

DOC-PP-2026 · CONFIDENTIAL
Legal & Compliance

LEGAL & COMPLIANCE

PRIVACY POLICY.

Governs the collection, processing, storage, and rights framework for all personal data handled within the RiseUp platform.
Compliance with Moroccan Law 09-08 and EU GDPR.

COMPLIANCE	Moroccan Law 09-08 · EU GDPR
LAST UPDATED	March 2026
STATUS	Active Policy · v1.0
CLASSIFICATION	Public-Facing · Customer Document
SCOPE	All RiseUp Data Processing Activities

1

Data Controller & Roles

Rise Up AI ("Company") acts as the **Data Processor**. The Football Club or Academy ("Customer") acts as the **Data Controller**. The Customer is responsible for obtaining all necessary consents from Players and Guardians before uploading footage to the Platform.

GDPR BASIS

Processing is conducted under GDPR Art. 6(1)(b) — performance of a contract — and Art. 6(1)(f) — legitimate interests of the Customer in player performance analysis.

2

The "Refinery" Protocol (Data Minimization)

To protect player privacy, RiseUp operates a strict **Extract & Purge** policy. Raw footage is never retained beyond operational necessity.

DATA TYPE	RETENTION	ACTION
Raw Match Video (4K/HD MP4)	30 Days	Permanent Deletion
Processed Frame Cache	7 Days	Automated Purge
Positional Tracking Data (JSON/CSV)	5 Years	Anonymization (Remove PII)
Performance Metadata (pseudonymized)	Long-term	Retained for scouting analytics
Tactical Reports (PDF/JSON)	10 Years	Archive (Audit/Legal)

3

The Smart-Lock & Identity Visibility

3.1

Players Under 18

Identity is locked by default. Only verified professional scouts and club managers may submit a request to "Unlock" a minor's identity. All unlock events are logged and auditable. Positional data for under-18 players is pseudonymized at the point of ingestion.

3.2

Players 18+

Operated under a **"Play to be Seen"** policy. Performance data and identity are visible to the RiseUp Professional Network to facilitate career opportunities. Players retain the right to request data access or erasure at any time.

4

AI Processing & Sub-Processors

RiseUp utilizes AI models including Anthropic, Groq, and Qwen to generate tactical insights. **No personally identifiable information (PII) is shared with these models.** Only raw numerical performance data (coordinates, velocities, event flags) is processed to generate narrative reports.

DATA FLOW

Raw footage → CV pipeline → anonymized numerical metrics → AI narrative generation. PII is stripped before any AI model call.

5

Data Residency (Sovereignty)

European Operations: All PostgreSQL and vector data for European clubs must reside in AWS/GCP Paris (eu-west-3) or Frankfurt (eu-central-1) regions.

On-Premises Privacy: Tactical reports generated by on-device LLM models are processed in-memory and stored within the client's siloed instance. No raw tactical insights are transmitted back to RiseUp central servers.

6

Right to Erasure — The "Forgotten Player" Protocol

In the event of a valid Data Subject Access Request (DSAR) from a player or agent, RiseUp will execute the following sequence:

- 01 Delete the identifiable player profile from the scouting UI.
- 02 Anonymize the historical tracking rows in PostgreSQL.
- 03 Retain the non-identifiable vector embeddings for statistical model integrity — these do not constitute personal data under GDPR Recital 26.

7

Contact & Policy Review

This policy is reviewed annually or upon major architectural changes. For data-related inquiries, contact: info@riseupai.co

RiseUp AI · Casablanca Finance City (CFC), Morocco