

FaceEye

ANEXO DE PROTEÇÃO DE DADOS PESSOAIS – DPA

Cliente × FaceEye

Campo	Informação
Versão	1.1
Data	11/09/2026
Status	MODELO CONTRATUAL PARA ADOÇÃO
Integração	Contrato de licenciamento, SaaS, serviços ou instrumento equivalente do FaceEye

Instrumento destinado a disciplinar o tratamento de dados pessoais realizado pelo FaceEye em nome do Cliente, em coerência com a Política Pública v2.2, RIPD v2.1 e ROPA v2.1.

1. Objeto e integração contratual

1.1. Este Anexo de Proteção de Dados Pessoais (“DPA”) integra o contrato celebrado entre o Cliente e o FaceEye para utilização da plataforma e prestação dos serviços relacionados (“Contrato Principal”) e disciplina o tratamento de Dados Pessoais realizado no contexto dos Serviços.

1.2. Em caso de conflito entre este DPA e disposições gerais do Contrato Principal especificamente sobre proteção de Dados Pessoais, prevalecerá este DPA quanto a essa matéria. As demais disposições do Contrato Principal permanecem inalteradas.

1.3. Este DPA deve ser interpretado em conjunto com a Lei nº 13.709/2018 (“LGPD”) e com a regulamentação aplicável da Autoridade Nacional de Proteção de Dados (“ANPD”).

2. Definições

2.1. Aplicam-se as definições da LGPD. Para fins deste DPA, “Cliente” significa a parte contratante dos Serviços FaceEye; “FaceEye” significa a parte prestadora dos Serviços; “Serviços” significa a disponibilização e operação da plataforma FaceEye; e “Dados do Cliente” significa os Dados Pessoais tratados pelo FaceEye em nome do Cliente no contexto dos Serviços.

2.2. Os termos Captura, Recorte Facial, Detecção, Representação Biométrica, Motor de Reconhecimento Facial, Coleção, Person ID, Localidade, Grupo e Perfil de Acesso têm o significado adotado na documentação de privacidade do FaceEye. “Provedor de Infraestrutura” significa o prestador de recursos de computação, hospedagem, processamento, armazenamento ou serviços tecnológicos necessários à operação da plataforma. “Região de Processamento” significa a localização geográfica da infraestrutura em que ocorre armazenamento ou processamento dos dados, podendo situar-se no Brasil ou no exterior.

3. Papéis dos agentes de tratamento

3.1. Regra geral

O Cliente atua como Controlador dos Dados do Cliente e determina as finalidades e o contexto do tratamento. O FaceEye atua como Operador e realiza o tratamento em nome do Cliente, para execução dos Serviços e segundo as instruções documentadas do Cliente, inclusive aquelas decorrentes das configurações realizadas diretamente na plataforma.

3.2. Meios técnicos

As decisões do FaceEye relativas à arquitetura, infraestrutura, Motor de Reconhecimento Facial, Coleção, armazenamento, processamento, disponibilidade, continuidade, suporte e demais recursos tecnológicos constituem, em regra, definição de meios técnicos necessários à prestação dos Serviços e não alteram a condição do Cliente como Controlador.

3.3. Tratamentos próprios do FaceEye

Quando o FaceEye tratar Dados Pessoais para finalidade própria, distinta da finalidade determinada pelo Cliente e não meramente instrumental aos Serviços, atuará como Controlador exclusivamente quanto a esse tratamento, assumindo as obrigações correspondentes. Podem incluir-se nessa hipótese atividades próprias de gestão contratual, faturamento e cumprimento de obrigações legais.

4. Instruções e responsabilidades do Cliente

4.1. O Cliente é responsável pela licitude das finalidades e das instruções de tratamento que determinar ao FaceEye e, em especial, por:

- definir as finalidades, os ambientes, as Localidades e os dispositivos em que utilizará os Serviços;
- identificar e documentar as hipóteses legais aplicáveis, inclusive as hipóteses do art. 11 da LGPD quando houver tratamento de dados biométricos para identificação;
- cumprir os deveres de transparência e fornecer avisos, informações ou comunicações exigíveis aos titulares;
- definir as Pessoas cadastradas, os dados cadastrais, os Grupos, classificações, regras, alertas, destinatários e demais parâmetros de seu ambiente;
- administrar seus usuários e Perfis de Acesso, mantendo sob sua responsabilidade a legitimidade das permissões concedidas;
- configurar os períodos de retenção e solicitar eliminações de acordo com suas finalidades, necessidades e obrigações legais;
- avaliar os resultados produzidos pelo Motor de Reconhecimento Facial e determinar as providências ou decisões tomadas a partir desses resultados;
- definir o conteúdo e a finalidade de exportações e, após disponibilização do arquivo, administrar sua guarda, compartilhamento e utilização;
- avaliar requisitos específicos quando o tratamento envolver crianças ou adolescentes ou puder produzir efeitos relevantes sobre titulares.

4.2. O Cliente não deverá instruir o FaceEye a realizar tratamento manifestamente incompatível com a legislação aplicável. Se o FaceEye identificar, de forma objetiva, que uma instrução específica viola a LGPD ou regulamentação diretamente aplicável ao tratamento executado pelo Operador, poderá comunicar o Cliente e suspender apenas a execução da instrução afetada enquanto as Partes buscam solução compatível, sem que isso transfira ao FaceEye a obrigação de validar previamente os casos de uso do Cliente.

5. Obrigações do FaceEye como Operador

5.1. O FaceEye deverá:

- tratar os Dados do Cliente para execução dos Serviços e de acordo com as instruções documentadas do Cliente;
- limitar o acesso de sua equipe aos Dados do Cliente às situações necessárias à prestação de suporte, manutenção, diagnóstico, continuidade ou demais atividades integrantes dos Serviços;
- adotar medidas técnicas e administrativas compatíveis com as características da plataforma e os riscos dos tratamentos sob sua responsabilidade;
- manter mecanismos de autenticação individual, Perfis de Acesso e segregação lógica entre ambientes de Clientes;
- executar tecnicamente as configurações de retenção e as instruções válidas de eliminação do Cliente, observados os ciclos operacionais e o backup previstos neste DPA;
- cooperar, na medida necessária e tecnicamente possível, com solicitações do Cliente relacionadas a direitos de titulares, incidentes e obrigações regulatórias referentes aos tratamentos em que o Cliente seja Controlador;
- assegurar que pessoas autorizadas a tratar Dados do Cliente estejam sujeitas a deveres de confidencialidade compatíveis com suas funções.

5.2. O FaceEye não assume a obrigação de determinar ou validar a finalidade, a hipótese legal, a proporcionalidade ou a legitimidade do caso de uso definido pelo Cliente, salvo quanto aos tratamentos em que o próprio FaceEye atuar como Controlador.

6. Características do tratamento

Elemento	Descrição contratual
Natureza e operações	Captura local, geração e transmissão de Recorte Facial, processamento facial, geração de Representação Biométrica, organização técnica na Coleção, criação e armazenamento de Detecções, cadastro nominal, consultas, Grupos/classificações, alertas, exportações, retenção, eliminação, suporte e backup.
Finalidade	Execução das finalidades definidas pelo Cliente mediante utilização dos Serviços FaceEye.
Duração	Durante a vigência do Contrato Principal e pelos períodos de retenção configurados pelo Cliente ou necessários ao cumprimento de obrigações aplicáveis.
Titulares	Pessoas detectadas ou cadastradas pelo Cliente e usuários autorizados da plataforma.
Dados	Recorte Facial, Representação Biométrica, Person ID, Detecções, data/hora, Localidade, dispositivo, dados cadastrais inseridos pelo Cliente, Grupos/classificações e dados de usuários.
Dados sensíveis	Dados biométricos quando utilizados para identificação.
Captura original	Permanece no dispositivo do Cliente, não é transmitida integralmente ao ambiente central e está sujeita a expiração automática atualmente limitada a 7 dias.

7. Reconhecimento facial, resultados e decisões

7.1. O Cliente reconhece que o reconhecimento facial é um processamento tecnológico sujeito a características e limitações inerentes à tecnologia, inclusive à possibilidade de resultados incorretos.

7.2. O FaceEye disponibiliza resultados, associações, classificações e alertas conforme as configurações do Cliente. Compete ao Cliente definir os procedimentos e as consequências práticas decorrentes desses resultados, especialmente quando possam produzir efeitos relevantes sobre uma Pessoa.

7.3. A disponibilização de funcionalidades pelo FaceEye não constitui recomendação, autorização ou validação jurídica de determinada utilização pelo Cliente.

8. Retenção e eliminação

8.1. O Cliente poderá configurar os períodos de retenção aplicáveis aos dados mantidos em seu ambiente, observados eventuais limites técnicos máximos estabelecidos para a plataforma.

8.2. Encerrado o período configurado ou recebida instrução válida de eliminação, o FaceEye executará os procedimentos técnicos correspondentes no ambiente ativo, observados os ciclos operacionais necessários.

8.3. A eliminação no ambiente ativo não implica restauração ou alteração retroativa da cópia de backup existente, que será substituída no ciclo subsequente conforme a Cláusula 9.

8.4. O FaceEye não utilizará atividades de suporte como finalidade autônoma para conservar cópias dos Dados do Cliente além das regras aplicáveis aos dados de origem.

9. Backup e continuidade

9.1. O FaceEye realiza 1 (um) backup diário, durante a madrugada, mediante cópia integral do servidor de aplicação, servidor de banco de dados e repositório de imagens.

9.2. O backup destina-se exclusivamente à recuperação integral do ambiente em caso de desastre ou perda total e não constitui mecanismo de arquivamento, versionamento, consulta histórica ou recuperação individual de registros.

9.3. A cada novo ciclo concluído, a cópia anterior é removida, permanecendo somente o backup do ciclo mais recente. Dados eliminados do ambiente ativo poderão permanecer temporariamente nessa cópia até sua substituição no ciclo seguinte.

10. Segurança e acesso

10.1. O FaceEye adotará medidas técnicas e administrativas compatíveis com a natureza dos Dados do Cliente, as características dos Serviços e os riscos dos tratamentos sob sua responsabilidade.

10.2. A plataforma utiliza autenticação individual, Perfis de Acesso e mecanismos de segregação lógica destinados a impedir que usuários de um Cliente acessem cadastros, Detecções, históricos, Localidades, Grupos e demais dados de outro Cliente.

10.3. O Cliente é responsável pela administração de seus usuários, credenciais, dispositivos e permissões, bem como por comunicar prontamente ao FaceEye situações de comprometimento de acesso de que tenha conhecimento.

10.4. Nenhuma disposição deste DPA deve ser interpretada como declaração de existência de controle técnico específico que não esteja efetivamente implantado na plataforma.

11. Suboperadores e fornecedores

11.1. O Cliente autoriza o FaceEye, de forma geral, a contratar Provedores de Infraestrutura e outros fornecedores ou suboperadores necessários à prestação dos Serviços.

11.2. Quando um fornecedor efetivamente tratar Dados do Cliente em nome do FaceEye no contexto dos Serviços, o FaceEye deverá estabelecer obrigações de proteção de dados compatíveis com a natureza da atividade contratada e com as obrigações aplicáveis ao FaceEye como Operador.

11.3. A substituição de tecnologia, Motor de Reconhecimento Facial, provedor de infraestrutura ou outro fornecedor não dependerá de autorização individual do Cliente quando não alterar materialmente a finalidade do tratamento determinada pelo Cliente, sem prejuízo do cumprimento das obrigações legais aplicáveis à cadeia de tratamento e às transferências internacionais.

11.4. O FaceEye permanece responsável por suas próprias obrigações legais e contratuais na contratação e gestão dos suboperadores, sem ampliação de responsabilidade além do que resulte da legislação aplicável e deste DPA.

12. Transferência internacional de dados

12.1. O Cliente declara estar informado de que o FaceEye poderá utilizar Provedores de Infraestrutura e Regiões de Processamento distintas ao longo da prestação dos Serviços. A Região de Processamento poderá estar localizada no Brasil ou no exterior.

12.2. Quando a localização da Região de Processamento, o acesso ou a atuação do Provedor de Infraestrutura caracterizar transferência internacional de Dados Pessoais, o FaceEye, na condição de Operador responsável pela execução técnica do fluxo utilizado nos Serviços, adotará e manterá mecanismo válido de transferência internacional aplicável, conforme a LGPD e a regulamentação da ANPD.

12.3. Quando o mecanismo de transferência internacional adotado for baseado em cláusulas-padrão contratuais aprovadas pela ANPD, o FaceEye observará os requisitos de incorporação e utilização previstos na regulamentação aplicável.

12.4. O Cliente permanece responsável pela legitimidade das finalidades e hipóteses legais do tratamento que determina, considerando as informações fornecidas pelo FaceEye sobre a infraestrutura e, quando aplicável, sobre a ocorrência de transferência internacional.

12.5. Quando houver transferência internacional, o FaceEye fornecerá ao Cliente as informações razoavelmente necessárias para que este cumpra os deveres de transparência que lhe sejam aplicáveis como Controlador.

13. Direitos dos titulares

13.1. As solicitações de titulares referentes aos Dados do Cliente deverão ser tratadas pelo Cliente, na condição de Controlador.

13.2. Quando receber diretamente solicitação que identifique tratamento realizado em nome de determinado Cliente, o FaceEye poderá encaminhá-la ao Cliente ou orientar o titular a utilizar o canal do Controlador, sem decidir o mérito do pedido em nome do Cliente.

13.3. Mediante solicitação razoável do Cliente, o FaceEye prestará cooperação técnica compatível com as funcionalidades da plataforma para localização, acesso, correção, eliminação ou outra providência aplicável aos dados tratados em seu nome.

13.4. Pedidos relacionados a tratamentos em que o FaceEye atuar como Controlador serão tratados diretamente pelo FaceEye.

14. Incidentes de segurança

14.1. O FaceEye comunicará ao Cliente, sem demora injustificada, incidente de segurança de que tenha conhecimento e que envolva Dados do Cliente tratados pelo FaceEye como Operador, fornecendo as informações disponíveis e pertinentes à avaliação do evento.

14.2. Compete ao Cliente, como Controlador, avaliar a necessidade de comunicação à ANPD e aos titulares e realizar as comunicações que lhe sejam exigíveis, cabendo ao FaceEye cooperar com as informações técnicas razoavelmente disponíveis.

14.3. Quando o FaceEye atuar como Controlador do tratamento afetado, caberá ao próprio FaceEye cumprir as obrigações regulatórias correspondentes.

14.4. A comunicação de um incidente pelo FaceEye não constitui, por si só, reconhecimento de falha, culpa, responsabilidade ou violação contratual.

15. Auditoria, evidências e cooperação

15.1. O FaceEye disponibilizará, mediante solicitação razoável do Cliente, informações e documentos existentes que sejam suficientes para demonstrar o cumprimento das obrigações deste DPA que lhe sejam aplicáveis como Operador.

15.2. Caso as informações fornecidas não sejam razoavelmente suficientes e exista fundamento objetivo relacionado ao tratamento dos Dados do Cliente, as Partes poderão acordar procedimento adicional de verificação, em horário comercial, mediante aviso prévio razoável, de forma a não comprometer segurança, confidencialidade, segredos comerciais, dados de outros Clientes ou continuidade dos Serviços.

15.3. Não será exigido do FaceEye conceder acesso irrestrito a sistemas, código-fonte, ambientes de outros Clientes, informações protegidas de terceiros ou permitir testes invasivos que possam afetar a segurança ou disponibilidade da plataforma, salvo obrigação legal específica ou determinação de autoridade competente.

15.4. Cada Parte arcará com seus custos ordinários de cooperação. Atividades extraordinárias solicitadas exclusivamente pelo Cliente poderão ser objeto de prévio acordo sobre escopo, prazo e custos, quando permitido pela legislação.

16. Confidencialidade

16.1. As Partes deverão preservar a confidencialidade dos Dados Pessoais e das informações não públicas a que tiverem acesso em razão deste DPA, observadas as disposições de confidencialidade do Contrato Principal.

16.2. O FaceEye limitará o acesso de seus profissionais aos Dados do Cliente conforme a necessidade de execução das respectivas atividades.

17. Responsabilidade entre as Partes

17.1. Cada Parte responderá pelas obrigações que lhe sejam atribuídas pela legislação aplicável e por este DPA, de acordo com sua atuação efetiva no tratamento.

17.2. O Cliente será responsável pelas consequências decorrentes de finalidades, instruções, configurações, cadastros, classificações, alertas, exportações, decisões ou utilizações da plataforma determinadas por ele em desconformidade com a legislação ou com este DPA.

17.3. O FaceEye será responsável por violações de suas obrigações legais ou contratuais que lhe sejam diretamente imputáveis na condição em que atuar no tratamento.

17.4. Na máxima extensão permitida pela legislação aplicável, eventuais limitações, exclusões e procedimentos de responsabilidade previstos no Contrato Principal também se aplicam às obrigações deste DPA, sem afastar direitos de titulares ou responsabilidades que não possam ser limitadas por contrato.

17.5. Se uma Parte suportar prejuízo, condenação ou despesa em razão de ato ou omissão imputável à outra Parte em violação de suas obrigações legais ou deste DPA, poderá exercer direito de regresso na proporção da responsabilidade atribuível à Parte causadora, observadas as regras do Contrato Principal e a legislação aplicável.

18. Término dos Serviços

18.1. Encerrado o Contrato Principal, o Cliente deverá adotar as providências de exportação ou preservação de dados que deseje realizar antes da indisponibilização de seu ambiente, observadas as funcionalidades e condições comerciais aplicáveis.

18.2. Após o encerramento, o FaceEye eliminará ou tornará inacessíveis os Dados do Cliente mantidos no ambiente ativo de acordo com o processo técnico aplicável, ressalvadas as hipóteses de conservação

exigidas ou autorizadas por lei e a permanência temporária no backup até sua substituição pelo ciclo subsequente.

18.3. Dados que o FaceEye deva conservar como Controlador para finalidade própria legítima e distinta dos Serviços não se submetem à instrução de eliminação do Cliente, permanecendo sujeitos à legislação aplicável.

19. Disposições gerais

19.1. Alterações materiais na forma de tratamento que afetem este DPA poderão ser refletidas por atualização contratual ou documental apropriada.

19.2. A substituição do Motor de Reconhecimento Facial ou de fornecedor tecnológico, isoladamente, não caracteriza alteração da finalidade do tratamento quando não modificar materialmente as categorias de dados, fluxos, compartilhamentos, retenção ou riscos do tratamento.

19.3. Este DPA não confere a qualquer Parte poder para assumir obrigações em nome da outra perante titulares, autoridades ou terceiros, exceto quando expressamente previsto em lei ou mediante autorização específica.

19.4. Permanecem aplicáveis as disposições do Contrato Principal relativas a vigência, foro, solução de controvérsias e demais matérias não reguladas especificamente neste DPA.

ANEXO I – Quadro resumido do tratamento

Tema	Descrição
Controlador	Cliente, como regra geral.
Operador	FaceEye, como regra geral.
Finalidades	Determinadas pelo Cliente conforme seu caso de uso.
Dados principais	Recorte Facial, biometria, Person ID, Detecções, metadados, dados cadastrais, Localidades, Grupos e dados de usuários.
Titulares	Pessoas detectadas/cadastradas e usuários.
Captura original	Permanece no dispositivo do Cliente; expiração automática atualmente limitada a 7 dias.
Ambiente central	Região de Processamento variável, no Brasil ou no exterior; transferência internacional somente quando caracterizada pela arquitetura efetivamente utilizada.
Retenção	Configurada pelo Cliente, sujeita a limites técnicos máximos.
Backup	Diário; cópia integral; somente ciclo mais recente; recuperação de desastre.
Exportações	Excel/PDF; podem conter imagem; uso externo sob governança do Cliente.
Alertas	Critérios e destinatários definidos pelo Cliente; execução técnica pelo FaceEye.
Suboperadores	Autorização geral, quando necessários aos Serviços, sujeitos às obrigações aplicáveis.

ANEXO II – Controle do documento

Campo	Informação
Documento	LGPD 5 – DPA / Anexo de Proteção de Dados Pessoais Cliente × FaceEye
Versão	1.1
Data	11/09/2026
Status	Modelo contratual para adoção
Base documental	LGPD 1 – Política Pública v2.2; LGPD 2 – RIPD v2.1; LGPD 3 – ROPA v2.1; LGPD 4 – Matriz de Consistência v1.1
Base normativa	LGPD; regulamentação da ANPD aplicável, inclusive transferência internacional e incidentes de segurança.