Data Processing Addendum

Last updated: 12 February 2026

This Data Processing Addendum (“DPA”) applies where Cutout Pty Ltd (“Cutout”, “we”, “us”, or “our”) processes personal data on behalf of a school, university, club, academy, or other organisation (“institution”) that uses the Cutout platform.

This DPA forms part of the agreement between Cutout and the institution.

1. Roles of the parties

For the purposes of applicable data protection laws (including the Australian Privacy Principles and, where applicable, the GDPR):

- The **institution** acts as the **data controller** for personal data it uploads, creates, or manages within the Cutout platform relating to its students, athletes, staff, or members.
- **Cutout** acts as a **data processor** that processes personal data solely on behalf of the institution and only to provide the services.

Cutout will not use institutional personal data for any purpose other than:

- Providing and maintaining the services
- Supporting authorised institutional workflows
- Ensuring platform security and reliability

2. Scope of processing

Cutout may process the following categories of personal data on behalf of the institution:

Categories of data

- Name
- Email address
- Role (student, athlete, coach, staff)
- Group/team/class membership
- Performance metrics
- Workout videos
- Session participation records
- Device and usage data

Categories of data subjects

- Students
- Athletes
- Coaches
- Teachers
- Staff
- Institutional users

Purpose of processing

- Delivering performance tracking and analysis
- Enabling institutional coaching/teaching workflows
- Providing session management tools
- Maintaining platform functionality and security

Processing will occur only as instructed by the institution through normal use of the platform.

3. Processor obligations

Cutout will:

- Process personal data only on documented instructions from the institution
- Ensure staff handling data are subject to confidentiality obligations
- Implement appropriate technical and organisational security measures
- Not sell or use institutional data for advertising
- Not share data with third parties except approved sub-processors
- Assist the institution with data subject requests where required

4. Security measures

Cutout implements industry-standard safeguards including:

- Encrypted storage via AWS S3
- Secure authentication via AWS Cognito
- Access controls and role-based permissions
- Secure transmission protocols
- Regular system monitoring and logging

Access to institutional data is limited to authorised personnel only.

5. Sub-processors

Cutout uses trusted infrastructure providers to deliver the services.

Current sub-processors include:

- Amazon Web Services (hosting, storage, authentication)
- RevenueCat (billing and subscription management, where applicable)

All sub-processors are required to maintain appropriate data protection and security standards.

Cutout remains responsible for sub-processor compliance.

6. Data subject rights

To the extent required by law, Cutout will assist institutions in responding to requests to:

- Access personal data
- Correct data
- Delete data
- Restrict processing
- Export data

Where a request is received directly by Cutout from a user whose account is managed by an institution, Cutout may refer the request to the institution where appropriate.

7. Data breach notification

If Cutout becomes aware of a personal data breach affecting institutional data, we will:

- Notify the institution without undue delay
- Provide relevant details about the incident

- Take reasonable steps to mitigate and remediate

The institution is responsible for determining any external notifications required by law.

8. Data retention and deletion

Cutout will retain institutional data only as long as necessary to provide the services and comply with legal obligations.

Upon termination of services or written request:

- Data will be securely deleted within 30 days
- Backup deletion will follow standard retention cycles

Institutions may request earlier deletion where feasible.

9. International transfers

Data may be processed on servers outside the institution's jurisdiction (including AWS infrastructure regions).

Cutout will ensure appropriate safeguards are in place, including:

- Contractual protections
- Secure transfer mechanisms
- Compliance with applicable laws

10. Audit and compliance

Where reasonably required for institutional compliance purposes, Cutout may provide:

- Information about security practices
- Documentation of safeguards
- Confirmation of compliance measures

Formal audits may be conducted only where legally required and subject to reasonable notice and confidentiality obligations.

11. Liability

Each party remains responsible for its own compliance with applicable data protection laws.

Cutout's liability will be limited to the extent permitted by the main services agreement.

12. Contact

For privacy and data protection enquiries:

Cutout Pty Ltd
info@cutout.fit
173 Hastings Parade
North Bondi NSW 2026