cláusula 2.9 ▪ D – Anexo I, Cláusula 6.1 ▪ F – Item 7.4.7 ▪ J – Art. 15 e 16 ▪ L – Cláusula 2.1, 20.1
Especificação da destinação final dos dados pessoais, incluindo disposições sobre retorno, transferência ou descarte de dados pessoais de uma maneira segura	▪ A – Cláusula 6.5 ▪ B – Cláusula 2.9 ▪ C – Cláusula 9, § 1º, XVII § 2º, VII ▪ D – Anexo I, Cláusula 6.2 ▪ E – Cláusula 10.5 ▪ F – Item 6.5.3.2, 7.4.5, 7.4.8, 8.4.2 ▪ H – Item 8.10, 8.11 ▪ L – Cláusula 20.1
Sujeição do operador a medidas resultantes do descumprimento do acordo, como a suspensão do compartilhamento de dados pessoais, a sua devolução, o seu compartilhamento a um terceiro, ou a sua eliminação	▪ A – Cláusula 12 ▪ L – Cláusula 23.2

4.2. Segurança

A LGPD define o princípio da segurança (Art. 6º, VII) como a “*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*”. Além disso, o normativo também traz o princípio da prevenção (Art. 6º, VIII), definido como a “*adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais*”.

Nesse sentido, o presente manual separou o tópico em duas partes. A primeira parte se refere a implementação de medidas de segurança e boas práticas, buscando-se implementar controles ao tratamento de dados pessoais para a minimização de riscos associados. A segunda parte se refere à comunicação de incidentes de segurança, um procedimento específico regulamentado pela ANPD que requer atenção especial.

¹³ Especialmente o Decreto Municipal nº 57.783, de 13 de julho de 2017 e a Portaria da Secretaria de Governo Municipal - SGM/SEGES/CGDOC nº 1 de 24 de maio de 2021.

4.2.1. Medidas de segurança

O tema da segurança e das boas práticas é tratado na LGPD com especial atenção, em seu capítulo VII (Arts. 46 a 51). Na elaboração dos contratos, é importante definir as 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. Isso é relevante para se garantir que a outra parte também adote cuidados especiais com relação ao tratamento, minimizando-se os riscos existentes.

A implementação das medidas de segurança deve considerar a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia. Tais medidas podem inclusive ultrapassar a vigência do contrato, como quando se prevê a retenção ou a eliminação dos dados pessoais em período posterior.

Entre as principais medidas de segurança, destaca-se o controle de acesso aos dados pessoais, a fim de se manter a confidencialidade das informações. Isso tem impacto nos próprios colaboradores das partes, cujo acesso aos dados pessoais deve ser restrito àqueles que necessitam realizar alguma operação de tratamento. Além disso, nota-se que a confidencialidade e outras medidas de segurança também devem atingir terceiros com quem eventualmente as partes necessitem compartilhar os dados pessoais, como operadores e suboperadores.

O Guia da ANPD sobre o “*Tratamento de Dados Pessoais pelo Poder Público*” ressalta, em seu tópico “(f) *Prevenção e segurança*”, que é importante que sejam estabelecidas as medidas de segurança proporcionais aos riscos às liberdades civis e aos direitos fundamentais dos cidadãos envolvidos no caso concreto.

Mapeamento de cláusulas para contratos entre Controlador e Operador	Referências
Obrigaç�o do operador de franquear acesso aos dados pessoais somente para o pessoal autorizado e necess�rio para a execu��o do acordo, ap�s compromisso formal de preservar a confidencialidade, sigilo e seguran�a dos dados pessoais, mesmo ap�s o t�rmino do acordo, incluindo o fornecimento de orienta��es e capacita��es conforme a necessidade	▪ A – Cl�usula 6.6, Anexo C ▪ B – Cl�usulas 2.2, 2.5 ▪ C – Cl�usula 9, � 1�, V, XI, XVIII ▪ D – Anexo I, Cl�usula 8.1 ▪ E - Cl�usula 10.6 ▪ F – Item 6.4.2.2, 6.5.2.1, 6.6.2.1, 6.10.2.4

	▪ H – Item 5.15, 6.3, 6.5, 6.6, 8.3 ▪ I – Item 6.4.2.2
Obrigação das partes de implementação de controles apropriados, de caráter administrativo e técnico, incluindo requisitos de segurança da informação	▪ A – Cláusula 6.1, 6.6, Anexo C ▪ B – Cláusula 2.3 ▪ C – Cláusula 9, § 1º, II, III, § 2º, II, ▪ D – Anexo I, Cláusula 9.1 ▪ E – Cláusula 10.10 ▪ F – Item 7.2.6 ▪ G - Item 8 ▪ H – Item 5.14, 5.19, 5.20 ▪ I – Item 6.5.2 ▪ J – Art. 46, 50 ▪ L – Cláusula 10.1, 21.1
Obrigação das partes em realizar esforços para adotar medidas de avaliação e revisão para manutenção de nível de segurança adequada	▪ A – Cláusula 6.1, 6.6, Anexo C ▪ E - Cláusula 10.11 ▪ G – Item 9 ▪ H – Item 5.22 ▪ I – Item 6.6 ▪ L – Cláusula 21.3

Especificidades para contratos entre Controladores conjuntos	
A LGPD atribui aos controladores o dever de adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais (Art. 46). Nesse sentido, o normativo estabelece que o controlador é responsável pelos danos decorrentes de violação de segurança se deixar de adotar medidas de segurança (Art. 44, parágrafo único). A definição de medidas de segurança nos casos de controladoria conjunta possui a particularidade de que todos os controladores respondem de forma solidária aos danos produzidos aos titulares de dados pessoais (Art. 42, §1º, II). Isso reforça a importância de que todos estejam em conformidade com a LGPD, implementando as medidas de segurança acordadas em contrato.	

4.2.2. Comunicação de incidente de segurança

A comunicação de incidente de segurança é tratada no Art. 48 da LGPD, que impõe o dever ao controlador de comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. O tema foi regulamentado na Resolução CD/ANPD nº 15/2024, que aprova o Regulamento de Comunicação de Incidente de Segurança.

A Resolução CD/ANPD nº 15/2024, define incidente de segurança como *“qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais”*. Sobre o tema, recomenda-se a leitura da resolução na íntegra.

A elaboração do contrato deve formalizar como as partes devem conduzir eventual incidente de segurança, pois os normativos implicam em prazos para comunicação, requisitos que devem

constar no comunicado, entre outros aspectos. Torna-se necessário, portanto, definir procedimentos e responsabilidades entre as partes para que o tema seja tratado de maneira eficiente e eficaz.

Mapeamento de cláusulas para contratos entre Controlador e Operador	Referências
Especificação das responsabilidades, procedimentos e prazos para comunicação de incidentes de segurança, incluindo-se a adoção de planos de resposta a incidentes	▪ A – Cláusula 6.6 ▪ B – Cláusula 2.7 ▪ C – Cláusula 9, § 1º, XIV ▪ F – Item 6.13.1.1, 6.13.1.5 ▪ H – Item 5.24, 5.25, 5.26
Obrigação do controlador sobre a comunicação de incidente de segurança à ANPD e aos titulares de dados pessoais	▪ C – Cláusula 9, § 2º, VI ▪ J – Art. 48 ▪ K – Art. 4º, 6º, 9º ▪ L – Cláusula 4.1A, 16.1
Obrigação do operador de notificar o controlador, tempestivamente, sobre todas as ocorrências de violações de segurança relacionadas ao tratamento de dados pessoais objeto do acordo, incluindo-se o dever de assistência ao controlador na resolução e na comunicação do incidente	▪ A – Cláusula 6.6 ▪ B – Cláusula 2.8 ▪ C – Cláusula 9, § 1º, X ▪ L – Cláusula 4.1A

Especificidades para contratos entre Controladores conjuntos
A LGPD conferiu a obrigação ao controlador de comunicar a ocorrência de incidente de segurança à ANPD e aos titulares dos dados pessoais (Art. 48). No caso da controladoria conjunta, todos os controladores respondem de forma solidária aos danos produzidos, conforme Art. 42, §1º, II da LGPD. Assim, é importante estabelecer procedimento adequado para a comunicação do incidente, pois entende-se que a responsabilidade dos controladores conjuntos é compartilhada. Nesse sentido, recomenda-se que todos os controladores envolvidos definam em contrato quem será o responsável por comunicar os incidentes e todo o procedimento operacional que deverá ser seguido. Contudo, deve-se lembrar que apesar da atribuição de competências e responsabilidades em contrato, todos os controladores respondem solidariamente.

4.3. Direitos do titular

Recomenda-se que o tema dos direitos do titular esteja disciplinado em contrato, com fundamento em dois importantes princípios da LGPD:

- **Livre acesso (Art. 6º, IV):** *“garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais”.*
- **Transparência (Art. 6º, VI):** *“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”.*

O presente manual dividiu o tópico dos direitos do titular em duas partes. A primeira parte se refere ao atendimento aos direitos do titular exercidos mediante requisição. A segunda parte se refere aos direitos relacionados à transparência.

4.3.1. Requisições do titular

A LGPD estabelece, em seu Capítulo III, disposições acerca dos direitos do titular. Nesse sentido, o Art. 18 garante ao titular o direito de obter do controlador, mediante requisição, uma série de informações relativas ao tratamento de seus dados pessoais. Entre esses direitos, destacam-se o acesso aos dados, a confirmação da existência do tratamento, a correção de dados incompletos, inexatos ou desatualizados, dentre outros. Esses direitos refletem os princípios do livre acesso e da transparência e visam assegurar maior controle do titular sobre suas próprias informações, sendo dever do controlador garantir mecanismos eficientes e acessíveis para o exercício desses direitos.

Estabelecer cláusulas contratuais que disciplinem o atendimento às requisições dos titulares é fundamental para se garantir os direitos previstos no Art. 18. É importante que o operador atue de forma coordenada com o controlador, viabilizando respostas eficientes e dentro dos prazos legais às requisições dos titulares. A ausência da definição de regras e procedimentos claros nesse sentido pode gerar falhas de comunicação, atrasos no atendimento e, conseqüentemente, responsabilização do controlador por descumprimento da legislação.

Além disso, cláusulas específicas fortalecem a governança no tratamento de dados pessoais, ao estabelecer deveres, fluxos e prazos para o cumprimento das requisições. Essas disposições contratuais contribuem para a prevenção de conflitos e garantem maior segurança jurídica entre as partes.

O Guia da ANPD sobre o “*Tratamento de Dados Pessoais pelo Poder Público*” ressalta, em seu tópico “(e) *Transparência e direitos dos titulares*”, que é importante delimitar as obrigações das partes no que se refere às responsabilidades e aos procedimentos a serem observados visando ao atendimento de solicitações apresentadas pelos titulares.

Mapeamento de cláusulas para contratos entre Controlador e Operador	Referências
Especificação de responsabilidades, procedimentos e prazos para atendimento aos direitos do titular	▪ A – Cláusula 7 ▪ F – Item 7.3.9 ▪ L – Cláusula 15.1
Obrigação do operador de cooperar para o atendimento às requisições dos titulares de dados pessoais. Caso ele não esteja autorizado a responder diretamente ao titular, pode-se estabelecer obrigação de: (a) informar ao titular sobre o canal de atendimento do controlador; e (b) encaminhar a requisição ao controlador	▪ A – Cláusula 7, 8 ▪ C – Cláusula 9, § 1º, IX ▪ F – Item 7.5.3, 8.3.1 ▪ L – Cláusula 4.6B, 15.4, 15.6
Obrigação do controlador de que o titular possa exercer os seus direitos em relação aos dados pessoais objeto do acordo mediante requisição	▪ F – Item 7.3.1 ▪ J – Art. 9º, 18 ▪ L – Cláusula 4.1A, 10.1, 14.1, 15.1

Especificidades para contratos entre Controladores conjuntos
A LGPD atribui ao controlador o dever de atender aos direitos do titular (Art. 18). O atendimento aos direitos do titular em contratos de controladoria conjunta possui a particularidade de que os controladores conjuntos devem providenciar canal de comunicação preferencialmente unificado para que o titular possa exercer os seus direitos de forma eficaz, independentemente de quem for responsável pela coleta, armazenamento ou demais operações de tratamento sobre os dados pessoais. É importante estabelecer responsabilidades e definir como os titulares serão atendidos por cada um dos controladores.

4.3.2. Transparência

A transparência no tratamento de dados pessoais é um dos princípios da LGPD e está associada a diversos requisitos específicos.

Inicialmente, destaca-se o dever de transparência quanto ao próprio tratamento de dados pessoais realizado. Nesse sentido, os titulares devem ser informados, de forma clara, acessível e adequada, sobre como seus dados pessoais estão sendo coletados, utilizados, armazenados e compartilhados. Essa obrigação abrange não apenas a fase inicial de coleta, mas todo o ciclo de vida do tratamento dos dados.

Ademais, a transparência também está relacionada com a publicidade de informações administrativas relacionadas ao tratamento. Nesse sentido, é necessário fornecer informações sobre a identidade do controlador e do seu respectivo encarregado, além dos mecanismos existentes para que o titular de dados pessoais possa exercer os seus direitos através de requisições.

O Guia da ANPD sobre o “*Tratamento de Dados Pessoais pelo Poder Público*” ressalta, em seu tópico “(e) *Transparência e direitos dos titulares*”, que é importante delimitar as obrigações

das partes no que se refere à divulgação das informações exigidas pela LGPD. Isso inclui a disponibilização de informações claras, precisas e facilmente acessíveis aos titulares sobre a realização do compartilhamento e sobre como exercer seus direitos. O documento indica que é uma boa prática divulgar na página eletrônica dos órgãos e entidades as informações pertinentes, conforme Art. 23, I da LGPD.

Mapeamento de cláusulas para contratos entre Controlador e Operador	Referências
Obrigação do controlador de garantir aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento, observados os segredos comercial e industrial, inclusive sobre a existência de compartilhamento (acordos com operadores)	▪ A – Cláusula 6.3 ▪ C – Cláusula 9, § 2º, III ▪ F – Item 7.3.2 ▪ J – Art. 10, § 2º, 11, § 2º, 23, I ▪ L – Cláusula 4.1A, 10.1, 14.1, 14.3
Obrigação do controlador de publicar em sua página na internet identificação dos agentes de tratamento e respectivos encarregados pelo tratamento de dados pessoais	▪ A – Cláusula 6.3 ▪ F – Item 7.3.2 ▪ J – Art. 23, III, 41, § 1º ▪ L – Cláusula 4.1A, 10.1, 14.1
Obrigação do controlador de publicar em sua página na internet informação sobre os direitos do titular e os meios para seu exercício	▪ A – Cláusula 7, 8 ▪ F – Item 7.3.2 ▪ L – Cláusula 10.1, 14.1

Especificidades para contratos entre Controladores conjuntos
A LGPD atribui dever de transparência a algumas atividades do controlador (Art. 23, I e 41). A transparência sobre as operações de tratamento de dados pessoais em contratos de controladoria conjunta possui a particularidade de que tanto o controlador como o controlador conjunto devem fornecer informações claras sobre o tratamento, garantindo a transparência ao titular sobre o uso compartilhado de dados. Recomenda-se que ao se conferir transparência, que haja a identificação clara de todos os controladores envolvidos, com suas respectivas funções e responsabilidades. Espera-se que o canal de comunicação com o titular seja preferencialmente unificado, havendo consistência nas comunicações.

4.4. Responsabilidade e documentação

O tema da responsabilidade e da documentação está relacionado ao princípio da responsabilização e prestação de contas (Art. 6º, X), definido pela LGPD como: *“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”*. Esse princípio impõe aos agentes de tratamento (controladores e operadores) o dever de não apenas cumprir a legislação, mas também de documentar e de demonstrar esse cumprimento sempre que necessário.

O presente tópico foi dividido em duas partes. Na primeira parte, serão tratados aspectos com relação a cláusulas que definem as responsabilidades associadas ao tratamento de dados

peçoais. Na segunda parte, serão explicitados deveres de documentação que também devem estar contidos nos contratos.

4.4.1. Responsabilidade

A LGPD dedica duas seções específicas ao tema da responsabilidade: a Seção II do Capítulo IV, que trata da responsabilidade pelo tratamento de dados pessoais pelo Poder Público, e a Seção III do Capítulo VI, que aborda as responsabilidades e o ressarcimento de danos associados aos agentes de tratamento. Esses dispositivos reforçam a importância de que os agentes de tratamento ajam com diligência e adotem mecanismos efetivos de controle, prevenção e mitigação de riscos.

O Guia da ANPD sobre o “*Tratamento de Dados Pessoais pelo Poder Público*” ressalta, em seu tópico “(g) *Outros requisitos*”, que é importante identificar as funções e as responsabilidades dos agentes de tratamento envolvidos no uso compartilhado de dados pessoais.

Mapeamento de cláusulas para contratos entre Controlador e Operador	Referências
Especificação sobre a responsabilidade perante o titular, que poderá pleitear a reparação do dano em razão da violação das cláusulas do acordo	▪ A - Cláusula 9 ▪ B – Cláusulas 2.10 e 2.11 ▪ C – Cláusula 9, § 1º, XV, XVI, § 2º, VIII ▪ F – Item 6.15.1.1 ▪ J – Art. 42, 44 ▪ L – Cláusula 4.2B, 17.1
Obrigação do operador de informar se uma instrução de tratamento violaria legislação aplicável ao caso	▪ A - Cláusula 11 ▪ F – Item 8.2.4
Obrigação do operador de responder, solidariamente, pelos danos causados pelo tratamento quando do descumprimento das cláusulas do acordo ou por não observância das instruções lícitas do controlador	▪ A - Cláusula 9 ▪ C – Cláusula 9, § 1º, XV, XVI, ▪ J – Art. 42, § 1º, I, 44 ▪ L – Cláusula 4.2B, 17.4
Previsão de que as partes só não serão responsabilizadas caso: não tenham realizado o tratamento de dados pessoais que constitua causa do dano; não tenham descumprido as cláusulas do acordo ou a legislação aplicável; o dano seja decorrente de culpa exclusiva do titular ou de terceiros, que não seja destinatário de compartilhamento posterior ou subcontratado pelas partes	▪ C – Cláusula 9, § 2º, VIII ▪ J – Art. 43 ▪ L – Cláusula 17.6
Previsão do direito de regresso pela parte que repara o dano ao titular em relação aos demais responsáveis, na medida da participação no evento danoso	▪ A - Cláusula 9 ▪ J – Art. 42, § 4º ▪ L – Cláusula 17.9

Especificidades para contratos entre Controladores conjuntos
A definição das responsabilidades nos casos de controladoria conjunta possui a particularidade de que todos os controladores respondem de forma solidária aos danos produzidos aos titulares de dados pessoais, conforme Art. 42, §1º, II da LGPD. É importante que os contratos de controladoria conjunta especifiquem procedimentos e responsabilidades de cada um dos controladores envolvidos, incluindo-se os mecanismos para a tomada de decisão em conjunto ou não.

4.4.2. Documentação

A LGPD trata o dever de prestar contas e de documentação em diversos trechos, notadamente nos artigos 37 e 38. Para que seja possível comprovar o cumprimento da LGPD perante os órgãos de controle, especialmente a ANPD, é essencial que os contratantes mantenham documentação comprobatória das medidas implementadas, como registros de operações de tratamento, avaliações de impacto à proteção de dados pessoais, termos de consentimento, cláusulas contratuais, políticas internas, relatórios de auditoria e treinamentos realizados com as equipes. Essa documentação serve não apenas como evidência de conformidade, mas também como ferramenta de governança e mitigação de riscos.

O Guia da ANPD sobre o “*Tratamento de Dados Pessoais pelo Poder Público*” ressalta, em seu tópico “(f) *Outros requisitos*”, que é importante avaliar a necessidade de elaboração de relatório de impacto à proteção de dados pessoais, de acordo com o caso concreto. Isso contribui para a conformidade do tratamento à legislação e também para a resposta aos riscos existentes.

Mapeamento de cláusulas para contratos entre Controlador e Operador	Referências
Obrigação do operador de manter registros relativos ao tratamento de dados pessoais, com condições de rastreabilidade e de prova eletrônica, inclusive sobre a destruição dos dados pessoais	▪ A – Cláusula 6.10, 10, 12 ▪ B – Cláusula 2.4 ▪ C – Cláusula 9, § 1º, IV ▪ E – Cláusula 10.9, 10.10 ▪ F – Item 7.2.8, 8.2.6 ▪ H – Item 5.37 ▪ J – Art. 37 ▪ L – Cláusula 10.1, 17
Obrigação do operador de manter registros da implementação das medidas de segurança para apoiar a demonstração de conformidade quando solicitado pelo controlador e por órgãos de controle	▪ A – Cláusula 6.1 ▪ B – Cláusula 2.4, § 2º ▪ C – Cláusula 9, § 1º, VIII
Obrigação do operador de contribuição quando da realização de auditorias das atividades de tratamento pelo controlador, bem como de disponibilização de documentação pertinente e resposta a consultas do controlador	▪ A – Cláusula 6.10, 10 ▪ B – Cláusula 2.4, § 1º ▪ C – Cláusula 9, § 1º, VI ▪ E – Cláusula 10.8, 10.9 ▪ F – Item 8.2.5
Obrigação do controlador em elaborar relatório de impacto	▪ F – Item 7.2.5 ▪ J – Art. 38

Especificidades para contratos entre Controladores conjuntos
O dever de documentação e de prestação de contas dos controladores está destacado em diversos trechos da LGPD, como a necessidade de manter os registros de operações de tratamento e de elaborar os relatórios de impacto à proteção de dados pessoais (Art. 37 e 38). Nesse aspecto, é importante que todos os controladores possam demonstrar, de forma coordenada, a adequação à LGPD. Recomenda-se que os controladores conjuntos estabeleçam procedimentos e responsabilidades sobre a documentação do tratamento e da implementação das medidas de segurança, a fim de se viabilizar resposta eficaz e eficiente a eventual auditoria ou solicitação de órgão de controle.

4.5. Compartilhamento posterior

A LGPD define, em seu art. 5º, inc. XVI, o uso compartilhado de dados como “(...) *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*”.

Entre os contratantes haverá compartilhamento de dados pessoais para a execução do objeto do acordo. O presente item trata dos casos em que a outra parte compartilha dados pessoais objeto do acordo com terceiros, subcontratados (operadores e suboperadores).

Nesse sentido, é fundamental que o contrato estabeleça cláusulas sobre a possibilidade de subcontratação, indicando se a outra parte poderá envolver terceiros no tratamento de dados pessoais, bem como os limites e as condições para esse compartilhamento. Caso seja permitida, a subcontratação deve estar condicionada à autorização do controlador, garantindo o controle sobre quem terá acesso aos dados pessoais.

Além disso, recomenda-se que o contrato preveja que qualquer subcontratado (operador ou suboperador) esteja igualmente sujeito às obrigações de proteção de dados pessoais estabelecidas no acordo principal, incluindo medidas técnicas e organizacionais de segurança, confidencialidade, cumprimento de prazos legais e atendimento às requisições dos titulares.

É importante manter registros atualizados sobre os subcontratados envolvidos e garantir que haja formalização dos acordos por meio de instrumentos jurídicos adequados. Dessa forma, o

compartilhamento de dados pessoais com terceiros ocorrerá de maneira controlada, transparente e em conformidade com os princípios da legislação.

O Guia da ANPD sobre o “*Tratamento de Dados Pessoais pelo Poder Público*” ressalta, em seu tópico “(b) *Objeto e finalidade*”, que é importante avaliar a compatibilidade entre a finalidade original da coleta dos dados pessoais e a finalidade do compartilhamento posterior. Por sua vez, no tópico “(g) *Outros requisitos*”, o documento destaca a necessidade de se formalizar a possibilidade de compartilhamento posterior e as condições aplicáveis.

Mapeamento de cláusulas para contratos entre Controlador e Operador	Referências
Especificação sobre a possibilidade ou não do compartilhamento posterior dos dados pessoais e as condições aplicáveis	▪ B – Cláusula 2.6, ▪ C – Cláusula 9, § 1º, VII ▪ D – Anexo I, Cláusulas 7.1, 7.2 ▪ E – Cláusula 10.3 ▪ F – Item 8.5.6 ▪ L – Cláusula 3, 18.1
Obrigação do operador de obter a anuência do controlador para o compartilhamento posterior, fornecendo cópia do contrato	▪ A – Cláusula 6.9 ▪ B – Cláusula 2.6 ▪ C – Cláusula 9, § 1º, VII ▪ E – Cláusula 10.4 ▪ F – Item 8.5.7 ▪ L – Cláusula 3, 18.1
Obrigação do operador de formalizar as obrigações do terceiro destinatário do compartilhamento posterior, incluindo a previsão de medidas de segurança na transferência dos dados pessoais, notificando o controlador sobre eventuais descumprimentos das obrigações pactuadas com o terceiro	▪ A – Cláusula 6.7, 6.9 e 7 ▪ B – Cláusula 2.5 ▪ C – Cláusula 9, § 1º, XIX ▪ E – Cláusula 10.7 ▪ F – Item 6.10.2.1, 6.12.1.2, 8.5.7 ▪ H – Item 5.14, 5.19, 5.20 ▪ J – Art. 47 ▪ L – Cláusula 3, 18.2
Obrigação do operador de analisar a compatibilidade da finalidade do compartilhamento posterior	▪ A – Cláusula 4, 6.9, Anexo B ▪ L – Cláusula 3, 18.2

Especificidades para contratos entre Controladores conjuntos
A definição quanto à autorização de compartilhamento posterior em contratos de controladoria conjunta possui a particularidade de que o compartilhamento deve ocorrer dentro dos limites estabelecidos pelo acordo entre os controladores conjuntos. É importante que o compartilhamento tenha a finalidade compatível com a finalidade original do tratamento e que seja respaldado por acordo com o terceiro que garanta a segurança dos dados e o atendimento aos direitos dos titulares.

5. Metodologia para implementação

Recomenda-se que a elaboração de modelos de cláusulas de proteção de dados pessoais pelos órgãos e entidades seja realizada após a implementação do “*Controle 15. Relação/lista dos*

contratos”. Isto porque o mapeamento dos contratos poderá gerar informações úteis para os gestores públicos, que poderão identificar padrões de contratação. Sugere-se que contratações que sejam frequentes e padronizadas, ou que ocorram em grande volume, possuam uma minuta de contrato que inclua cláusulas de proteção de dados pessoais, se necessário. Assim, as cláusulas devem ser adaptadas para o contexto de cada contratação.

O procedimento de adequação dos contratos pode ser realizado de várias maneiras. Para contratações que ainda não ocorreram, é possível editar minutas de contratos para inclusão de cláusulas de proteção de dados pessoais. Para contratações em andamento, é possível aditar os contratos para inclusão das cláusulas aplicáveis.

5.1. Competências e responsabilidades

Para a implementação do presente controle, há quatro importantes atores: (i) unidade de gestão contratual¹⁴; (ii) unidade de tecnologia e/ou segurança da informação; (iii) unidade de assessoramento jurídico; e (iv) coordenador da implantação dos controles.

Recomenda-se que seja designado responsável por coordenar a implementação deste controle, que realizará a interlocução com as áreas conforme as respectivas competências. À unidade de gestão contratual caberá avaliar as cláusulas que seriam aplicáveis a determinada contratação, com apoio da unidade de assessoramento jurídico e da unidade de tecnologia e/ou segurança da informação.

5.2. Formalização e aprovação

Para a aprovação e disponibilização dos modelos de cláusulas aplicáveis a determinado tipo de relação jurídica, após a análise da unidade de assessoramento jurídico do órgão ou da entidade, é importante que as cláusulas sejam formalizadas e aprovadas por decisão administrativa dos gestores competentes, para observância dos agentes públicos do órgão ou da entidade.

¹⁴ Eventualmente, também a unidade responsável pela formalização de termos de colaboração, termos de fomento, acordos de cooperação e contratos de gestão celebrados pela Administração Municipal com organizações da sociedade civil, conforme discutido na seção 3 deste Manual.

6. Referências

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27001:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2022.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27002:2022. Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27557:2023. Segurança da Informação, segurança cibernética e proteção da privacidade – Aplicação da ABNT NBR ISO 31000:2018 para gestão de riscos de privacidade organizacional. Rio de Janeiro: ABNT, 2023.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27701:2020. Tecnologia de segurança – Extensão da ABNT NBR/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes. Rio de Janeiro: ABNT, 2024.

BRASIL. Advocacia-Geral da União. Modelos da Lei nº 14.133/21 para pregão e concorrência. Modelo Contrato Serviços Sem Mão de Obra Lei 14.133 (setembro/2025). Disponível em: <https://www.gov.br/agu/pt-br/composicao/cgu/cgu/modelos/licitacoescontratos/14133/pregao-e-concorrencia>. Acesso em 01/10/2025.

BRASIL, Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>. Acesso em 14/07/2025.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 19, de 23 de agosto de 2024. Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396>. Acesso em: 14/07/2025.

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo. Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Maio de 2021. Brasília, DF. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf> Acesso em: 24/07/2025

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo. Tratamento de Dados Pessoais pelo Poder Público. Versão 2.0 Jun/2023. Brasília, DF. Disponível em: <<https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>> Acesso em: 14/07/2025

BRASIL. Autoridade Nacional de Proteção de Dados. Consulta Pública. Regulamento sobre o Uso Compartilhado de Dados Pessoais pelo Poder Público. Brasília, DF. Disponível em:

<<https://www.gov.br/participamaisbrasil/regulamento-sobre-o-uso-compartilhado-de-dados-pessoais-pelo-poder-publico>> Acesso em: 24/11/2025

BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, *Diário Oficial da União*, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 29/10/2024.

MATO GROSSO DO SUL. Procuradoria-Geral do Estado. Pareceres Referencias e Minutas-Padrão. Disponível em: <https://www.pge.ms.gov.br/wp-content/uploads/2021/12/Minuta-Padiao.pdf>. Acesso em 14/07/2025.

PERNAMBUCO. Procuradoria-Geral do Estado. Instrumentos Padronizados. Disponível em: https://www.pge.pe.gov.br/App_Themes/CONTRATO_SERVICOS_comuns_ou_especiais_v12.pdf. Acesso em: 14/07/2025.

REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. Guia para a Implementação de Cláusulas Contratuais Modelo Para a Transferência Internacional de Dados Pessoais. Disponível em: <https://www.redipd.org/pt/document/guia-implementacao-clausulas-contratuais-modelo-tidp-pt.pdf>. Acesso em: 14/07/2025.

REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. Anexo Modelo de Cláusulas Contratuais. Disponível em: <https://www.redipd.org/pt/document/anexo-modelos-clausulas-contratuais-pt.pdf>. Acesso em: 14/07/2025.

RIO DE JANEIRO (Cidade). Secretaria de Integridade, Transparência e Proteção de Dados (SMIT). Minuta de Termo Aditivo ao Contrato (ou Instrumento Congênere). Disponível em: <https://lgpd.prefeitura.rio/wp-content/uploads/sites/102/2023/07/Minuta-de-Termo-Aditivo-Cla%CC%81usulas-Contratuais_Orientac%CC%A7o%CC%83es_Controlador_Operador_VFinal_SMTDI.docx.pdf> Acesso em: 07/08/2025

SÃO PAULO (Cidade). Decreto Municipal nº 59.767, de 15 de setembro de 2020. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) - no âmbito da Administração Municipal direta e indireta. São Paulo, *Diário Oficial da Cidade de São Paulo*, 15 de setembro de 2020. Disponível em: <<https://legislacao.prefeitura.sp.gov.br/leis/decreto-59767-de-15-de-setembro-de-2020>>. Acesso em: 29/10/2024.

SÃO PAULO (Cidade). Decreto Municipal nº 57.783, de 13 de julho de 2017. Dispõe sobre a Política de Gestão Documental e o Sistema de Arquivos do Município de São Paulo. São Paulo, *Diário Oficial da Cidade*, 13 de julho de 2017. Disponível em: <<https://legislacao.prefeitura.sp.gov.br/leis/decreto-57783-de-13-de-julho-de-2017>>. Acesso em: 02/10/2025.

SÃO PAULO (Cidade). Decreto Municipal nº 62.100, de 27 de dezembro de 2022. Dispõe sobre normas de licitação e contratos administrativos para a Administração Pública direta, autárquica e fundacional do Município de São Paulo, nos termos previstos na Lei Federal nº 14.133, de 1º de abril de 2021, bem como consolida a regulamentação da matéria em âmbito municipal. São Paulo, *Diário Oficial da Cidade*, 27 de dezembro de 2022. Disponível em:

<<https://legislacao.prefeitura.sp.gov.br/leis/decreto-62100-de-27-de-dezembro-de-2022>>. Acesso em: 19/09/2025.

SÃO PAULO (Cidade). Portaria CGM/SP nº 27, de 22 de Junho de 2026. Regulamenta o modelo de Programa de Governança em Privacidade e Proteção de Dados Pessoais da Administração Pública Municipal (PGPP), assim como o procedimento do Diagnóstico de Maturidade em Proteção de Dados Pessoais. Disponível em: <<https://legislacao.prefeitura.sp.gov.br/portaria-controladoria-geral-do-municipio-cgm-27-de-22-de-junho-de-2026>>. Acesso em: 23/06/2026.

SÃO PAULO (Cidade). Portaria da Secretaria de Governo Municipal - SGM/SEGES/CGDOC nº 1 de 24 de Maio de 2021. Implementa a Política Municipal de Gestão Documental (PGDOC), instituída pelo Decreto Municipal nº 57.783, de 13 de julho de 2017, e dá outras providências. São Paulo, *Diário Oficial da Cidade*, 24 de maio de 2021. Disponível em: <<https://legislacao.prefeitura.sp.gov.br/leis/portaria-1-de-24-de-maio-de-2021>>. Acesso em: 02/10/2025.

Apêndice I – Exemplos da atuação do controlador e do operador

Situação 1: Controlador e operador

A “Secretaria Municipal B” contratou a “Fundação X” para realizar um levantamento de dados sobre as famílias e pessoas moradoras numa determinada área da cidade que possui histórico de alagamentos frequentes, com o objetivo de planejar sua remoção daquele local de risco e a sua realocação em um novo conjunto habitacional que será construído numa área sem risco de inundações. Por meio de visitas e entrevistas com os moradores do local, a Fundação X fará a identificação de todos os moradores da comunidade, incluindo o registro de nome completo, sexo/gênero, data de nascimento, RG, nível de escolaridade, ocupação, renda individual, etc. Após a realização desse levantamento, a Fundação X deve entregar à Secretaria B um banco de dados eletrônico com todos os dados coletados e um relatório analítico com as informações de quantidade e perfil das famílias e pessoas moradoras da área, com o objetivo de subsidiar o planejamento do novo conjunto habitacional.

Neste exemplo, a Secretaria Municipal B é o agente controlador, pois coube a ela as decisões sobre as finalidades do tratamento de dados pessoais (realizar estudos para subsidiar o planejamento de moradias), os dados pessoais a serem tratados (identificação e características sociodemográficas) e os tipos de tratamento de dados realizados, como coleta, armazenamento, processamento, classificação, análise etc.

Por sua vez, a Fundação X é o agente operador, uma vez que realiza o tratamento de dados pessoais em nome do controlador e conforme a finalidade e instruções por ele determinadas, sem autonomia decisória quanto aos meios e objetivos do tratamento.

Situação 2: Controladores conjuntos

A “Secretaria Municipal C” e a “Secretaria Estadual E” firmaram uma parceria para implantar um sistema integrado de controle de acesso e segurança predial nos edifícios que ambas ocupam. O objetivo é unificar o cadastro de visitantes, tornando o processo de entrada mais ágil e seguro e permitindo o compartilhamento de registros entre as unidades administrativas. Para isso, as duas secretarias contrataram conjuntamente a “Empresa de Segurança Y” para executar o serviço de controle de acesso e recepção de visitantes. Dentre as responsabilidades da Empresa Y definidas em contrato, está o registro do nome completo, número de RG, telefone de contato e fotografia facial de todos os visitantes, bem como o armazenamento dessas informações por 30 dias após a data da visita. Os dados são utilizados para identificar e autorizar o ingresso de pessoas, bem como para gerar relatórios de segurança e monitoramento de acessos em ambas as secretarias.

Neste caso, a Secretaria Municipal C e a Secretaria Estadual E são controladoras conjuntas, pois decidem de forma convergente sobre as finalidades e os meios do tratamento de dados pessoais. Ambas determinam o uso do sistema integrado, a base de dados compartilhada e as regras de gestão da informação. Há, portanto, interdependência e cooperação entre as controladoras quanto às decisões essenciais sobre o tratamento.

A Empresa de Segurança Y, por sua vez, atua como operadora, executando o tratamento de dados pessoais em nome das controladoras conjuntas e de acordo com as instruções por elas definidas.

Situação 3: Controlador, operador e suboperador
A “Secretaria Municipal D” contratou a “Empresa Z” para implementar e operar um serviço de atendimento ao cidadão, com o objetivo de registrar solicitações e reclamações sobre serviços de limpeza e zeladoria urbana. A Empresa Z, por sua vez, subcontratou um serviço de atendimento automatizado pelo aplicativo de mensagens da “Empresa ZapIA” e que usa inteligência artificial para agilizar o contato com os cidadãos e o registro das solicitações e reclamações no serviço de atendimento. Para essa finalidade, os munícipes devem informar seu número de CPF, o CEP de sua residência e confirmar seu endereço completo, sendo que o aplicativo ZapIA automaticamente coleta e registra o número de telefone e a localização do celular que está realizando a solicitação ou reclamação. Após isso, se necessário, o munícipe é direcionado para uma central telefônica, onde pessoas empregadas da Empresa Z prosseguem com o atendimento. Neste exemplo, a Secretaria D atua como controladora pois é a responsável por definir as finalidades e os meios de tratamento de dados pessoais (identificação de pessoas que solicitam ou reclamam de serviços de limpeza e zeladoria urbana; identificação e pré-atendimento automatizado dessas pessoas). A Empresa Z exerce o papel de operadora, pois está realizando o tratamento de dados pessoais de acordo com as instruções e orientações definidas pela Secretaria D, controladora, sem definir por conta própria as finalidades do tratamento. Por fim, a empresa responsável pelo aplicativo ZapIA, exerce o papel de suboperadora neste processo de tratamento de dados pessoais, pois é contratada pela operadora Empresa Z para auxiliá-la a realizar o tratamento de dados pessoais em nome da controladora Secretaria D.



**PREFEITURA DE
SÃO PAULO**