

**ANEXO SEI Nº 27154439/2025 - SAP.ARC.AUN****ANEXO IV - CLÁUSULAS DE PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO****FUNDAMENTOS JURÍDICOS E GOVERNANÇA****CLÁUSULA PRIMEIRA - DEFINIÇÕES E POSIÇÕES DAS PARTES**

1.1. A CONTRATADA deverá observar e cumprir rigorosamente todos os dispositivos legais previstos na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), na Lei nº 12.965/2014 (Marco Civil da Internet) e demais normas aplicáveis à proteção de dados pessoais e segurança da informação.

1.2. Para os fins desta contratação e em conformidade com a LGPD:

a) A CONTRATANTE será considerada CONTROLADORA, sendo responsável por definir as finalidades e os meios de tratamento dos dados pessoais;

b) A CONTRATADA será considerada OPERADORA, sendo responsável por realizar o tratamento dos dados pessoais em nome da CONTRATANTE e exclusivamente de acordo com as instruções documentadas e fornecidas pela CONTRATANTE.

c) Eventuais subcontratadas deverão assumir idênticas obrigações.

**CLÁUSULA SEGUNDA - BASE LEGAL, FINALIDADE E TRANSPARÊNCIA**

2.1. O tratamento de dados pessoais, em especial os de natureza biométrica, será realizado exclusivamente para a finalidade de segurança pública, nos termos dos artigos 7º, III, e 23 da LGPD.

2.2. É vedada a utilização dos dados para qualquer outro objetivo, bem como sua cessão ou comercialização.

2.3. A CONTRATADA manterá políticas de boas práticas e demais documentos relacionados à segurança da informação e proteção de dados atualizadas, incluindo mas não se limitando à: Política de Segurança da Informação, Política de Proteção de Dados e Privacidade, Processos e Procedimentos operacionais, Mapa de Riscos e Impactos, Plano de Mitigação de Riscos, Plano de Resposta a Incidentes e Plano de Recuperação de Desastres.

**CLÁUSULA TERCEIRA - RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (RIPD)**

3.1. Antes da entrada em operação do sistema, a CONTRATADA apresentará Relatório de Impacto à Proteção de Dados, elaborado em conformidade com padrões internacionais de avaliação (ISO/IEC 29134), descrevendo fluxos de dados, riscos, medidas de mitigação e planos de contingência.

3.2. O relatório será submetido ao Encarregado de Tratamento de Dados Pessoais do Município e deverá ser atualizado semestralmente ou sempre que houver alterações significativas no sistema.

**CLÁUSULA QUARTA - GOVERNANÇA E CONTROLE SOCIAL**

4.1. Será instituído Comitê Gestor do Sistema de Videomonitoramento, composto inicialmente por profissionais técnicos da área de segurança pública do Município, acompanhados de representantes da Procuradoria-Geral, Controladoria-Geral e Encarregado de Tratamento de Dados Pessoais do Município.

4.2. O Comitê será incumbido de avaliar casos críticos, incluindo incidentes de segurança, situações de viés algorítmico, reconhecimentos equivocados e alertas de alto impacto social.

4.3. O Comitê analisará, sempre que necessário, a documentação técnica de apoio à explicabilidade das decisões automatizadas, podendo recomendar ajustes ou medidas corretivas.

4.4. A CONTRATADA deverá realizar auditorias regulares de toda a solução com intervalo não superior a 6 (seis) meses, apresentando relatórios ao Comitê Gestor e à CONTRATANTE, contemplando informações claras e compreensíveis sobre os critérios técnicos utilizados pelos sistemas de inteligência artificial.

**CLÁUSULA QUINTA - DIREITOS DOS TITULARES**

5.1. A CONTRATADA deverá colaborar com a CONTRATANTE no atendimento aos direitos dos titulares de dados previstos nos artigos 17 a 22 da LGPD, incluindo acesso, retificação, anonimização, bloqueio, eliminação e oposição ao tratamento.

5.2. As solicitações dos titulares deverão ser atendidas observando-se os prazos estabelecidos na Lei de Acesso à Informação (Lei nº 12.527/2011): 20 (vinte) dias corridos, prorrogáveis por mais 10 (dez) dias corridos, mediante justificativa expressa, conforme artigo 11, §§ 1º e 2º da referida lei.

5.3. A CONTRATADA manterá procedimentos claros para o exercício dos direitos dos titulares, garantindo canais de comunicação acessíveis e resposta adequada às solicitações, em conformidade com os

## **SEGURANÇA E PROTEÇÃO TÉCNICA**

### **CLÁUSULA SEXTA - MEDIDAS DE SEGURANÇA DA INFORMAÇÃO**

6.1. A CONTRATADA deverá adotar medidas técnicas e organizacionais aptas a proteger os dados pessoais contra acessos não autorizados, destruição acidental ou ilícita, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

6.2. Medidas de Criptografia e Proteção de Dados:

- a) Implementar criptografia para dados em trânsito e em repouso;
- b) Utilizar algoritmos de criptografia reconhecidos internacionalmente;
- c) Realizar backup seguro dos dados com criptografia adequada.

6.3. Controles de Acesso e Autenticação:

- a) Implementar controles de acesso baseados no princípio do menor privilégio;
- b) Utilizar autenticação multifator para acesso aos sistemas;
- c) Manter trilhas de auditoria completas de todos os acessos.

6.4. Proteção de Dados Sensíveis e Biométricos:

- a) O reconhecimento facial será tratado como dado sensível, exigindo salvaguardas adicionais de proporcionalidade, minimização e restrição de acesso;
- b) Implementar monitoramento específico contra vieses algorítmicos;
- c) O sistema descartará automaticamente registros/alertas com níveis de confiabilidade abaixo do percentual estabelecido tecnicamente;
- d) Nenhuma decisão automatizada poderá produzir efeitos jurídicos relevantes sem revisão humana qualificada.

6.5. Testes e Monitoramento:

- a) Realizar testes periódicos de vulnerabilidade e penetração;
- b) Manter planos atualizados de continuidade e recuperação de desastres;
- c) Implementar sistema de monitoramento contínuo de segurança.

6.6. A CONTRATADA se compromete a implementar o conceito de Privacy by Design, assegurando que a privacidade e a proteção de dados pessoais sejam incorporadas desde a concepção do sistema até seu ciclo final de vida. E, o conceito *Privacy by Default*, adotando soluções técnicas e organizacionais que garantam a proteção de dados em todo o ciclo de vida do serviço, incluindo, mas não se limitando ao controle de acessos com registro de logs, gestão de perfis de acesso, capacidade de anonimização ou pseudonimização dos dados sempre que viável e atualização periódica das soluções de segurança e controle.

### **CLÁUSULA SÉTIMA - TREINAMENTO E CAPACITAÇÃO**

7.1. A CONTRATADA assegurará que todos os profissionais envolvidos na operação, manutenção e suporte do sistema recebam treinamento adequado e contínuo em proteção de dados pessoais, segurança da informação e uso responsável das tecnologias de reconhecimento facial.

7.2. O conteúdo mínimo do treinamento abrangerá:

- a) Fundamentos da LGPD e direitos dos titulares;
- b) Boas práticas de segurança da informação;
- c) Protocolos de resposta a incidentes;
- d) Prevenção de vieses e explicabilidade dos sistemas de inteligência artificial;
- e) Procedimentos específicos para tratamento de dados biométricos.

7.3. A CONTRATANTE poderá acompanhar e validar os programas de capacitação, devendo a CONTRATADA manter registro das ações de treinamento realizadas.

## **OPERAÇÕES E GESTÃO DE DADOS**

### **CLÁUSULA OITAVA - HOSPEDAGEM, ARMAZENAMENTO E TRANSFERÊNCIA DE DADOS**

8.1. Os dados serão armazenados obrigatoriamente em datacenters localizados em território nacional, sendo vedada a transferência internacional sem autorização formal e prévia do Município.

8.2. Havendo necessidade de transferência internacional de dados, devidamente acordada com a CONTRATANTE, a CONTRATADA se compromete a:

- a) Observar rigorosamente o disposto nos artigos 33 a 36 da LGPD;
- b) Assegurar a adoção de cláusulas contratuais específicas e garantias adequadas;
- c) Demonstrar conformidade com os padrões exigidos pela ANPD;
- d) Comunicar formalmente à CONTRATANTE sobre a transferência.

8.3. A CONTRATADA não poderá compartilhar, ceder, vender ou disponibilizar os dados pessoais a terceiros, exceto quando expressamente autorizado pela CONTRATANTE, para cumprimento de ordem judicial ou para atendimento de requisições de órgãos de controle.

8.4 O armazenamento de dados e imagens deve observar os prazos técnicos definidos no contrato, sendo obrigatória a eliminação segura dos dados ao término do contrato, salvo obrigações legais ou expressa deliberação da CONTRATANTE.

#### **CLÁUSULA NONA - GESTÃO DE INCIDENTES E CORREÇÃO DE VULNERABILIDADES**

9.1. A CONTRATADA manterá acordo de níveis de serviço específico para incidentes de segurança, estabelecendo prazos claros para resposta, comunicação e mitigação baseados na criticidade do incidente.

9.2. Procedimentos para Incidentes de Segurança, devem observar a Resolução CD/ANPD nº15/2024:

a) Notificar a CONTRATANTE no prazo máximo de 24 (vinte e quatro) horas a contar da ciência do incidente;

b) Apresentar, em até 48 (quarenta e oito) horas, relatório técnico detalhado contendo a descrição do ocorrido, os dados afetados, medidas adotadas e responsáveis pelo tratamento;

c) Colaborar com a CONTRATANTE no cumprimento das obrigações de comunicação à ANPD e aos titulares dos dados, quando aplicável.

9.3. Correção de Vulnerabilidades:

a) As vulnerabilidades críticas deverão ser corrigidas em até 24 horas;

b) As vulnerabilidades altas deverão ser corrigidas em até 72 horas;

c) As vulnerabilidades médias e baixas deverão ser corrigidas conforme cronograma acordado;

d) A CONTRATADA disponibilizará toda a documentação comprobatória das providências adotadas.

#### **CLÁUSULA DÉCIMA - RETENÇÃO, DESCARTE E PORTABILIDADE DOS DADOS**

10.1. As imagens e informações coletadas terão prazo máximo de retenção de 15 dias, salvo ordem judicial ou vínculo a ocorrência oficial devidamente registrada.

10.2. Procedimentos de Descarte:

a) O descarte dos dados será realizado de forma segura e irreversível;

b) A CONTRATADA fornecerá certificado de eliminação segura dos dados;

c) Ao término do contrato, os dados deverão ser entregues à CONTRATANTE em formato aberto e padrão não proprietário.

10.3. Portabilidade de Dados:

a) A CONTRATANTE terá direito à portabilidade integral dos dados a qualquer tempo;

b) Os dados serão entregues em formato estruturado, de uso comum e leitura automatizada;

c) A migração não poderá implicar em perda de funcionalidades ou informações.

#### **CLÁUSULA DÉCIMA PRIMEIRA - REGISTRO DE OPERAÇÕES E AUDITABILIDADE**

11.1. Todas as operações de tratamento deverão ser registradas em conformidade com o art. 37 da LGPD, possibilitando rastreabilidade e auditoria integral.

11.2. Registros Obrigatórios:

a) Acessos realizados: identificação do usuário, data, horário e finalidade do acesso;

b) Decisões automatizadas: registro de cada alerta ou reconhecimento facial, com taxa de confiabilidade e parâmetros utilizados;

c) Alterações nos dados: histórico de retenção, descarte ou exportação de informações;

d) Incidentes de segurança: logs de tentativas de acesso indevido, falhas ou vulnerabilidades detectadas.

11.3. A CONTRATANTE poderá, a qualquer tempo, solicitar documentos e realizar auditorias para verificação do cumprimento da legislação de proteção de dados, com comunicação prévia de 10 (dez) dias úteis.

#### **RESPONSABILIDADES E COMPLIANCE**

##### **CLÁUSULA DÉCIMA SEGUNDA - CONFIDENCIALIDADE E SUBCONTRATAÇÃO**

12.1. Termos de Confidencialidade:

a) Todos aqueles que tiverem acesso aos dados deverão firmar termos específicos de compromisso, sigilo e confidencialidade;

b) Os termos constituem instrumento de responsabilização em casos de incidentes ou vazamentos;

c) A violação dos termos sujeitará o infrator às sanções contratuais e legais cabíveis.

12.2. Subcontratação:

a) Qualquer subcontratação que envolva tratamento de dados dependerá de autorização expressa e prévia da CONTRATANTE;

b) Os subcontratados ficarão vinculados às mesmas obrigações de proteção de dados e segurança da informação;

c) A CONTRATADA permanece integralmente responsável pelos atos de seus subcontratados.

### CLÁUSULA DÉCIMA TERCEIRA - INTEGRAÇÃO COM CÂMERAS PRIVADAS

13.1. A integração do sistema com câmeras privadas dependerá de termo formal firmado com os proprietários, observada a base legal adequada ao caso concreto.

13.2. Os termos de integração deverão delimitar claramente as responsabilidades quanto ao compartilhamento das imagens e à proteção dos dados pessoais captados.

13.3. A CONTRATADA auxiliará na elaboração dos instrumentos jurídicos necessários para a integração, garantindo conformidade com a LGPD.

### CLÁUSULA DÉCIMA QUARTA - SANÇÕES E ATUALIZAÇÃO LEGISLATIVA

14.1. Sanções por Descumprimento:

a) O descumprimento das cláusulas de proteção de dados sujeitará a CONTRATADA às sanções administrativas previstas no contrato;

b) A CONTRATADA responderá civil e criminalmente pelos danos causados aos titulares de dados;

c) A CONTRATANTE poderá exercer direito de regresso em caso de condenação ou aplicação de multa pela ANPD.

14.2. Vigência Pós-Contratual: As obrigações relacionadas à proteção de dados permanecerão válidas após o término do contrato, especialmente quanto à confidencialidade e eliminação segura dos dados.

14.3. Adequação Legislativa: Em caso de alterações na legislação de proteção de dados durante a vigência do contrato, a CONTRATADA deverá adequar-se às novas exigências sem ônus adicional para a CONTRATANTE, no prazo máximo de 90 (noventa) dias da publicação da nova norma.



Documento assinado eletronicamente por **Evelin Fernanda Vargas, Coordenador(a)**, em 06/11/2025, às 16:48, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.



Documento assinado eletronicamente por **Paulo Rogerio Rigo, Secretário (a)**, em 06/11/2025, às 16:57, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.



Documento assinado eletronicamente por **Paulo Isaias Stremel de Almeida, Gerente**, em 07/11/2025, às 09:03, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.



Documento assinado eletronicamente por **Rodolfo Lauro Weinert, Diretor (a) Executivo (a)**, em 07/11/2025, às 13:15, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.



A autenticidade do documento pode ser conferida no site <https://portalsei.joinville.sc.gov.br/> informando o código verificador **27154439** e o código CRC **C02009ED**.

Av. Hermann August Lepper, 10 - Bairro Saguau - CEP 89221-005 - Joinville - SC - [www.joinville.sc.gov.br](http://www.joinville.sc.gov.br)