DATA PROCESSING AGREEMENT

Between:

Client ("Data Controller" or "Controller" or "Customer")

AND

Aberdeen Captioning Inc.
DBA: Aberdeen Broadcast Services
30211 Avenida de las Banderas, Suite 110
Rancho Santa Margarita, CA 92688
("Data Processor" or "Processor" or "Aberdeen")

---

1. PURPOSE AND SCOPE

1.1 Purpose

This Data Processing Agreement ("DPA") forms part of the agreement between Customer and Aberdeen (the "Agreement") for the provision of captioning, transcription, and translation services ("Services"). This DPA governs Aberdeen's processing of Personal Data on behalf of Customer.

1.2 Scope

This DPA applies whenever Aberdeen processes Personal Data as a Processor on behalf of Customer acting as a Controller, in connection with the Services provided under the Agreement.

1.3 Hierarchy

In the event of any conflict or inconsistency between this DPA and the Agreement, this DPA shall prevail with respect to the processing of Personal Data.

---

2. DEFINITIONS

For purposes of this DPA:

"Applicable Data Protection Law" means all laws and regulations applicable to the processing of Personal Data under this DPA, including:

- General Data Protection Regulation (EU) 2016/679 ("GDPR")
- UK Data Protection Act 2018 and UK GDPR
- California Consumer Privacy Act (Cal. Civ. Code § 1798.100 et seq.) and California Privacy Rights Act ("CCPA/CPRA")
- Health Insurance Portability and Accountability Act ("HIPAA") (where applicable)
- Any other applicable U.S. state privacy laws

"Controller" means the entity that determines the purposes and means of processing Personal Data. For purposes of this DPA, Customer acts as the Controller.

"Customer Data" means all data, including Personal Data and audio/video content, that Customer submits to Aberdeen for processing through the Services.

"Data Subject" means an identified or identifiable natural person whose Personal Data is processed under this DPA. This includes "Consumer" as defined under CCPA and any individual identified or referenced in audio/video content.

"Personal Data" means any information relating to an identified or identifiable natural person that is processed by Aberdeen under this DPA. This includes audio recordings containing voices, video recordings containing images, names, and any other identifiable information in Customer Data.

"Processing" means any operation or set of operations performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, retrieval, use, disclosure, transmission, deletion, or destruction.

"Processor" means an entity that processes Personal Data on behalf of the Controller. For purposes of this DPA, Aberdeen acts as the Processor.

"Security Incident" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

"Standard Contractual Clauses" or **"SCCs"** means the standard contractual clauses for the transfer of personal data to third countries approved by the European Commission.

"Sub-processor" means any third party engaged by Aberdeen to process Personal Data on Customer's behalf.

---

3. ROLES AND RESPONSIBILITIES

3.1 Aberdeen as Processor

Aberdeen acts as a Processor when processing Personal Data on Customer's behalf for the provision of Services. Aberdeen will process Personal Data only in accordance with Customer's documented instructions and Applicable Data Protection Law.

3.2 Customer as Controller

Customer acts as the Controller and is responsible for:

- Determining the purposes and means of processing Personal Data
- Ensuring it has all necessary legal bases for processing (including obtaining consents where required)
- Providing Aberdeen with lawful processing instructions
- Ensuring compliance with Applicable Data Protection Law regarding its provision of Personal Data to Aberdeen
- Responding to Data Subject requests regarding Personal Data

3.3 Independent Controllers

When each party processes Personal Data for its own purposes (e.g., Aberdeen processing Customer contact information for account management), each party acts as an independent Controller and is responsible for its own compliance with Applicable Data Protection Law.

---

4. PROCESSING DETAILS

4.1 Nature and Purpose of Processing

Aberdeen processes Personal Data for the following purposes:

- Providing captioning services (live CART and post-production)
- Providing transcription services
- Providing translation services
- Delivering completed transcripts and captions to Customer
- Customer support and service delivery
- Compliance with legal obligations

4.2 Duration of Processing

Aberdeen will process Personal Data for the duration necessary to provide the Services and as follows:

- **Live Captioning:** Audio processed in real-time is retained only during active service delivery and deleted immediately after transcript delivery unless Customer requests otherwise

- **Post-Production Captioning:** Audio/video files retained for 2 weeks after delivery by default, or as customized per Customer's instructions (immediate deletion or extended retention)
- **Account Data:** Retained for the duration of the business relationship and as required by law

4.3 Categories of Data Subjects

Personal Data processed may relate to the following categories of Data Subjects:

- Customer's employees, contractors, and authorized users
- Attendees of meetings, conferences, events, and training sessions
- Speakers at government proceedings, educational lectures, ministry services
- Participants in recorded content
- Any individuals whose voices or images appear in audio/video content
- End-users of Customer's services

4.4 Types of Personal Data

Aberdeen may process the following categories of Personal Data:

- **Contact Information:** Names, email addresses, phone numbers, job titles
- **Audio Data:** Voice recordings, speech patterns, conversations
- **Visual Data:** Video recordings, images of individuals
- **Content Data:** Transcripts, captions, meeting content, educational materials
- **Account Data:** Login credentials, service preferences, billing information
- **Usage Data:** Service utilization data, timestamps, file metadata

Special Categories of Data: Aberdeen does not intentionally process special categories of Personal Data (such as health information, biometric data, racial/ethnic origin, religious beliefs) unless explicitly authorized by Customer in writing and with appropriate safeguards.

---

5. CUSTOMER INSTRUCTIONS

5.1 Documented Instructions

Customer instructs Aberdeen to process Personal Data as follows:

- To provide the Services as described in the Agreement
- To comply with this DPA and Applicable Data Protection Law
- As further specified in Customer's service requests and configurations

5.2 Additional Instructions

Aberdeen will process Personal Data only in accordance with Customer's documented instructions unless required to do so by Applicable Data Protection Law, in which case Aberdeen will inform Customer of that legal requirement before processing (unless prohibited by law from doing so).

5.3 Instruction Modifications

Customer may modify, amend, or add to its instructions by providing written notice to Aberdeen. Aberdeen will assess whether it can comply with modified instructions and will inform Customer if it cannot.

5.4 Unlawful Instructions

If Aberdeen believes that any instruction from Customer violates Applicable Data Protection Law, Aberdeen will promptly inform Customer and may suspend processing until the instruction is confirmed or modified.

---

6. DATA SECURITY

6.1 Security Measures

Aberdeen implements appropriate technical and organizational security measures to protect Personal Data against Security Incidents, including:

Encryption:

- All data in transit encrypted using TLS 1.2 or stronger
- All data at rest encrypted using AES 256 or stronger

Access Controls:

- Role-based access controls (RBAC)
- Multi-factor authentication for system access
- Regular access reviews and permission audits
- Principle of least privilege access

Monitoring and Logging:

- Continuous security monitoring and logging
- Automated alerting for suspicious activities
- Security Information and Event Management (SIEM)
- Audit trails of all data access

Personnel Security:

- Background checks for employees with data access
- Confidentiality agreements and NDAs required for all personnel
- Monthly security and privacy training
- Defined roles and responsibilities

Infrastructure Security:

- Hosted on Salesforce and AWS platforms with SOC 2 Type II and ISO 27001 certifications
- Regular security audits and assessments
- Secure development practices
- Incident response procedures

6.2 Security Documentation

Aberdeen will provide Customer with reasonable information about its security measures upon written request, subject to confidentiality obligations.

6.3 Security Updates

Aberdeen will regularly review and update its security measures to maintain an appropriate level of security for the risks presented by processing Personal Data.

---

7. SUB-PROCESSORS

7.1 General Authorization

Customer provides general authorization for Aberdeen to engage Sub-processors to process Personal Data, subject to the requirements in this Section 7.

7.2 Current Sub-processors

Aberdeen currently engages the following Sub-processors:

Sub-processor	Service Provided	Location
Salesforce	CRM and service delivery platform	United States
Amazon Web Services (AWS)	Cloud hosting and infrastructure	United States
AWS Transcribe	AI transcription services (when AI selected)	United States
Deepgram	AI transcription services (when AI selected)	United States
Speechmatics	AI transcription services (when AI selected)	United States
OpenAI Whisper	AI transcription services (when AI selected)	United States

7.3 Sub-processor Obligations

Aberdeen will:

- Impose data protection obligations on each Sub-processor that are substantially equivalent to those in this DPA
- Ensure Sub-processors comply with Applicable Data Protection Law
- Remain fully liable to Customer for the performance of each Sub-processor
- Ensure Sub-processors maintain appropriate security measures

7.4 Changes to Sub-processors

Aberdeen will provide Customer with at least 30 days' prior written notice of any new Sub-processor or changes to existing Sub-processors. Notice will be provided via email to Customer's designated contact.

7.5 Customer Objection Rights

Customer may object to a new or replacement Sub-processor on reasonable grounds relating to data protection. Customer must notify Aberdeen in writing within 15 days of receiving notice. If Customer objects, the parties will work together in good faith to find a resolution. If no resolution is found, Customer may terminate the affected Services.

7.6 Sub-processor List

An up-to-date list of Sub-processors is available upon request by emailing matt@aberdeen.io or deepthi@aberdeen.io.

---

8. DATA SUBJECT RIGHTS

8.1 Assistance with Data Subject Requests

Aberdeen will provide reasonable assistance to Customer in responding to Data Subject requests to exercise their rights under Applicable Data Protection Law, including:

- Right of access
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restriction of processing
- Right to data portability
- Right to object to processing
- Rights related to automated decision-making

8.2 Forwarding Requests

If Aberdeen receives a Data Subject request directly, Aberdeen will promptly forward it to Customer without undue delay and will not respond to the request without Customer's prior written authorization.

8.3 Technical Assistance

Aberdeen will provide Customer with access to Aberdeen's systems and tools necessary to enable Customer to respond to Data Subject requests, taking into account the nature of the processing.

8.4 Fees

Aberdeen may charge reasonable fees for assistance with Data Subject requests that require extensive time and resources beyond normal service operations. Fees will be communicated to Customer in advance.

---

9. SECURITY INCIDENTS

9.1 Notification Obligation

Aberdeen will notify Customer without undue delay, and in any event within 72 hours, upon becoming aware of a Security Incident affecting Customer's Personal Data.

9.2 Notification Contents

The notification will include, to the extent possible:

- Description of the nature of the Security Incident

- Categories and approximate number of Data Subjects affected
- Categories and approximate number of Personal Data records affected
- Likely consequences of the Security Incident
- Measures taken or proposed to address the Security Incident and mitigate potential adverse effects

9.3 Investigation and Remediation

Aberdeen will:

- Promptly investigate the Security Incident
- Take reasonable steps to remediate the Security Incident
- Implement measures to prevent similar incidents
- Provide Customer with reasonable cooperation and assistance

9.4 Additional Information

Aberdeen will provide additional information about the Security Incident as it becomes available and upon Customer's reasonable request.

9.5 No Acknowledgment of Liability

Notification of a Security Incident under this Section 9 does not constitute Aberdeen's acknowledgment of fault or liability.

---

10. DATA TRANSFERS

10.1 Location of Processing

Personal Data is primarily processed and stored in the United States through Aberdeen's Salesforce and AWS infrastructure. All data is stored within AWS regions in the United States.

10.2 International Transfers

If Personal Data is transferred outside the European Economic Area (EEA), United Kingdom, or Switzerland, Aberdeen will ensure that:

- The transfer is to a country deemed adequate by the relevant data protection authority, or
- Appropriate safeguards are in place, such as Standard Contractual Clauses (SCCs), Binding Corporate Rules, or other legally recognized transfer mechanisms

10.3 Standard Contractual Clauses

Upon Customer's request, Aberdeen will execute the Standard Contractual Clauses approved by the European Commission for transfers of Personal Data to third countries. Aberdeen relies on the SCCs implemented by Salesforce and AWS for data transfers.

10.4 Additional Safeguards

Aberdeen implements additional technical and organizational measures to protect Personal Data transferred internationally, including encryption, access controls, and contractual protections with Sub-processors.

---

11. DATA RETENTION AND DELETION

11.1 Retention Periods

Aberdeen will retain Personal Data only as long as necessary for the purposes set out in this DPA and as instructed by Customer:

Live Captioning:

- Audio: Deleted immediately after transcript delivery (unless Customer requests retention)
- Transcripts: Delivered to Customer and retained per Customer's instructions

Post-Production Captioning:

- **Default:** Audio/video files retained for 2 weeks after delivery, then automatically purged
- **Upon Request:** Immediate deletion after delivery OR extended retention per Customer's schedule
- Transcripts: Delivered to Customer and retained per Customer's instructions

Account Information:

- Retained during the business relationship
- Financial records retained for 7 years per IRS requirements
- Other data retained as required by law

11.2 Deletion or Return

Upon termination of the Agreement or upon Customer's request, Aberdeen will, at Customer's choice:

- Delete all Personal Data (including copies) within 30 days, or
- Return all Personal Data to Customer in a commonly used, machine-readable format

11.3 Retention Exceptions

Aberdeen may retain Personal Data to the extent required by Applicable Data Protection Law, in which case Aberdeen will inform Customer of such legal requirement and will continue to protect the Personal Data in accordance with this DPA.

11.4 Backup Copies

Personal Data in backup systems will be securely isolated and deleted in accordance with Aberdeen's backup retention policies (generally within 90 days of deletion from production systems).

---

12. AUDITS AND COMPLIANCE

12.1 Audit Rights

Customer has the right to conduct audits or inspections to verify Aberdeen's compliance with this DPA, subject to the following conditions:

- Audits may be conducted no more than once per year
- Customer must provide at least 30 days' advance written notice
- Audits must be conducted during normal business hours
- Audits must not unreasonably interfere with Aberdeen's operations
- Customer or its auditor must execute a confidentiality agreement
- Customer is responsible for all costs of the audit

12.2 Aberdeen Certifications

In lieu of conducting its own audit, Customer may request and review Aberdeen's existing audit reports and certifications, including:

- SOC 2 Type II reports (from Salesforce and AWS platforms)
- ISO 27001 certifications (from Salesforce and AWS platforms)
- Other relevant security certifications and attestations

12.3 Cooperation

Aberdeen will cooperate with reasonable audit requests and provide Customer with information necessary to demonstrate compliance with this DPA.

12.4 Remediation

If an audit reveals non-compliance with this DPA, Aberdeen will:

- Provide a written remediation plan within 30 days
- Implement corrective measures in a timely manner
- Provide updates on remediation progress

---

13. CONFIDENTIALITY

13.1 Personnel Obligations

Aberdeen will ensure that all personnel who have access to Personal Data:

- Are bound by appropriate confidentiality obligations
- Have signed Non-Disclosure Agreements (NDAs)
- Receive regular security and privacy training
- Process Personal Data only as authorized by Aberdeen

13.2 Confidentiality Period

Confidentiality obligations survive the termination of this DPA and the Agreement.

---

14. LIABILITY AND INDEMNIFICATION

14.1 Aberdeen's Liability

Aberdeen is liable to Customer for damages resulting from Aberdeen's breach of this DPA or Applicable Data Protection Law, subject to the limitations of liability set forth in the Agreement.

14.2 Sub-processor Liability

Aberdeen remains fully liable for the acts and omissions of its Sub-processors to the same extent as if Aberdeen had performed the services itself.

14.3 Indemnification

Aberdeen will indemnify and hold Customer harmless from and against any claims, damages, losses, liabilities, and expenses (including reasonable attorneys' fees) arising from Aberdeen's breach of this DPA or violation of Applicable Data Protection Law, except to the extent the claim arises from Customer's instructions or actions.

---

15. CALIFORNIA-SPECIFIC PROVISIONS

15.1 CCPA/CPRA Compliance

When acting as a Service Provider under the CCPA/CPRA, Aberdeen certifies that:

- Aberdeen understands the restrictions and obligations of this DPA
- Aberdeen will process Personal Data only for the business purposes specified in this DPA
- Aberdeen will not sell or share Personal Data
- Aberdeen will not retain, use, or disclose Personal Data outside the business relationship with Customer
- Aberdeen will not combine Personal Data with data from other sources

15.2 Disclosure Prohibition

Aberdeen will not disclose Personal Data to any third party except as authorized by Customer or required by law.

15.3 Consumer Requests

Aberdeen will assist Customer in responding to consumer requests under CCPA/CPRA and will forward any such requests received directly to Customer.

---

16. HIPAA PROVISIONS (IF APPLICABLE)

16.1 Business Associate Agreement

If Customer provides Protected Health Information (PHI) as defined by HIPAA to Aberdeen, the parties agree to execute a separate Business Associate Agreement (BAA) that complies with HIPAA requirements.

16.2 HIPAA Compliance

Aberdeen will:

- Implement appropriate safeguards to protect PHI
- Report any unauthorized use or disclosure of PHI
- Ensure Sub-processors handling PHI execute BAAs
- Make PHI available for amendment or accounting
- Make internal practices and records available for HHS review

16.3 BAA Requirement

Customer must explicitly request a BAA before providing any PHI to Aberdeen. Services involving PHI will not commence until a BAA is fully executed.

---

17. NO AI TRAINING ON CUSTOMER DATA

17.1 Prohibition on Model Training

Aberdeen will NOT use Customer Data to train AI models. Aberdeen maintains strict contractual agreements with all AI Sub-processors (AWS Transcribe, Deepgram, Speechmatics, OpenAI Whisper) that prohibit the use of Customer Data for:

- Training proprietary AI models
- Training models made available to other customers
- Training public models
- Improving or developing AI services beyond direct service delivery

17.2 Service Delivery Only

AI Sub-processors process Customer Data solely for the purpose of providing the requested transcription services and will not retain Customer Data beyond the time necessary to deliver the service.

17.3 Customer Consent

Aberdeen will only use Customer Data for AI training purposes if Customer provides explicit written consent. No such training will occur without Customer's prior authorization.

---

18. DATA PROTECTION IMPACT ASSESSMENTS

18.1 Assistance with DPIAs

Aberdeen will provide reasonable assistance to Customer in conducting Data Protection Impact Assessments (DPIAs) required under Applicable Data Protection Law.

18.2 Information Provision

Aberdeen will provide Customer with information about Aberdeen's processing activities, security measures, and Sub-processors necessary to conduct DPIAs.

18.3 Prior Consultation

If a DPIA indicates that processing would result in high risk, Aberdeen will provide reasonable assistance to Customer in consulting with relevant supervisory authorities.

---

19. RECORDS AND DOCUMENTATION

19.1 Processing Records

Aberdeen will maintain records of all categories of processing activities carried out on behalf of Customer, including:

- Name and contact details of Aberdeen and Customer
- Categories of processing
- Categories of Data Subjects and Personal Data
- Sub-processors
- International data transfers
- Security measures

19.2 Availability

Aberdeen will make these records available to Customer and relevant supervisory authorities upon request.

---

20. TERM AND TERMINATION

20.1 Term

This DPA takes effect on the Effective Date and continues for the duration of the Agreement or as long as Aberdeen processes Personal Data on behalf of Customer.

20.2 Effect of Termination

Upon termination of this DPA or the Agreement:

- Aberdeen will cease processing Personal Data
- Aberdeen will delete or return Personal Data per Section 11
- The obligations regarding confidentiality, data deletion, and audit rights survive termination

20.3 Survival

The following sections survive termination: Sections 11 (Data Retention and Deletion), 13 (Confidentiality), 14 (Liability and Indemnification), and 17 (No AI Training).

---

21. GENERAL PROVISIONS

21.1 Amendments

This DPA may only be amended by written agreement signed by both parties.

21.2 Severability

If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions will remain in full force and effect.

21.3 Entire Agreement

This DPA, together with the Agreement, constitutes the entire agreement between the parties regarding data processing.

21.4 Governing Law

This DPA is governed by the same law as the Agreement, except where Applicable Data Protection Law requires otherwise.

21.5 Notices

All notices under this DPA must be in writing and sent to:

Aberdeen Captioning Inc.
30211 Avenida de las Banderas, Suite 110
Rancho Santa Margarita, CA 92688
Email: matt@aberdeen.io and deepthi@aberdeen.io