

FaceEye

POLÍTICA DE TRATAMENTO DE DADOS BIOMÉTRICOS E RECONHECIMENTO FACIAL

Versão Pública Definitiva

Campo	Informação
Versão	2.2
Data	10/09/2026
Status	VERSÃO DEFINITIVA
Abrangência	Plataforma FaceEye

Política pública consolidada sobre o tratamento de dados pessoais, imagens e biometria realizado por meio da plataforma FaceEye, harmonizada com o RIPD v2.1 e o ROPA v2.1.

1. Objetivo

Esta Política estabelece os princípios, responsabilidades e regras gerais aplicáveis ao tratamento de dados pessoais, imagens e dados biométricos realizado por meio da plataforma FaceEye, especialmente nas atividades de detecção, reconhecimento facial, cadastro, consulta, alertas, exportação, retenção e suporte.

A Política busca oferecer transparência sobre a arquitetura da solução e sobre a divisão de responsabilidades entre o Cliente que utiliza a plataforma e o FaceEye, sem substituir os avisos, políticas, bases legais e demais providências que devam ser adotados pelo Cliente em razão de sua finalidade e contexto específicos.

2. Abrangência

Esta Política aplica-se à plataforma FaceEye, aos seus recursos de visão computacional e reconhecimento facial e às operações de tratamento realizadas no contexto da prestação dos Serviços.

As condições concretas de cada implantação, incluindo ambientes, Localidades, Pessoas, finalidades, regras, períodos de retenção e decisões decorrentes dos resultados da plataforma, são determinadas pelo Cliente.

3. Definições

Termo	Definição
Cliente	Organização que contrata ou utiliza o FaceEye e que, como regra geral, determina as finalidades e o contexto do tratamento.
Pessoa	Indivíduo detectado pela solução, cadastrado nominalmente ou não.
Pessoa Cadastrada	Pessoa à qual o Cliente associou dados cadastrais e referência facial em seu ambiente.
Captura	Imagem original obtida no dispositivo do Cliente. Permanece localmente e não é transmitida integralmente ao ambiente central.
Recorte Facial	Região da imagem correspondente à face, extraída no dispositivo e transmitida ao FaceEye.
Deteção	Registro resultante do processamento facial, associado aos elementos técnicos e contextuais aplicáveis.
Representação Biométrica	Representação matemática ou geométrica derivada da face e utilizada para comparação e reconhecimento.
Motor de Reconhecimento Facial	Componente tecnológico que extrai, processa, compara e reconhece características faciais. Pode utilizar tecnologia própria, open-source ou de terceiros.
Coleção	Repositório lógico de referências biométricas utilizado pelo Motor de Reconhecimento Facial.

Termo	Definição
Person ID	Identificador técnico interno associado à referência biométrica na Coleção. Não constitui, por si só, cadastro de negócio do Cliente.
Localidade	Estrutura hierárquica definida pelo Cliente para contextualizar dispositivos, Pessoas, Detecções, Grupos e regras.
Grupo	Classificação contextual criada e administrada pelo Cliente.
Perfil de Acesso	Conjunto de permissões atribuído aos usuários do Cliente.
Provedor de Infraestrutura	Prestador de recursos de computação, hospedagem, processamento, armazenamento ou serviços tecnológicos necessários à operação da plataforma FaceEye.
Região de Processamento	Localização geográfica da infraestrutura em que ocorre armazenamento ou processamento dos dados. Poderá situar-se no Brasil ou no exterior e ser alterada ao longo da prestação dos Serviços.

4. Princípios de tratamento

O tratamento realizado por meio do FaceEye deve observar os princípios e requisitos da legislação aplicável de proteção de dados pessoais, incluindo finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização.

A utilização de dados biométricos para identificação envolve dados pessoais sensíveis e exige que o Cliente avalie a legitimidade, necessidade e proporcionalidade do tratamento em seu contexto concreto.

5. Papéis e responsabilidades

5.1 Cliente como Controlador

Como regra geral, o Cliente atua como Controlador dos dados pessoais tratados por meio do FaceEye, por determinar as finalidades e os contextos em que a plataforma será utilizada.

- definir os ambientes, Localidades e dispositivos em que a solução será utilizada;
- definir as Pessoas a serem cadastradas e os dados cadastrais associados;
- definir Grupos, classificações, regras, critérios de alerta e destinatários;
- identificar e documentar as hipóteses legais aplicáveis aos tratamentos sob sua responsabilidade;
- definir e configurar os períodos de retenção de seu ambiente, observados eventuais limites técnicos da plataforma;
- administrar seus usuários e Perfis de Acesso;

- avaliar os resultados do reconhecimento e determinar as providências ou decisões tomadas a partir deles;
- definir o conteúdo, a finalidade, a guarda e o compartilhamento dos arquivos exportados;
- cumprir os deveres de transparência e atender os direitos dos titulares quando atuar como Controlador.

5.2 FaceEye como Operador

O FaceEye atua, como regra geral, como Operador, realizando o tratamento de dados pessoais em nome do Cliente e para execução dos Serviços contratados.

As decisões relacionadas à arquitetura, infraestrutura, Motor de Reconhecimento Facial, Coleção, mecanismos de armazenamento, processamento, segurança, disponibilidade e demais recursos tecnológicos constituem, em regra, definição dos meios técnicos utilizados pelo Operador e não modificam a condição do Cliente como Controlador.

A disponibilização de funcionalidades, configurações ou recursos técnicos não significa que o FaceEye determine a finalidade de sua utilização pelo Cliente nem transfere ao FaceEye a responsabilidade pelas decisões tomadas pelo Cliente a partir dos resultados da plataforma.

O FaceEye adota as medidas técnicas e administrativas que lhe sejam aplicáveis como Operador, executa as regras de retenção e eliminação configuradas pelo Cliente e coopera tecnicamente com o Cliente quando necessário ao cumprimento de suas obrigações.

5.3 Atuação excepcional do FaceEye como Controlador

Excepcionalmente, o FaceEye atuará como Controlador quando realizar tratamento de dados pessoais para finalidade própria, distinta daquela determinada pelo Cliente e não meramente instrumental à prestação dos Serviços. Nessa hipótese, caberá ao FaceEye determinar a finalidade e os elementos essenciais do tratamento e cumprir as obrigações correspondentes.

Podem enquadrar-se nessa situação tratamentos estritamente próprios relacionados à gestão da relação contratual, faturamento e cumprimento de obrigações legais do FaceEye.

6. Como ocorre a captura e o reconhecimento facial

6.1 Captura no dispositivo

A captura ocorre em tablets ou celulares pertencentes ou administrados pelo Cliente e associados a determinada Localidade. A Captura original permanece no dispositivo e não é transmitida integralmente ao ambiente central do FaceEye.

O processamento inicial necessário à identificação da região facial ocorre no dispositivo, que gera o Recorte Facial. Somente esse Recorte Facial é transmitido ao FaceEye.

As Capturas mantidas temporariamente no dispositivo estão sujeitas a mecanismo de expiração automática, atualmente limitado a 7 dias. A administração física e operacional do dispositivo permanece sob responsabilidade do Cliente.

6.2 Processamento pelo Motor de Reconhecimento Facial

O Recorte Facial é processado pelo Motor de Reconhecimento Facial para extração e comparação das características necessárias à individualização ou ao reconhecimento.

O Motor é um componente tecnológico da solução e pode utilizar tecnologia própria do FaceEye, tecnologia open-source ou tecnologia de terceiros. A substituição da tecnologia utilizada não altera, por si só, as finalidades determinadas pelo Cliente.

6.3 Coleção e Person ID

A Coleção é o repositório lógico utilizado pelo Motor para organizar referências biométricas. O Person ID é uma chave técnica interna associada à referência biométrica.

A arquitetura pode reutilizar uma mesma referência biométrica para evitar armazenamento redundante. Essa organização técnica não implica compartilhamento entre Clientes de cadastros nominais, Detecções, históricos, Localidades, Grupos ou demais informações de negócio. Os dados e processos de cada Cliente permanecem logicamente segregados.

7. Dados tratados

Dependendo da configuração e do caso de uso definido pelo Cliente, o FaceEye poderá tratar as seguintes categorias de dados:

Categoria	Exemplos
Imagem e biometria	Captura mantida localmente, Recorte Facial, Representação Biométrica e referências utilizadas pelo Motor.
Identificadores técnicos	Person ID e identificadores necessários ao funcionamento da solução.
Detecções e metadados	Data/hora, Localidade, dispositivo, Recorte Facial e parâmetros técnicos associados.
Dados cadastrais	Dados inseridos pelo Cliente, que podem incluir nome, CPF, telefone, e-mail, data de nascimento, sexo, endereço e outros campos disponibilizados.
Dados contextuais	Localidades, Grupos, classificações, regras e associações configuradas pelo Cliente.
Dados de usuários	Dados necessários à identificação, autenticação e atribuição de Perfil de Acesso.

8. Finalidades e bases legais

O FaceEye pode ser utilizado para diferentes finalidades definidas pelo Cliente. Por esse motivo, não existe uma única hipótese legal aplicável indistintamente a toda a plataforma.

Compete ao Cliente, como Controlador, determinar a finalidade do tratamento, identificar e documentar a hipótese legal aplicável e avaliar a licitude, necessidade, adequação e

proporcionalidade do uso pretendido, inclusive quando houver dados biométricos utilizados para identificação.

O FaceEye, como Operador, trata os dados em nome do Cliente e segundo suas instruções, não lhe cabendo substituir o Cliente na definição da finalidade ou da hipótese legal de seu caso de uso.

Quando o FaceEye realizar excepcionalmente tratamento próprio como Controlador, caberá ao próprio FaceEye identificar e documentar a hipótese legal aplicável àquela operação.

9. Pessoas Cadastradas, Localidades e Grupos

O Cliente decide quais Pessoas serão cadastradas nominalmente, quais dados serão associados ao cadastro e como as Pessoas serão organizadas em Localidades, Grupos ou classificações.

A denominação, composição, critérios de inclusão e utilização de Grupos e classificações são definidos pelo Cliente, que deve avaliar sua legitimidade e as consequências decorrentes de sua utilização.

O FaceEye fornece a estrutura tecnológica para cadastro, associação e classificação, sem determinar a finalidade concreta dessas escolhas.

10. Alertas e notificações

O FaceEye disponibiliza funcionalidade para geração automática de notificações conforme regras definidas pelo Cliente.

O Cliente pode determinar que uma notificação seja gerada quando determinada Pessoa for reconhecida ou quando uma Pessoa não for reconhecida, definindo também a Localidade, o dispositivo, os critérios e os destinatários da regra.

O FaceEye apenas executa tecnicamente os parâmetros configurados pelo Cliente. Não cabe ao FaceEye escolher quem deve ser monitorado, qual situação deve produzir alerta ou em qual Localidade a regra deve ser aplicada.

Os canais utilizados para entrega das notificações poderão variar conforme os recursos disponibilizados e configurados.

11. Consultas, relatórios e exportações

Usuários autorizados podem consultar Detecções e históricos existentes no ambiente de seu Cliente, conforme o respectivo Perfil de Acesso.

O FaceEye permite exportar listas de Detecções em Excel e PDF, utilizando filtros definidos pelo Cliente, como data, Localidade, dispositivo, intervalo de horário e outros critérios disponibilizados pela plataforma.

Conforme a opção selecionada, a exportação poderá conter a imagem associada à Detecção na respectiva linha da planilha ou do relatório PDF.

O Cliente define o conteúdo e a finalidade da exportação. Após a geração e disponibilização do arquivo, sua guarda, compartilhamento, conservação e utilização externa ficam sob governança do Cliente.

12. Retenção e eliminação

O Cliente define e configura os períodos de retenção aplicáveis aos dados pessoais tratados em seu ambiente FaceEye, de acordo com suas finalidades, hipóteses legais e necessidades.

O FaceEye disponibiliza os mecanismos técnicos necessários à execução das regras de retenção e eliminação definidas pelo Cliente, podendo estabelecer limites técnicos máximos de armazenamento aplicáveis à plataforma.

Encerrado o período configurado ou recebida instrução válida de eliminação, o FaceEye executará os procedimentos técnicos correspondentes nos ambientes ativos, observados os ciclos operacionais necessários à efetivação da exclusão.

13. Backup e recuperação de desastre

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

O backup destina-se exclusivamente à recuperação integral do ambiente em caso de desastre ou perda total. Não é utilizado para recuperação individual de registros, consulta histórica ou restauração de dados excluídos durante a operação normal.

A cada novo ciclo de backup concluído, o backup anterior é removido, permanecendo apenas a cópia do ciclo mais recente. Assim, dados eliminados do ambiente ativo poderão permanecer temporariamente na cópia existente até sua substituição no ciclo seguinte.

14. Segurança e controle de acesso

O FaceEye adota medidas técnicas e administrativas compatíveis com as características da plataforma e com os riscos dos tratamentos realizados sob sua responsabilidade, destinadas à proteção contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado.

A plataforma utiliza autenticação individual e Perfis de Acesso. Os dados dos diferentes Clientes são submetidos a mecanismos de segregação lógica destinados a impedir que usuários de um Cliente tenham acesso a dados, Detecções, cadastros, Localidades, Grupos e históricos de outro Cliente.

Profissionais autorizados do FaceEye poderão acessar o ambiente do Cliente quando necessário à prestação de suporte, manutenção, diagnóstico ou continuidade dos Serviços, limitando-se às informações necessárias à atividade.

15. Suporte e manutenção

O acesso realizado pela equipe FaceEye para suporte e manutenção ocorre no contexto da prestação dos Serviços e não constitui, por si só, finalidade autônoma de tratamento.

O FaceEye não utilizará o atendimento de suporte como finalidade autônoma de conservação de cópias dos dados pessoais existentes no ambiente do Cliente. Os dados tratados durante o suporte permanecem sujeitos às regras de retenção aplicáveis aos dados de origem.

16. Infraestrutura, fornecedores e transferência internacional

O FaceEye poderá utilizar um ou mais Provedores de Infraestrutura para hospedagem, armazenamento, processamento e demais recursos tecnológicos necessários à prestação dos Serviços. A identidade do Provedor de Infraestrutura e a Região de Processamento constituem elementos da arquitetura tecnológica da plataforma e poderão ser alterados ao longo do tempo, sem que isso, por si só, modifique as finalidades do tratamento.

A Região de Processamento poderá estar localizada no Brasil ou no exterior. Quando a localização da infraestrutura, o acesso ou a atuação do Provedor de Infraestrutura caracterizar transferência internacional de dados pessoais, o FaceEye observará os requisitos e mecanismos aplicáveis previstos na LGPD e na regulamentação da ANPD.

O Provedor de Infraestrutura poderá atuar como suboperador quando efetivamente realizar tratamento de dados pessoais no contexto dos Serviços. A utilização de infraestrutura tecnológica pelo FaceEye não autoriza o Provedor de Infraestrutura a utilizar os Dados do Cliente para finalidade própria, ressalvadas hipóteses legalmente aplicáveis ou tratamentos próprios e independentes do provedor que não decorram de instrução do FaceEye.

A arquitetura, a identidade do Provedor de Infraestrutura e a Região de Processamento constituem meios técnicos empregados pelo FaceEye e poderão ser alterados sem modificação das finalidades determinadas pelo Cliente, observadas as obrigações legais aplicáveis, inclusive quando a alteração resultar em transferência internacional.

17. Resultados do reconhecimento e decisões do Cliente

Os resultados produzidos pelo Motor de Reconhecimento Facial possuem natureza tecnológica e estão sujeitos às características e limitações inerentes a esse tipo de processamento, inclusive à possibilidade de reconhecimento incorreto.

O FaceEye fornece recursos de detecção, reconhecimento, associação, classificação e geração de informações ou alertas conforme as configurações realizadas pelo Cliente. As decisões e providências adotadas a partir desses resultados são determinadas pelo Cliente, de acordo com suas finalidades, procedimentos e responsabilidades.

Quando a utilização puder produzir efeitos relevantes sobre uma Pessoa, cabe ao Cliente definir os procedimentos de avaliação adequados antes da adoção da medida correspondente.

18. Crianças e adolescentes

Quando a utilização do FaceEye envolver crianças ou adolescentes, cabe ao Cliente, na condição de Controlador, avaliar previamente os requisitos legais aplicáveis ao tratamento, considerando a finalidade, o contexto da utilização e as normas específicas de proteção desses titulares.

A disponibilização das funcionalidades da plataforma não pressupõe autorização ou validação, pelo FaceEye, de determinada utilização envolvendo crianças ou adolescentes.

19. Direitos dos titulares

Quando o tratamento for realizado sob determinação do Cliente, as solicitações relativas aos direitos previstos na legislação devem ser dirigidas ao respectivo Cliente, na condição de Controlador.

O FaceEye cooperará tecnicamente com o Cliente, na condição de Operador, quando sua atuação for necessária ao atendimento de solicitação válida relacionada aos dados tratados por meio da plataforma.

Quando o FaceEye atuar excepcionalmente como Controlador de tratamento próprio, as solicitações referentes a esse tratamento serão atendidas pelo FaceEye nos termos da legislação aplicável.

20. Incidentes de segurança

Na ocorrência de incidente de segurança relacionado a tratamento realizado pelo FaceEye como Operador, o FaceEye comunicará o Cliente e fornecerá as informações disponíveis necessárias para que o Cliente avalie e cumpra as obrigações que lhe sejam aplicáveis como Controlador.

Quando o FaceEye atuar como Controlador do tratamento afetado, caberá ao próprio FaceEye adotar as providências correspondentes previstas na legislação e regulamentação aplicáveis.

21. Revisão da Política

Esta Política poderá ser atualizada quando houver alteração relevante nas finalidades, categorias de dados, fluxo de tratamento, funcionalidades, arquitetura, infraestrutura, compartilhamento, retenção, medidas de segurança, papéis dos agentes ou requisitos legais aplicáveis.

A substituição do Motor de Reconhecimento Facial ou de fornecedor tecnológico, isoladamente, não exige alteração estrutural desta Política quando não modificar materialmente as finalidades, categorias de dados, fluxos, compartilhamentos, retenção ou riscos do tratamento.

22. Documentos relacionados

Documento	Relação
LGPD 2 – RIPD v2.1 – Versão Definitiva	Avaliação consolidada de impacto, arquitetura, riscos e medidas relacionadas ao tratamento realizado pela plataforma.
LGPD 3 – ROPA v2.1 – Versão Definitiva	Registro consolidado das operações de tratamento realizadas por meio da plataforma.

23. Controle do documento

Campo	Informação
Documento	LGPD 1 – Política de Tratamento de Dados Biométricos e Reconhecimento Facial
Versão	2.2

Campo	Informação
Data	10/09/2026
Status	Versão pública definitiva
Abrangência	Plataforma FaceEye
Documentos harmonizados	LGPD 2 – RIPD v2.1 e LGPD 3 – ROPA v2.1