ClearCue – Data Processing Agreement (DPA) v1.2

Last updated: 02 February 2026

This Data Processing Agreement (“DPA”) forms part of the ClearCue Terms of Service and applies where ClearCue processes personal data on behalf of a customer using a **Studio (team) plan**.

---

1. Parties

Processor:

ClearCue Ltd, Hawarden, United Kingdom (“ClearCue”)

Controller:

The Studio plan customer (“Controller”)

---

2. Purpose & Scope

This DPA governs the processing of personal data by ClearCue on behalf of the Controller solely for the purpose of providing ClearCue’s **team-based timing-generation and clip-based cue tools** (the “Service”).

ClearCue:

- processes only the minimum personal data required to operate the Service
- does **not** access, analyse, store, or process creative content
- does **not** use customer data for analytics, profiling, AI training, advertising, or resale

This DPA applies **only** where ClearCue acts as a processor under UK GDPR / EU GDPR.

---

3. Roles of the Parties

Controller

The Studio plan customer determines the purposes and means of processing personal data relating to its team members.

Processor

ClearCue processes personal data strictly on documented instructions from the Controller to deliver the Service.

Sub-Processors

Only the sub-processors listed in Section 9 are authorised.

ClearCue does not appoint additional sub-processors without prior notice.

---

4. Categories of Data Processed

4.1 Account & Team Data

- Name
- Email address
- Team membership (Studio plan)
- Seat assignments and roles (admin / user)

4.2 Service Usage Data

- Cue generation counts
- Selected parameters (e.g. BPM, cue type, duration, mode)
- Download timestamps
- Remaining quota
- Non-identifiable device/browser metadata

4.3 Payment Metadata

Payment processing is handled independently by Stripe.

ClearCue receives only limited billing metadata (e.g. subscription status, invoice records).

Explicit Exclusions

ClearCue does **not** process:

- audio or video uploads
- creative project files
- user-generated content
- special category (sensitive) personal data

---

5. Processing Instructions

ClearCue processes personal data only on the Controller's documented instructions, including to:

- create and manage team seats
- authenticate users
- enforce usage limits
- provide admin-visible usage reporting

No processing occurs beyond these purposes.

---

6. Processor Obligations

6.1 Confidentiality

All personnel with access to personal data are bound by confidentiality obligations.

6.2 Security Measures

ClearCue implements appropriate technical and organisational measures, including:

- TLS encryption in transit
- encryption at rest
- role-based access controls
- Firestore security rules
- audit logging
- least-privilege access
- key rotation

6.3 Breach Notification

ClearCue will notify the Controller **without undue delay** of any personal data breach, including:

- nature of the breach
- data affected
- mitigation steps taken
- recommended Controller actions

6.4 Assistance

ClearCue will reasonably assist with:

- data subject requests
- GDPR compliance queries
- security and compliance information

6.5 Data Deletion

Upon termination or written request, ClearCue will:

- delete or return personal data
- purge relevant system records

- confirm deletion where requested

---

7. Controller Obligations

The Controller is responsible for:

- ensuring a lawful basis for processing
- providing appropriate privacy notices to team members
- managing seat access appropriately
- ensuring authorised email addresses are used

---

8. International Transfers

Where data is processed outside the UK/EU, ClearCue ensures safeguards including:

- Standard Contractual Clauses (SCCs)
- UK GDPR Addendum
- encryption and access controls

---

9. Approved Sub-Processors

Sub-Processor	Purpose	Region
Google Cloud Platform	Database, storage, security	EU / US
Clerk	Authentication	US / EU

Stripe	Billing & invoicing	US / EU
Cloudflare	CDN & security	Global

---

10. Data Subject Rights

ClearCue assists the Controller in fulfilling GDPR rights, including:

- access
- rectification
- erasure
- restriction
- portability
- objection

ClearCue does not communicate directly with team members unless authorised.

---

11. Audit & Compliance

On reasonable request, ClearCue may provide:

- a summary of security controls
- an updated sub-processor list
- confirmation of compliance measures

No on-site or intrusive audits will occur without mutual written agreement.

---

12. Term & Termination

This DPA remains in effect for the duration of the Studio subscription.

Upon termination:

- personal data is deleted within 30 days
- backups expire automatically per infrastructure lifecycle policies

---

13. Liability

Liability is governed by the ClearCue Terms of Service, except where restricted by law.

---

14. Governing Law

This DPA is governed by the laws of England and Wales.

Jurisdiction lies exclusively with the courts of England and Wales.
