ANEXO VIII DO CONTRATO - DIRETRIZES DE GOVERNANÇA E PROTEÇÃO DE DADOS PESSOAIS

CONTRATO DE CONCESSÃO ADMINISTRATIVA Nº [●]/[●] PARCERIA PÚBLICO-PRIVADA — PLATAFORMA DE CIDADE INTELIGENTE MUNICÍPIO DE DIVINÓPOLIS/MG

1. OBJETO E APLICAÇÃO

1.1. Este ANEXO estabelece as diretrizes de governança da informação, de segurança e de proteção de dados pessoais aplicáveis a todo tratamento realizado na execução da CONCESSÃO, na forma do Capítulo XI do CONTRATO.

1.2. Aplica-se a todos os dados captados, transmitidos, armazenados, processados ou gerados pelos SISTEMAS DE CIDADE INTELIGENTE, incluídos imagens, vídeos, metadados, registros de conexão, dados de geolocalização, leituras de sensores, telemetria de iluminação, registros de atendimento e logs de auditoria.

1.3. Aplica-se à CONCESSIONÁRIA, a seus empregados, prepostos, fornecedores, integradores, provedores de nuvem e demais contratados, cabendo à CONCESSIONÁRIA estender-lhes contratualmente as obrigações aqui previstas e responder integralmente perante o PODER CONCEDENTE.

1.4. O cumprimento deste ANEXO é aferido pelo VERIFICADOR INDEPENDENTE e reflete-se no ICGD — ÍNDICE DE CONFORMIDADE EM GOVERNANÇA DE DADOS, que compõe o critério CGD do IDGMS, na forma do ANEXO II.

2. PAPÉIS E RESPONSABILIDADES

2.1. Para todos os fins da Lei Federal nº 13.709/2018 (LGPD):

MINUTA

Papel	Titular	Competências
CONTROLADOR	PODER CONCEDENTE	decisões sobre finalidade, base legal, hipóteses de compartilhamento, prazos de retenção, políticas de acesso e resposta a titulares
OPERADOR	CONCESSIONÁRIA	tratamento conforme instruções documentadas do controlador; implantação e manutenção das medidas técnicas e organizacionais
ENCARREGADO	designado pelo PODER CONCEDENTE	canal de comunicação com titulares e com a ANPD
PREPOSTO DE DADOS	designado pela CONCESSIONÁRIA	interlocução técnica permanente com o encarregado e com o VERIFICADOR INDEPENDENTE

2.1.1. A CONCESSIONÁRIA atua como controladora apenas quanto aos dados que trate por interesse próprio — notadamente de seus empregados, fornecedores e das ATIVIDADES RELACIONADAS regularmente autorizadas —, hipótese em que responde autonomamente perante os titulares e a ANPD.

2.2. Instruções documentadas. O PODER CONCEDENTE formalizará suas instruções por escrito, mantendo-se registro auditável de cada uma, com identificação do agente emissor, data e fundamento.

2.3. Dever de advertência. Recebendo instrução que repute contrária à LGPD, a CONCESSIONÁRIA advertirá formalmente o PODER CONCEDENTE, por escrito e com cópia ao VERIFICADOR INDEPENDENTE, antes de executá-la.

2.3.1. A advertência formal, quando desatendida, transfere ao PODER CONCEDENTE o risco das sanções e custos decorrentes, na forma do item 41.2.iii do CONTRATO.

2.3.2. A ausência de advertência, quando a desconformidade era técnica e juridicamente aferível pela CONCESSIONÁRIA, mantém o risco com esta.

2.4. A CONCESSIONÁRIA designará preposto de dados até o término da FASE 0 e manterá equipe dedicada à segurança da informação, com qualificação comprovada.

MINUTA

3. FINALIDADES, BASES LEGAIS E MINIMIZAÇÃO

3.1. O tratamento limita-se às seguintes finalidades:

#	Finalidade	Base legal indicativa
i	execução dos SERVIÇOS e operação dos SISTEMAS DE CIDADE INTELIGENTE	art. 7º, III e V, da LGPD
ii	segurança e preservação de logradouros públicos	art. 7º, III, da LGPD; art. 149-A da CF
iii	apoio à resposta a emergências e à defesa civil	art. 7º, IV e VIII, da LGPD
iv	fiscalização contratual e aferição de desempenho	art. 7º, III, da LGPD
v	atendimento a requisição de autoridade competente	art. 7º, II e III, da LGPD
vi	continuidade do serviço público após a extinção da CONCESSÃO	art. 7º, III, da LGPD

3.1.1. É vedado qualquer tratamento para finalidade não relacionada no item 3.1.

3.2. Minimização. A captação, o armazenamento e o processamento limitar-se-ão ao necessário à finalidade declarada, sendo vedada a captação deliberada de interior de imóveis, de áreas privadas e de espaços de expectativa legítima de privacidade.

3.2.1. Sempre que o posicionamento de dispositivo alcançar área privada de forma inevitável, será aplicada máscara de privacidade irreversível no próprio equipamento, registrada em projeto e verificada no comissionamento.

3.3. Vedação de vigilância dirigida. É vedado o direcionamento de dispositivos, o uso de analítica ou a extração de relatórios com o propósito de acompanhar pessoa determinada, salvo mediante requisição de autoridade competente, registrada na forma do item 6.

3.4. Transparência. O PODER CONCEDENTE manterá publicada a relação georreferenciada dos pontos de monitoramento, as finalidades do tratamento, os prazos de retenção e os canais de exercício de direitos, e a CONCESSIONÁRIA instalará sinalização informativa nas áreas monitoradas, na forma do ANEXO I.

4. CICLO DE VIDA E RETENÇÃO

4.1. Os prazos máximos de retenção são os seguintes, contados da captação:

MINUTA

Categoria	Prazo de retenção	Observação
Imagens de videomonitoramento	30 dias	eliminação automática após o prazo
Imagens objeto de requisição formal de autoridade	prazo da requisição	preservadas em repositório segregado
Metadados de analítica de vídeo	90 dias	
Registros de conexão do WI-FI PÚBLICO	1 (um) ano	art. 15 do Marco Civil da Internet
Leituras de sensores ambientais	5 anos	dado não pessoal, salvo se associável
Telemetria de iluminação pública	5 anos	dado não pessoal
Registros de atendimento aos usuários	5 anos	
Logs de auditoria de acesso	5 anos	não podem ser inferiores ao prazo do dado auditado

4.2. A eliminação será automática, irreversível e registrada em log, vedada a retenção além do prazo e vedado o arquivamento paralelo em qualquer ambiente da CONCESSIONÁRIA.

4.3. A prorrogação de prazo de retenção depende de instrução escrita do PODER CONCEDENTE, com indicação da base legal e do prazo adicional, e será registrada no relatório trimestral.

5. SEGURANÇA DA INFORMAÇÃO

5.1. A CONCESSIONÁRIA implantará e manterá, no mínimo:

i. criptografia dos dados em trânsito e em repouso, com algoritmos e comprimentos de chave reconhecidos e revisados periodicamente;
ii. segregação de ambientes de produção, homologação e desenvolvimento, sendo vedado o uso de dados pessoais reais em ambientes não produtivos sem anonimização;
iii. controle de acesso baseado em papéis, com privilégio mínimo, autenticação multifator para acessos administrativos e revisão periódica de credenciais;
iv. registro de auditoria íntegro e não repudiável de todo acesso, consulta, exportação e alteração;

MINUTA

v. gestão de vulnerabilidades, com varredura periódica e aplicação de correções de segurança nos prazos do ANEXO I;

vi. testes de intrusão independentes, no mínimo anuais, com plano de remediação e reteste;

vii. cópias de segurança com testes periódicos de restauração e plano de recuperação de desastres, com objetivos de tempo e de ponto de recuperação definidos no ANEXO I;

viii. segmentação de rede e isolamento dos ambientes críticos; e

ix. plano de resposta a incidentes documentado, testado ao menos anualmente.

5.2. Localização dos dados. Os dados serão armazenados e processados em território nacional, sendo vedada transferência internacional sem autorização prévia, expressa e específica do PODER CONCEDENTE e sem observância dos arts. 33 a 36 da LGPD.

5.3. Subcontratados e nuvem. A utilização de provedores de nuvem ou de qualquer sub-operador depende de autorização prévia do PODER CONCEDENTE e da assunção contratual, pelo sub-operador, das obrigações deste ANEXO, permanecendo a CONCESSIONÁRIA integralmente responsável.

5.4. Sanitização de mídias. A substituição, o descarte ou a devolução de qualquer mídia que tenha armazenado dados exige sanitização certificada ou destruição física documentada, na forma do item 4.3 do ANEXO V.

6. ACESSO, REQUISIÇÕES E CADEIA DE CUSTÓDIA

6.1. O acesso às imagens e às bases é privativo dos agentes públicos formalmente credenciados pelo PODER CONCEDENTE, por meio de credencial individual e intransferível, vedado o compartilhamento de contas.

6.2. Toda consulta, visualização, exportação e download será registrada com: identificação do agente; data e hora; ativo consultado; período consultado; e motivação declarada.

6.3. As requisições de autoridade competente serão atendidas mediante ato formal, registrado em protocolo próprio, cabendo ao PODER CONCEDENTE, na qualidade de controlador, decidir sobre o atendimento.

MINUTA

6.3.1. A CONCESSIONÁRIA não atenderá requisição diretamente, devendo encaminhá-la ao PODER CONCEDENTE, salvo determinação judicial que lhe seja diretamente dirigida, hipótese em que comunicará o fato imediatamente.

6.4. A exportação de imagens observará procedimento de cadeia de custódia, com geração de resumo criptográfico do arquivo, registro do responsável pela extração e termo de entrega, de modo a assegurar a integridade e a rastreabilidade da prova.

7. TRATAMENTO DE DADOS BIOMÉTRICOS E RECONHECIMENTO FACIAL

7.1. A ativação de qualquer funcionalidade de reconhecimento facial depende do atendimento cumulativo das seguintes condições, na forma da Cláusula 62 do CONTRATO:

i. ato normativo municipal que defina a finalidade, a base legal, as hipóteses de uso, as autoridades competentes e os controles aplicáveis;
ii. relatório de impacto à proteção de dados pessoais (RIPD) específico, elaborado e publicado previamente à ativação;
iii. utilização exclusiva de bases oficiais fornecidas ou indicadas pelo PODER CONCEDENTE, vedada a constituição de base biométrica própria pela CONCESSIONÁRIA;
iv. revisão humana obrigatória de todo resultado antes de qualquer providência operacional, vedada medida automatizada com efeito sobre pessoa determinada; e
v. registro auditável de cada consulta, com identificação do agente, data, hora e motivação.

7.2. É vedado, em qualquer hipótese:

i. o reaproveitamento, em outro serviço ou contrato, de dados biométricos obtidos na CONCESSÃO;
ii. o treinamento de modelos próprios da CONCESSIONÁRIA com imagens captadas na CONCESSÃO, salvo autorização expressa e específica do PODER CONCEDENTE, com finalidade delimitada e registro no RIPD;

MINUTA

iii. a inferência ou o tratamento de dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, saúde ou vida sexual a partir das imagens; e

iv. a aplicação da funcionalidade para monitoramento de manifestações, reuniões, atos religiosos ou atividade sindical.

7.3. O PODER CONCEDENTE publicará relatório semestral com o número de consultas realizadas, o número de correspondências positivas, o número de correspondências afastadas em revisão humana e as providências adotadas.

7.4. Verificada taxa de falso positivo superior a 5% em auditoria, a funcionalidade será suspensa até a comprovação de sua correção.

8. INCIDENTES DE SEGURANÇA

8.1. A CONCESSIONÁRIA comunicará ao PODER CONCEDENTE, ao encarregado e ao VERIFICADOR INDEPENDENTE:

Classificação	Critério	Prazo de comunicação
Crítico	comprometimento de dados pessoais em escala, indisponibilidade de sistema essencial ou acesso não autorizado a imagens	imediato e, no máximo, 2 (duas) horas da ciência
Grave	tentativa bem-sucedida de acesso não autorizado sem exfiltração comprovada; indisponibilidade parcial relevante	24 (vinte e quatro) horas
Moderado	vulnerabilidade explorável identificada; falha de controle sem comprometimento	72 (setenta e duas) horas

8.2. A comunicação conterá: descrição do incidente; dados afetados; número estimado de titulares; medidas de contenção adotadas; riscos identificados; e cronograma de remediação.

8.3. A CONCESSIONÁRIA apresentará relatório de causa-raiz em até 30 dias e implementará o plano de remediação, com verificação pelo VERIFICADOR INDEPENDENTE.

8.4. A comunicação à ANPD e aos titulares compete ao PODER CONCEDENTE, na qualidade de controlador, com o apoio técnico e as informações fornecidas pela CONCESSIONÁRIA nos prazos legais.

MINUTA

8.5. A CONCESSIONÁRIA manterá registro de todos os incidentes, inclusive os não comunicáveis, disponível para auditoria.

9. DIREITOS DOS TITULARES

9.1. As solicitações de titulares serão recebidas pelo encarregado do PODER CONCEDENTE, cabendo à CONCESSIONÁRIA prestar o apoio técnico necessário em até 10 dias do encaminhamento.

9.2. São assegurados os direitos dos arts. 18 e 20 da LGPD, observadas as restrições legais aplicáveis ao tratamento para fins de segurança pública e de apuração de infrações.

9.3. O exercício do direito de revisão de decisão automatizada é assegurado sempre que houver aplicação de analítica com efeito sobre pessoa determinada, na forma do item 7.1.iv.

10. AUDITORIA, RIPD E CONFORMIDADE

10.1. A CONCESSIONÁRIA manterá RIPD atualizado de todos os tratamentos, revisado, no mínimo, anualmente e sempre que houver alteração relevante de escopo ou tecnologia.

10.2. A CONCESSIONÁRIA manterá registro das operações de tratamento, na forma do art. 37 da LGPD, disponível ao PODER CONCEDENTE, ao VERIFICADOR INDEPENDENTE e à ANPD.

10.3. O PODER CONCEDENTE e o VERIFICADOR INDEPENDENTE terão acesso irrestrito aos ambientes, sistemas, configurações, logs e documentação necessários à verificação de conformidade, resguardados os segredos industriais de terceiros, mediante termo de confidencialidade.

10.4. Será realizada auditoria independente de conformidade ao menos a cada 12 meses, custeada pela CONCESSIONÁRIA, com relatório encaminhado ao PODER CONCEDENTE e ao COMITÊ DE GOVERNANÇA.

MINUTA

11. REVERSIBILIDADE E TITULARIDADE

11.1. Os dados, bases, imagens, metadados, documentação técnica, integrações, parametrizações e credenciais gerados na execução da CONCESSÃO são de titularidade do MUNICÍPIO.

11.2. A CONCESSIONÁRIA entregará, ao término da CONCESSÃO ou quando solicitado, a totalidade desses elementos em formatos abertos, estruturados e interoperáveis, com dicionário de dados, modelo lógico e documentação suficiente à continuidade operacional.

11.3. É vedada qualquer retenção após a extinção do CONTRATO, devendo a CONCESSIONÁRIA comprovar, mediante certificação, a eliminação segura de todas as cópias remanescentes em seus ambientes e nos de seus sub-operadores.

11.4. É vedada arquitetura, cláusula com terceiro ou configuração que impeça, dificulte ou onere a migração dos dados, aplicando-se o item 63.3.1 do CONTRATO.

12. APURAÇÃO DO ICGD

12.1. O ICGD é apurado trimestralmente pelo VERIFICADOR INDEPENDENTE, com base nos seguintes componentes:

Componente	Peso indicativo
Conformidade dos controles de segurança da seção 5	30%
Tempestividade e completude da comunicação de incidentes	20%
Regularidade dos registros de acesso e da cadeia de custódia	20%
Atualização do RIPD e do registro de operações	10%
Cumprimento dos prazos de retenção e eliminação	15%
Apoio tempestivo às solicitações de titulares	5%

12.2. O ICGD será fixado em zero no trimestre de apuração, na forma do item 4.9.1 do ANEXO II, na ocorrência de qualquer das seguintes falhas graves:

i. constituição de base biométrica própria pela CONCESSIONÁRIA;

MINUTA

ii. tratamento em desvio de finalidade, inclusive uso econômico ou compartilhamento não autorizado;

iii. transferência internacional de dados sem autorização;

iv. adoção de providência operacional com efeito sobre pessoa determinada sem revisão humana; e

v. retenção de dados além do prazo, ou omissão na eliminação automática.

12.3. As falhas do item 12.2 sujeitam ainda a CONCESSIONÁRIA à multa do item 46.4.xv e, conforme a gravidade, à declaração de caducidade, na forma do item 52.1.xix do CONTRATO.

MINUTA