

DATA PROCESSING ADDENDUM

Standard Controller-to-Processor Clauses (GDPR Art. 28, UK GDPR, and CCPA)

BETWEEN THE PARTIES:

1. The football club, sports academy, federation, or collegiate organization executing this Addendum ("Customer" or "Data Controller"); and
2. Trequa Corporation, operating Touchline360 and its hosted services including Debrief and Kickoff Pulse ("Touchline360" or "Data Processor").

WHEREAS, Customer has entered into an agreement or subscription with Touchline360 for sports performance analytics, match debriefing, and tactical preparation software; and

WHEREAS, providing the services requires the processing of personal data on behalf of Customer, the parties agree to the binding terms set forth herein.

1. Scope, Status and Priority

1.1 Customer enters into this DPA as the Data Controller under Regulation (EU) 2016/679 ("GDPR"), the UK Data Protection Act 2018 ("UK GDPR"), and the California Consumer Privacy Act ("CCPA"). Touchline360 processes personal data exclusively as a Data Processor on documented instructions from Customer.

1.2 In the event of any conflict between the main Subscription Agreement and this DPA, the terms of this DPA shall govern regarding personal data protection and privacy.

2. Nature, Purpose and Categories of Processing

2.1 Scope of Data: Ingestion of match recordings, training footage, squad rosters, player positional coordinates, physical load telemetry, coach annotations, tactical findings, lineups, and film session presentations.

2.2 Categories of Data Subjects: Registered coaching staff, tactical analysts, match officials, and players (including youth academy players under eighteen years of age) appearing in recordings.

2.3 Non-Biometric Optical Processing: The parties acknowledge that Touchline360 utilizes optical computer vision to determine pitch coordinates, jersey numbers, and bounding-box coordinates. Touchline360 does NOT perform facial biometric profiling, emotional affect detection, or facial recognition matching against third-party databases.

3. Processor Obligations

Touchline360 covenants and warrants that it will:

- (a) Process personal data solely on documented, lawful instructions from Customer, including regarding data transfers;
- (b) Ensure that all personnel authorized to access customer data have committed themselves to statutory or contractual confidentiality;
- (c) Never sell, lease, or monetize customer data or match footage;
- (d) Never train foundation machine learning models for third parties on Customer match video or coaching plans without affirmative, opt-in governance approval under Customer's tenancy settings.

4. Technical and Organizational Security Measures (TOMs)

Pursuant to Article 32 GDPR, Touchline360 implements rigorous security controls appropriate to the risk:

- Tenant Isolation: Multi-tenant architecture logically partitioned at the database query layer. Every API request enforces the organization boundary before reading or writing data.
- Cryptographic Controls: TLS 1.3 encryption for all data in transit; AES-256 server-side encryption for all stored video files, database records, and backups at rest.
- Access Governance: Role-Based Access Control (RBAC) with mandatory multi-factor authentication for technical administrators. Access logs are maintained and retained for security audits.
- Resilience & Redundancy: High-availability cloud infrastructure with continuous health monitoring and daily encrypted database backups.

5. Youth Athlete Safeguarding Commitment

5.1 Academy Video Protection: Touchline360 is engineered to support club compliance with national youth safeguarding standards (including The FA Safeguarding Children Policy and US Soccer Safe Soccer).

5.2 Model Exclusion: Customer footage featuring youth academy players is excluded from commercial AI training by default (`model_improvement_consent = none`). No youth profiles are sold or aggregated across clubs for commercial scout marketplaces.

5.3 Parental Erasure Rights: Customer or verified legal guardians may request expedited redaction or deletion of youth player recordings through dpo@touchline360.com or safeguarding@touchline360.com.

6. Sub-processors Management

6.1 General Authorization: Customer grants general authorization for Touchline360 to engage sub-processors listed in Schedule 2 (Sub-processors Directory).

6.2 Notice of Changes: Touchline360 will notify Customer at least thirty (30) calendar days prior to onboarding any new or replacement sub-processor.

6.3 Right to Object: Customer may object to a new sub-processor on reasonable data protection grounds within the 30-day notice window. If an objection cannot be mutually resolved, Customer may terminate the affected service without penalty.

7. Personal Data Breach Notification

In the event of a confirmed Personal Data Breach impacting Customer data, Touchline360 shall notify Customer without undue delay and, in any event, within 48 hours of becoming aware of the incident. Touchline360 will provide reasonable remediation details, impact assessments, and technical mitigation logs.

8. International Transfers & Standard Contractual Clauses

To the extent Customer personal data is transferred outside the European Economic Area (EEA), United Kingdom, or Switzerland, the parties hereby incorporate the European Commission Standard Contractual Clauses (Module 2: Controller-to-Processor) and the UK International Data Transfer Addendum by reference.

9. Data Return, Export and Cryptographic Purge

Upon subscription expiry or termination, Customer shall have a thirty (30) day window to export tactical findings, match data, and videos. Upon expiration of this export window, Touchline360 shall securely delete and overwrite all Customer personal data and video blobs within thirty (30) days, unless applicable statutory law requires further retention.

SCHEDULE 2: AUTHORIZED INFRASTRUCTURE SUB-PROCESSORS

Sub-processor	Role / Service	Location / Region	Safeguards
Railway Corporation	Cloud container compute, API hosting	US / EU regions	SOC 2 Type II, DPA
Cloud Object Storage	Encrypted match footage & clips	US / EU regions	AES-256, ISO 27001
PostgreSQL Managed	Relational database tenancy & notes	US / EU regions	VPC, TLS, Encrypted
Transactional Email Relay	Authentication links & system alerts	US / EU regions	TLS 1.3, DPA

EXECUTION AND COUNTERSIGNATURE

IN WITNESS WHEREOF, the authorized representatives of the parties have executed this Addendum:

ON BEHALF OF CUSTOMER (CONTROLLER):

Club / Organization: _____

Signatory Name: _____

Title / Position: _____

Signature: _____

Date: _____

ON BEHALF OF TREQUA / TOUCHLINE360:

Entity: Trequa Corporation

Signatory Name: Data Protection Officer

Title: Compliance & Security Director

Signature: [Signed / Touchline360 DPO]

Contact: dpo@touchline360.com