

Data Processing Agreement

Between ScoutCo and Client · Version date: 30 August 2026

Parties

This Data Processing Agreement ("DPA") is entered into between:

Data Controller: [Client company name] ("Client"), a company registered in [jurisdiction] with registered number [number].

Data Processor: ScoutCo, a trading name currently operating as a pre-incorporation entity, with legal entity registration pending, whose correspondence address is [address] ("ScoutCo"). ScoutCo operates the review and approval platforms available at earshots.io, trackscout.io, mixscout.io, cutscout.io, filescout.io, scoutco.io and podlook.io (together, "the Platform"). Each of these, including Podlook, is a product of ScoutCo.

This DPA forms part of and is subject to the ScoutCo Terms of Service ("Principal Agreement") between the parties, and takes effect on the date the Client accepts the Principal Agreement or signs this document, whichever is earlier.

1. Definitions

"Applicable Data Protection Law" means the UK GDPR, the Data Protection Act 2018, and any successor legislation.

"Controller", "Processor", "Data Subject", "Personal Data", "Processing", and "Supervisory Authority" have the meanings given in Applicable Data Protection Law.

"Platform Data" means any Personal Data uploaded to or generated within the Platform by or on behalf of the Client, including audio, video and podcast content, transcripts, user email addresses, project metadata, timestamped comments, and approval records.

2. Roles

The Client is the Data Controller of Platform Data. ScoutCo is the Data Processor, processing Platform Data solely on behalf of and under the instructions of the Client, as set out in Schedule 1.

3. ScoutCo's Obligations

ScoutCo shall:

- Process Platform Data only on documented instructions from the Client, including as set out in this DPA and the Principal Agreement, unless required to do so by applicable law
- Ensure that persons authorised to process Platform Data are subject to appropriate confidentiality obligations

- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including those set out in Schedule 2
- Not engage any sub-processor without prior notification to the Client (see clause 5)
- Assist the Client in responding to Data Subject rights requests, to the extent reasonably practicable
- Assist the Client in meeting its obligations under Articles 32–36 UK GDPR (security, breach notification, DPIAs), having regard to the nature of processing and information available to ScoutCo
- Notify the Client without undue delay (and within 48 hours where feasible) of any Personal Data breach affecting Platform Data
- At the Client's choice, delete or return all Platform Data on termination of the Principal Agreement, and certify in writing that it has done so, unless retention is required by law
- Make available to the Client all information reasonably necessary to demonstrate compliance with this DPA, and allow for and contribute to audits conducted by the Client or a mandated auditor

4. Client's Obligations

The Client warrants that:

- It has a lawful basis for processing the Personal Data it uploads to the Platform
- It has provided all necessary notices to, and obtained all necessary consents from, Data Subjects whose data it submits to the Platform — including, where AI-assisted features are used, any notices required in respect of the processing described in Schedule 1
- Its instructions to ScoutCo comply with Applicable Data Protection Law

5. Sub-processors

The Client provides general authorisation for ScoutCo to appoint sub-processors, subject to ScoutCo maintaining a current list of sub-processors (Schedule 3) and giving the Client at least 14 days' written notice of any new sub-processor. The Client may object to a new sub-processor on reasonable data protection grounds by notifying ScoutCo within 10 days of notice.

ScoutCo shall impose data protection obligations on sub-processors that are no less protective than this DPA and shall remain liable to the Client for sub-processor performance.

6. Access Controls — Specific Commitment

ScoutCo expressly commits that:

- No individual associated with ScoutCo who operates as a practitioner in the audio post-production, music supervision, video post-production or podcast production industries shall have access to Client project content in the ordinary course of business
- Access to the underlying databases is restricted to the Chief Technology Officer of ScoutCo (currently Jon Nangle) for operational and maintenance purposes only, and is not used for

commercial intelligence

- Each product line runs in its own isolated database, so Client data held in one ScoutCo product is not accessible through another
- These restrictions shall survive any change of personnel at ScoutCo and shall be reflected in updated internal access control policies

7. International Transfers

ScoutCo shall not transfer Platform Data outside the UK or EEA unless appropriate safeguards are in place in accordance with Chapter V UK GDPR, including the use of UK International Data Transfer Agreements, Standard Contractual Clauses with the UK Addendum, or reliance on adequacy regulations. The Client acknowledges that file storage and certain processing (Schedule 3) take place in the United States under such safeguards.

8. Liability

Each party's liability under this DPA shall be subject to the limitations set out in the Principal Agreement. Nothing in this DPA limits either party's liability for fraudulent misrepresentation or for death or personal injury caused by negligence.

9. Term and Termination

This DPA continues in force for the duration of the Principal Agreement. Obligations of confidentiality and deletion survive termination.

10. Governing Law

This DPA is governed by the laws of England and Wales. The parties submit to the exclusive jurisdiction of the English courts.

Schedule 1 — Details of Processing

Subject matter: Operation of the ScoutCo review and approval platforms, including Podlook

Duration: The term of the Principal Agreement

Nature and purpose: Hosting, storage, and delivery of audio, video and podcast content; facilitating timestamped review, comment and approval; managing access via share links scoped to the recipient; and, where the Client uses these features, speech-to-text transcription, translation, and AI-assisted summarisation and clip suggestion carried out through the sub-processors listed in Schedule 3

Types of Personal Data: Email addresses, names, IP addresses, voices and any Personal Data contained in uploaded audio/video/podcast content, transcripts derived from that content, timestamped comments, and approval records (approver names and email addresses)

Categories of Data Subjects: Client employees and freelance collaborators; composers, music supervisors and editors; podcast hosts, guests and producers; and end-user reviewers

Schedule 2 — Technical and Organisational Measures

- Encryption in transit (TLS 1.2 minimum) for all data
- Encryption at rest for all stored files (AWS S3 / Cloudflare R2 managed encryption)
- Role-based access control with least-privilege principles, enforced in the database by row-level security policies
- Isolated databases per product line; no cross-product data access
- Database access restricted to the CTO; infrastructure access events logged and auditable
- Share links generated with high-entropy cryptographically random codes; optional password protection
- Media served via signed, time-limited URLs scoped to the requesting project
- Password hashing using bcrypt or equivalent
- AI sub-processors receive only the content necessary for the requested operation, under terms that prohibit use of that content for model training
- Voice dictation for comments is processed in the reviewer's browser; that audio is not transmitted to or stored on ScoutCo servers
- Regular dependency and security updates; independent security review of changes before release
- Incident response procedure with 48-hour breach notification target

Schedule 3 — Approved Sub-processors

The following sub-processors are approved as at the date of this DPA:

Sub-processor	Services
Amazon Web Services, Inc. (AWS)	Object storage (S3, US-East regions); media processing (transcoding, exports); speech-to-text transcription (Amazon Transcribe); translation (Amazon Translate)
Cloudflare, Inc.	CDN and edge network; application hosting (Pages/Workers); object storage mirror (R2); inbound email routing
Supabase, Inc.	Databases and authentication, hosted within the EEA. Each product line runs in its own isolated database project (Podlook data is held separately from the other products' data)
Resend, Inc.	Transactional email delivery (sign-in links, notifications, early-access and approval emails)
Anthropic, PBC	AI processing on the Client's instruction: episode summaries and clip suggestions (Podlook). Content is processed solely to return results and is not used to train models, per API terms
AssemblyAI, Inc.	Speech-to-text transcription (Podlook)

Functional Software, Inc. (Sentry)	Application error monitoring (technical event data; not project content)
Stripe, Inc.	Payment processing (billing data only; no project data)
Netlify, Inc.	Legacy hosting and serverless functions (being decommissioned)

Signatures

Signed for and on behalf of ScoutCo:

Signature: _____

Name: _____

Title: _____

Date: _____

Signed for and on behalf of Client:

Signature: _____

Name: _____

Title: _____

Date: _____