

FaceEye

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS – RIPD

Versão Definitiva

Versão	2.1
Data	10/09/2026
Status	VERSÃO DEFINITIVA
Abrangência	Plataforma FaceEye

Documento consolidado de governança para avaliação dos tratamentos de dados pessoais e biométricos realizados por meio da plataforma FaceEye, seus fluxos, riscos e medidas aplicáveis.

1. Objetivo e natureza do documento

Este Relatório de Impacto à Proteção de Dados Pessoais – RIPD consolida a avaliação da arquitetura e das operações de tratamento viabilizadas pela plataforma FaceEye, com ênfase no uso de reconhecimento facial, dados biométricos, imagens, Detecções e informações associadas.

O documento descreve a solução efetivamente definida para o FaceEye na presente versão. Não apresenta funcionalidades inexistentes como compromissos futuros e não utiliza marcadores de projeto, tais como “previsto”, “recomendado” ou “a definir”.

Como regra geral, cada Cliente atua como Controlador dos tratamentos realizados em seu contexto, enquanto o FaceEye atua como Operador. Este RIPD de plataforma apoia a governança e a compreensão dos riscos do serviço, sem substituir avaliações específicas que sejam de responsabilidade do Cliente em razão de sua implantação, finalidade, contexto, categorias de titulares ou consequências do tratamento.

A definição dos papéis considera a função efetivamente desempenhada em cada tratamento: o Controlador toma as principais decisões e define a finalidade, enquanto o Operador trata dados em nome do Controlador.

2. Visão geral da plataforma

O FaceEye é uma plataforma de visão computacional e reconhecimento facial destinada a suportar diferentes casos de uso definidos pelo Cliente, incluindo segurança, controle de acesso, recorrência, frequência, permanência, análise de Detecções e outras utilizações compatíveis com a finalidade determinada em cada implantação.

A solução é estruturada para operar em escala, com múltiplos Clientes, Localidades e dispositivos, mantendo segregação lógica dos dados pertencentes a cada Cliente.

3. Conceitos essenciais

Termo	Definição
Cliente	Organização que contrata ou utiliza o FaceEye e, como regra geral, determina as finalidades e o contexto do tratamento.
Pessoa	Indivíduo detectado pelo sistema, cadastrado nominalmente ou não.
Pessoa Cadastrada	Pessoa à qual o Cliente associou dados cadastrais e referência facial em seu próprio contexto.
Captura	Imagem original obtida no dispositivo do Cliente. Permanece localmente e não é enviada integralmente ao ambiente central do FaceEye.
Recorte Facial	Região da imagem correspondente à face, extraída no dispositivo e transmitida ao FaceEye para processamento.
Detecção	Registro resultante do processamento, associado aos elementos técnicos e contextuais aplicáveis, como data/hora, Localidade, dispositivo e Person ID.

Termo	Definição
Representação Biométrica	Representação matemática ou geométrica derivada da face e utilizada pelo Motor de Reconhecimento Facial para comparação.
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.
Person ID	Identificador técnico interno associado à referência biométrica na Coleção. Sua função é tecnológica e 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 para suas próprias finalidades.
Perfil de Acesso	Conjunto de permissões atribuído aos usuários do Cliente para acesso às funções e informações da plataforma.
Provedor de Infraestrutura	Prestador de recursos de computação, hospedagem, processamento, armazenamento ou serviços tecnológicos necessários à operação da plataforma.
Região de Processamento	Localização geográfica da infraestrutura em que ocorre armazenamento ou processamento dos dados, no Brasil ou no exterior.

4. Agentes de tratamento e responsabilidades

4.1 Cliente como Controlador

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

- define os ambientes e Localidades em que a solução será utilizada;
- define as Pessoas que serão cadastradas e os dados cadastrais associados;
- define Grupos, classificações, critérios de utilização e regras de alerta;
- define os períodos de retenção aplicáveis ao seu ambiente, observados eventuais limites técnicos da plataforma;
- identifica e documenta as hipóteses legais aplicáveis aos tratamentos sob sua responsabilidade;
- define as providências e decisões adotadas a partir dos resultados produzidos pela plataforma;

- administra seus usuários, Perfis de Acesso, exportações e utilização externa dos arquivos gerados.

4.2 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 utilizados para execução dos Serviços constituem, em regra, definição dos meios técnicos de tratamento pelo Operador e não modificam a condição do Cliente como Controlador.

A disponibilização de funcionalidades, configurações ou recursos técnicos pelo FaceEye 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 dessas funcionalidades ou dos resultados produzidos pela plataforma.

4.3 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, determinará a finalidade e os elementos essenciais daquele tratamento e assumirá as responsabilidades correspondentes previstas na LGPD.

Exemplos podem incluir tratamentos estritamente próprios relacionados à gestão da relação contratual, faturamento e cumprimento de obrigações legais do próprio FaceEye.

5. Categorias de titulares e dados tratados

As categorias de titulares dependem da implantação realizada pelo Cliente e podem incluir Pessoas não cadastradas, Pessoas Cadastradas, funcionários, clientes, visitantes, prestadores de serviços, usuários do sistema e, conforme o ambiente, crianças e adolescentes.

Categoria de dado	Exemplos / conteúdo
Imagem e biometria	Captura local, Recorte Facial, Representação Biométrica e referência biométrica utilizada pelo Motor.
Identificadores técnicos	Person ID e demais identificadores necessários ao funcionamento da plataforma.
Metadados de Detecção	Data/hora, dispositivo, Localidade, parâmetros técnicos e demais elementos associados à Detecção.
Dados cadastrais	Campos preenchidos pelo Cliente, que podem incluir nome, CPF, telefone, e-mail, data de nascimento, sexo, endereço e outros campos disponibilizados.
Dados contextuais	Associações a Localidades, Grupos, classificações, regras e filtros definidos pelo Cliente.
Dados de usuários	Identificação dos usuários do sistema e permissões correspondentes ao Perfil de Acesso.

6. Fluxo operacional do tratamento

6.1 Captura local e geração do Recorte Facial

A captura de imagem ocorre em tablets ou celulares pertencentes ou administrados pelo Cliente e associados a determinada Localidade. O processamento inicial necessário à identificação da região facial é realizado no próprio dispositivo.

A Captura original permanece no dispositivo. Somente o Recorte Facial necessário ao processamento é transmitido ao ambiente central do FaceEye.

As Capturas mantidas temporariamente no dispositivo estão sujeitas a mecanismo de expiração automática, atualmente limitado a 7 dias. O dispositivo e sua administração permanecem sob responsabilidade do Cliente.

6.2 Processamento facial

O Recorte Facial é processado pelo Motor de Reconhecimento Facial para extração e comparação das características necessárias à individualização ou ao reconhecimento. A tecnologia específica do Motor poderá ser própria do FaceEye, open-source ou fornecida por terceiro, sem alteração da estrutura jurídica do tratamento quando permanecerem inalteradas as finalidades, os dados, os fluxos e os riscos relevantes.

6.3 Coleção e Person ID

A Coleção funciona como repositório lógico das referências biométricas utilizadas pelo Motor. 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 dados de negócio. Os dados e processos de cada Cliente permanecem logicamente segregados.

A organização interna da Coleção, os identificadores técnicos e os mecanismos de deduplicação constituem meios técnicos utilizados pelo FaceEye como Operador.

6.4 Geração e armazenamento da Detecção

Após o processamento, o FaceEye registra a Detecção e os elementos necessários à sua utilização no ambiente do Cliente, incluindo, conforme aplicável, Recorte Facial, Person ID, Representação Biométrica ou elementos geométricos associados, data/hora, dispositivo, Localidade e parâmetros técnicos do reconhecimento.

Quando o Cliente realiza cadastro nominal, os dados cadastrais são associados ao contexto daquele Cliente e permanecem segregados dos ambientes dos demais Clientes.

7. Finalidades e hipóteses legais

A plataforma não possui uma única hipótese legal aplicável indistintamente a todas as implantações. A hipótese legal depende da finalidade, do contexto, das categorias de titulares e da utilização concreta determinada pelo Cliente.

Compete ao Cliente, na condição de Controlador, determinar as finalidades do tratamento realizado por meio do FaceEye, identificar e documentar as hipóteses legais aplicáveis e avaliar a licitude, necessidade, adequação e proporcionalidade do tratamento pretendido, inclusive quando envolver dados pessoais sensíveis e biométricos.

O FaceEye, na condição de Operador, realiza o tratamento em nome do Cliente e segundo suas instruções, não lhe cabendo substituir o Cliente na definição da finalidade ou da hipótese legal aplicável ao caso de uso.

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

8. Alertas e notificações automáticas

A plataforma permite a geração automática de notificações a partir de regras configuradas pelo Cliente.

O Cliente define se a notificação será gerada quando determinada Pessoa for reconhecida ou quando uma Pessoa não for reconhecida, bem como as Localidades, dispositivos, critérios e destinatários aos quais a regra será aplicada.

O FaceEye, como Operador, limita-se a executar tecnicamente os parâmetros definidos pelo Cliente, processando as Detecções e gerando as notificações correspondentes. O FaceEye não escolhe quem deve ser monitorado, qual evento deve produzir alerta ou em qual Localidade a regra deve ser aplicada.

Os canais concretamente utilizados para entrega das notificações poderão variar conforme a configuração e a arquitetura disponibilizada, sem alteração do princípio de que o Cliente define a regra e o FaceEye executa tecnicamente a automação.

9. Consulta, relatórios e exportações

Usuários autorizados do Cliente podem consultar Detecções, históricos e informações disponíveis em seu próprio ambiente, de acordo com seus Perfis de Acesso.

O FaceEye permite a exportação, em formatos Excel e PDF, de listas de Detecções selecionadas segundo filtros definidos pelo Cliente, tais como data, Localidade, dispositivo, intervalo de horário e outros critérios disponibilizados pela plataforma.

Conforme a opção escolhida pelo usuário, a exportação poderá incluir a imagem associada à Detecção na respectiva linha da planilha ou do relatório PDF.

O Cliente determina os filtros, 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.

10. Retenção e eliminação

O Cliente, na condição de Controlador, define e configura os períodos de retenção aplicáveis aos dados pessoais tratados em seu ambiente FaceEye, de acordo com as finalidades, hipóteses legais e necessidades do tratamento sob sua responsabilidade.

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

Encerrado o período de retenção 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.

A gestão interna de chaves, referências biométricas e mecanismos de deduplicação da Coleção constitui detalhe técnico da implementação, devendo ser operada de modo que a exclusão determinada em um ambiente não exponha nem altere indevidamente dados pertencentes a outro Cliente.

11. Backup e recuperação de desastre

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

O backup destina-se exclusivamente à recuperação integral do ambiente em situação de desastre ou perda total. Não é utilizado como mecanismo de recuperação individual de dados, restauração de registros excluídos ou consulta a informações históricas.

A cada novo ciclo de backup concluído, o backup anterior é removido, permanecendo apenas a cópia correspondente ao ciclo mais recente.

Em razão dessa arquitetura, dados eliminados do ambiente ativo poderão permanecer temporariamente na cópia de segurança existente até a execução do ciclo seguinte de backup, quando a cópia anterior será substituída.

O backup não constitui mecanismo de arquivamento ou versionamento e não se destina à recuperação de registros individualmente excluídos, alterados ou sobrescritos durante a utilização ordinária da plataforma.

12. Segurança e controle de acesso

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

A plataforma utiliza mecanismos de autenticação individual e controle de permissões de acordo com os Perfis de Acesso atribuídos aos usuários.

Os dados pertencentes aos diferentes Clientes são submetidos a mecanismos de segregação lógica destinados a impedir que usuários de um Cliente tenham acesso aos dados, Detecções, cadastros, Localidades, Grupos, históricos e demais informações pertencentes a outro Cliente.

Profissionais autorizados do FaceEye poderão acessar os ambientes dos Clientes quando necessário à prestação de suporte, manutenção, diagnóstico ou continuidade dos Serviços, observadas as permissões e os controles de acesso aplicáveis.

As Capturas mantidas temporariamente nos dispositivos utilizados pelo Cliente estão sujeitas ao mecanismo de expiração automática definido pela solução, atualmente limitado a 7 dias.

13. Suporte e manutenção

Profissionais autorizados do FaceEye poderão acessar dados existentes no ambiente do Cliente quando necessário à prestação de suporte, manutenção, diagnóstico ou continuidade dos Serviços. O acesso será realizado no contexto da prestação dos Serviços e limitado às informações necessárias à atividade executada.

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.

14. Infraestrutura 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 meios técnicos da arquitetura e poderão ser alterados ao longo do tempo.

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

O Provedor de Infraestrutura poderá atuar como suboperador quando efetivamente realizar tratamento de dados pessoais no contexto dos Serviços. Sua contratação e a escolha da Região de Processamento integram os meios técnicos utilizados pelo FaceEye como Operador.

A localização, arquitetura e os fornecedores da infraestrutura constituem meios técnicos empregados pelo FaceEye na prestação dos Serviços e poderão ser alterados sem modificação das finalidades de tratamento determinadas pelo Cliente, desde que sejam observados os requisitos legais aplicáveis.

O Cliente, na condição de Controlador, é responsável pela decisão de utilizar o FaceEye para as finalidades por ele determinadas, considerando as características de infraestrutura informadas pelo FaceEye. Quando houver transferência internacional, a execução técnica do fluxo integra a prestação dos Serviços pelo FaceEye, sem alterar a responsabilidade do Cliente pelas finalidades e hipóteses legais do tratamento.

15. Situações de maior impacto

15.1 Falsos positivos e limitações do reconhecimento

Os resultados produzidos pelo Motor de Reconhecimento Facial possuem natureza tecnológica e estão sujeitos às características e limitações inerentes a esse tipo de processamento. Compete ao Cliente avaliar a utilização desses resultados e definir os procedimentos aplicáveis antes da adoção de medidas que possam produzir efeitos relevantes sobre uma Pessoa.

15.2 Decisões e consequências

O FaceEye fornece recursos tecnológicos 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 próprias finalidades, procedimentos e responsabilidades.

15.3 Grupos, classificações e regras

Compete ao Cliente definir a criação, denominação, composição, critérios de inclusão e utilização de Grupos, classificações e regras configuradas em seu ambiente, bem como avaliar sua legitimidade e as consequências decorrentes de sua utilização.

15.4 Crianças e adolescentes

Quando a utilização do FaceEye envolver crianças ou adolescentes, caberá 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. O risco deve ser avaliado de acordo com o contexto concreto, não sendo classificado automaticamente como crítico apenas em razão da idade do titular.

16. Avaliação consolidada de riscos

A avaliação considera a natureza biométrica do tratamento, a escala potencial da plataforma, o contexto de utilização definido pelo Cliente, as consequências possíveis para os titulares e os controles efetivamente existentes na arquitetura descrita neste documento.

Risco	Nível	Tratamento / mitigação
Reconhecimento facial incorreto ou falso positivo	Alto	O resultado do Motor é suporte tecnológico. O Cliente define o uso e deve avaliar o resultado antes de medidas com efeitos relevantes sobre a Pessoa.
Acesso não autorizado a dados biométricos ou imagens	Alto	Autenticação individual, Perfis de Acesso, segregação lógica entre Clientes e acesso restrito da equipe FaceEye quando necessário à prestação dos Serviços.

Risco	Nível	Tratamento / mitigação
Retenção excessiva de dados	Alto	O Cliente define e configura os períodos de retenção conforme sua finalidade e necessidade. O FaceEye executa tecnicamente as regras configuradas e pode impor limites técnicos máximos.
Uso incompatível de Grupos, classificações ou alertas	Alto	O Cliente define critérios, Pessoas, Localidades, dispositivos, Grupos e gatilhos. O FaceEye apenas disponibiliza e executa os mecanismos tecnológicos.
Uso envolvendo crianças e adolescentes sem avaliação adequada	Alto	O Cliente avalia previamente os requisitos legais e o contexto específico. A plataforma não presume nem valida a legitimidade de cada implantação.
Transferência internacional de dados	Médio/Alto	Região de Processamento variável, no Brasil ou no exterior. Quando a arquitetura efetivamente utilizada caracterizar transferência internacional, aplicam-se os requisitos da LGPD e da regulamentação da ANPD.
Persistência temporária de Capturas no dispositivo	Médio	A Captura original permanece no dispositivo do Cliente e está sujeita a expiração automática, atualmente limitada a 7 dias; somente o Recorte Facial é transmitido ao ambiente central.
Perda total do ambiente	Alto	Backup integral diário do ambiente para recuperação de desastre. Apenas o backup mais recente é mantido; o anterior é removido após conclusão do novo ciclo.
Exportação e uso externo de Detecções	Alto	A exportação é iniciada por usuário autorizado e segue filtros definidos pelo Cliente. Após a geração do arquivo, sua guarda, compartilhamento e utilização ficam sob governança do Cliente.

17. Risco residual e conclusão

O tratamento realizado por meio do FaceEye envolve dados pessoais sensíveis quando a biometria é utilizada para identificação, além de imagens, Detecções e informações contextuais. Esses elementos justificam a manutenção de avaliação formal de impacto e revisão periódica da arquitetura e dos riscos.

A distribuição de responsabilidades adotada neste RIPD parte do princípio de que o Cliente determina o “por quê” e o “para quê” do tratamento e responde pela legitimidade de sua utilização concreta, enquanto o FaceEye fornece e opera os meios tecnológicos necessários à execução do tratamento, segundo as instruções do Cliente, adotando as medidas técnicas e administrativas que lhe sejam aplicáveis como Operador.

Consideradas as características e medidas descritas nesta versão, os riscos identificados são administráveis dentro do modelo de governança proposto, sem prejuízo da necessidade de avaliação específica pelo Cliente quando sua implantação envolver contexto, finalidade ou consequência que eleve materialmente o impacto sobre os titulares.

Este RIPD deverá ser revisado quando houver alteração relevante nas finalidades, categorias de dados, fluxo de tratamento, arquitetura, localização internacional, forma de compartilhamento, retenção, medidas de segurança ou perfil de risco da plataforma.

18. Referências normativas

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD.
- Autoridade Nacional de Proteção de Dados – Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.
- Normas e orientações da ANPD aplicáveis à transferência internacional, segurança, incidentes e demais matérias relacionadas ao tratamento de dados pessoais.

19. Controle do documento

Campo	Informação
Documento	LGPD 2 – Relatório de Impacto à Proteção de Dados Pessoais – RIPD
Versão	2.1
Data	10/09/2026
Status	Versão definitiva
Abrangência	Plataforma FaceEye
Critério de revisão	Mudança relevante de finalidade, dados, fluxo, arquitetura, infraestrutura, compartilhamento, retenção, segurança ou risco.