

Where your data lives, and who can touch it.

An EU-only data path, an append-only provenance ledger, and controls enforced in the database — not in a policy document.

THE DATA PATH — EVERY STEP INSIDE THE EU

01

Capture
Episodes are captured in the EU.

02

Processing
Annotation and QA run on EU infrastructure.

03

Storage
OVHcloud Paris (eu-west-par).

04

Delivery
Streamed to the customer; every access logged.

No US entity holds, processes, or can be compelled to disclose this data at any step.

WHAT THE LAW SAYS — WHAT THE STACK MAKES IMPOSSIBLE

GDPR ART. 48
Foreign judgments need an EU legal basis
The law
A third-country order to disclose personal data is recognised only if based on an international agreement. Without an EU legal basis, the order has no effect here.
Our stack
Our storage operator is French-owned. There is no US parent anywhere in the chain of control for a foreign order to arrive through.

SCHREMS II — CJEU C-311/18
US surveillance law failed EU adequacy
The law
The CJEU invalidated Privacy Shield, holding US surveillance law incompatible with EU adequacy requirements for personal data transfers.
Our stack
No US entity holds keys or credentials to this data. No US-side arrangement in the data path whose validity we depend on.

US CLOUD ACT §103(A)
US providers can be compelled anywhere
The law
US providers can be compelled to disclose data in their possession, custody, or control — regardless of where in the world it is stored.
Our stack
No US provider possesses or controls the data at any step. Payload access is gated by EU-issued stream tokens; every access is logged.

CONTROLS — ENFORCED IN THE DATABASE, NOT THE APPLICATION

Streamed, never downloaded
Payloads are delivered through 120-second scoped stream tokens. Every view is logged. Bulk export of sensitive payloads is not a feature that exists.

Row-level security
Customers see only what they own — enforced by row-level security policies in the database, not by application code that could be bypassed.

WHAT JURISDICTION ACTUALLY MEANS

	EU-SOVEREIGN SUPPLY CHAIN (AISCÉAL)	US-CLOUD SUPPLY CHAIN
Governing law	EU law and GDPR, end to end.	Subject to US CLOUD Act reach wherever a US entity controls the data.
Storage ownership	French-owned operator (OVHcloud); no US parent in the chain of control.	US-headquartered operators, regardless of bucket region.
Disclosure	Requires EU legal process.	US authorities can compel disclosure from the US entity, including for data stored in the EU.
Audit mechanism	Cryptographic ledger — customers recompute the hash chain themselves.	Contractual assurance and vendor attestations.

PROVENANCE — AUDITABLE BY CONSTRUCTION

Every annotation and QA event writes to an append-only provenance ledger. Delivered bundles include the ledger extract for every episode they contain, sealed by chain-head hashes in the frozen manifest — verifying our supply chain requires no trust in our word, only arithmetic. Since 2 August 2026, EU AI Act Article 10 requires high-risk AI providers to document the origin of their training data: every Aiscéal bundle ships that record by construction.