

• Security and LGPD

Technical sheet for the security team and the data protection officer of whoever contracts. Everything here is published on the site, with the label of each item's state.

Keys and encryption

Per-record envelope available

Every sensitive record has its own data key, wrapped by the master key in the key module. Decrypting one record opens no other; privileged decryption only happens in a separate service.

Receipt key available

ECDSA P-256 in the key module; the private key never leaves. Only the receipt-issuing service signs; the public key is published as JWKS.

Isolation and access

Row-level isolation available

Real row-level security in Postgres, with an application role that cannot bypass it. A query without a client returns nothing.

Levels within the client available

Analyst, supervisor and administrator, with floor-based authorization on every route and tests proving none was left without a floor.

Operations

Transport, edge and release available

Automatic TLS, strict transport with preload, API responses uncached by default; every release applies the migration with a backup first.

Decryption trail available

Every privileged decryption enters an append-only trail with a hash chain: gaps, reordering and forks show.

Certified component available

Live presence comes from an AWS certified component, declared in the receipt with its version, with the opt-out from AI training use applied.

Keys, sessions and MFA available

API keys per client and per scope. Dashboard with app-based MFA, recovery codes and attempt limits.

Hummand's console leaves a trace available

Every view of client data through the console is recorded and attributed to a person. Opening an act's encrypted content requires a reason, and the client sees in the dashboard who opened it.

Declared limits target architecture

Client mTLS in layers, still off for the binding to the contract; mTLS between internal services comes later. Rate limits per key, per client and per IP.

Personal data

Consent per step available

General before anything, biometric before any capture; versioned texts, with instant, hash and version recorded in the receipt. General consent never unlocks biometrics.

References as hashes available

The person's reference enters as an HMAC with a per-client secret; the context, as a hash. This is pseudonymization (art. 13, §4), not anonymization.

Retention by term available

Encrypted verdict and CPF: 90 days. Consent evidence and event trail: five years. A sweep every six hours.

Where the data lives

Today's installation

Server and database in the European Union, encrypted backups also in the European Union; live presence, match and key module on AWS, in the United States, with no frames kept. International transfer in the record of processing, with contractual safeguards.

Records and requests

Access records available

By legal obligation (Marco Civil, art. 15), 190 days: date, time, IP and protocol, in a record separate from the database, backups and receipts.

No image, no template available

Live presence and match return the result, and the image and template are discarded. It is a product invariant, not a setting.

Erasure by key destruction available

By act or by the client's reference, synchronous, with a record of who erased and when. Erasure has its own scope, which no integration gets by default.

Roles

The client is the controller; Hummand, the processor. Record of processing and impact assessment filled in by the data protection officer on 2026-09-21, reviewed with every change in data flow.

National residency by agreement

By contract, the operation can be entirely national: server, database, backups, keys and live presence itself, which also runs in a Brazilian region.

Legal orders

Personal data only leaves on a written order from a competent authority, in the narrowest scope, with legal review before and a record after; the client is notified unless the law forbids it.