

Data Processing Agreement

Version: 1.0.0 **Date:** 2026-07-07

This Data Processing Agreement (“**DPA**”) is entered into between:

- **Data Controller:** The customer (“**Controller**”, “**you**”, “**Customer**”) as identified in the applicable Order
- **Data Processor:** TODO COMPANY LEGAL NAME (“**Processor**”, “**we**”, “**us**”), registered at Laan van Chartroise 219
3552ET Utrecht
Netherlands, KVK TODO KVK NUMBER

This DPA forms part of the Terms and Conditions and applies where Processor processes Personal Data on behalf of Controller.

Definitions

Means the GDPR, applicable EU Member State data protection laws, and any other laws relating to privacy and data protection. Means Personal Data that Processor processes on behalf of Controller in connection with the Service. Means an identified or identifiable natural person whose Personal Data is processed. Means Regulation (EU) 2016/679 (General Data Protection Regulation). Means any information relating to an identified or identifiable natural person. Means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. Has the meaning given in the GDPR. Means a third party engaged by Processor to process Controller Personal Data. Means an independent public authority established by an EU Member State pursuant to the GDPR.

Scope and Roles

Roles

The parties acknowledge that:

1. Controller is the data controller for Controller Personal Data
2. Processor is the data processor for Controller Personal Data
3. Processor processes Controller Personal Data on behalf of Controller

Scope

This DPA applies to all Processing of Controller Personal Data in connection with the Service.

Duration

This DPA remains in effect for the duration of Processing, including after termination of the main Agreement until all Controller Personal Data is deleted or returned.

Details of Processing

Subject Matter

Processing of Personal Data in connection with the provision of the Evidia Platform, including meeting recording, transcription, AI-powered analysis, and compliance reporting.

Duration of Processing

Processing continues for the term of the main Agreement and until deletion or return of Controller Personal Data.

Nature and Purpose of Processing

Activity	Purpose
Recording	Capture audio from meetings for transcription
Transcription	Convert audio to text using speech-to-text technology
Analysis	Generate compliance scores, summaries, action items
Storage	Retain recordings, transcripts, and analysis results
Access control	Enable authorised users to access data
Reporting	Generate compliance and audit reports
Support	Provide customer support and troubleshooting
Security	Detect and prevent security incidents

Categories of Personal Data

- **Account data:** Name, email address, role, organisation
- **Meeting data:** Audio recordings (voice/biometric), transcripts, metadata
- **Analysis data:** AI-generated compliance findings, summaries
- **Consent records:** Consent timestamps, IP addresses
- **Usage data:** Access logs, feature usage, device information

Special Categories of Data

Processor processes the following special categories of Personal Data:

- **Biometric data (voice):** Audio recordings contain voice data that may be used for speaker identification
- **Health data:** May be present in meeting content if discussed during financial advice conversations

Controller is responsible for ensuring a valid legal basis for Processing special categories of data under Article 9 GDPR.

Categories of Data Subjects

- Controller's employees and authorised users
- Meeting participants (clients, candidates, colleagues)
- Other individuals whose data is contained in meeting recordings

Controller Obligations

Controller warrants and undertakes that:

Lawful Processing

1. Processing of Controller Personal Data by Processor will be lawful
2. Controller has provided (and will continue to provide) all required notices to Data Subjects
3. Controller has obtained (and will continue to obtain) all necessary consents
4. Controller has and will maintain a valid legal basis for Processing

Dual Consent

For meeting recordings, Controller shall:

1. Obtain explicit consent from the advisor before recording
2. Obtain explicit consent from each meeting participant before recording
3. Maintain records of consent in accordance with Article 7 GDPR
4. Inform participants of AI analysis and its implications

Instructions

1. Controller's instructions to Processor will comply with Applicable Law
2. Controller will ensure Processor's Processing remains within the scope of instructions
3. Controller will not instruct Processor to process Personal Data in violation of Applicable Law

Data Minimisation

Controller will minimise the Personal Data uploaded to the Service and will not upload Personal Data that is not necessary for the intended purposes.

Processor Obligations

Processor agrees to:

Process Only on Instructions

1. Process Controller Personal Data only on documented instructions from Controller
2. Immediately inform Controller if any instruction infringes Applicable Law
3. Not process Controller Personal Data for Processor's own purposes

Confidentiality

1. Ensure that persons authorised to process Controller Personal Data are bound by confidentiality obligations
2. Limit access to Controller Personal Data to those who need to know

Security Measures

Implement appropriate technical and organisational measures to secure Controller Personal Data, including:

1. **Encryption:** AES-256 at rest, TLS 1.3 in transit
2. **Access control:** Role-based access, multi-tenant isolation via row-level security (RLS)
3. **Authentication:** OpenID Connect with MFA support
4. **Audit logging:** Hash-chained, tamper-evident audit trail
5. **Infrastructure security:** Regular vulnerability scanning, security assessments

See Chapter ?? for detailed security information.

Staff Training

Ensure that staff processing Controller Personal Data:

1. Have received appropriate training on data protection
2. Are aware of the confidential nature of Controller Personal Data
3. Understand their obligations under this DPA

Conditions for Sub-processing

1. Engage Sub-processors only with Controller's prior written authorisation
2. Impose data protection obligations on Sub-processors equivalent to this DPA
3. Remain fully liable to Controller for Sub-processor performance

Assistance

Assist Controller with:

1. Data subject rights requests (access, rectification, erasure, portability)
2. Data protection impact assessments (DPIAs)
3. Prior consultations with Supervisory Authorities

Deletion and Return

Upon termination or at Controller's request:

1. Delete or return all Controller Personal Data
2. Delete existing copies unless retention is required by law
3. Certify deletion upon request

Sub-processors

Authorised Sub-processors

Controller authorises Processor to engage the following Sub-processors:

Name	Location	Purpose
Recall.ai Inc.	EU	Meeting bot recording and calendar integration
Deepgram, Inc.	EU	Speech-to-text transcription
Soniox d.o.o.	EU	Speech-to-text transcription
Hetzner	EU	Cloud infrastructure and hosting
S3-compatible storage	EU	Object storage for recordings
PostgreSQL	EU	Database services

Changes to Sub-processors

1. Processor will notify Controller of additions or replacements at least 30 days in advance
2. Notification will be sent to Controller's email address on file
3. Controller may object on reasonable data protection grounds within 15 days
4. If objection is unresolved, Controller may terminate the affected Processing

Sub-processor Agreements

Processor will ensure each Sub-processor is bound by a written agreement providing:

1. The same level of protection as this DPA
2. GDPR Article 28 compliant terms
3. Technical and organisational security measures

Data Subject Rights

Assistance

Processor will assist Controller in responding to Data Subject requests by:

1. Providing technical capabilities to export or delete Personal Data

2. Responding to Controller's requests for assistance within reasonable timeframes
3. Not responding directly to Data Subjects without Controller's authorisation

Response Timeframe

Processor will respond to Controller's assistance requests within 10 business days, or within the timeframe required to meet Controller's GDPR obligations.

Security Measures

Technical Measures

Processor implements the following technical measures:

1. Encryption:

- AES-256 encryption for data at rest
- TLS 1.3 for data in transit
- Encrypted secrets management

2. Access Control:

- Role-based access control (RBAC)
- Row-level security (RLS) for multi-tenant isolation
- Multi-factor authentication (MFA)
- Session management and timeout

3. Audit Logging:

- Hash-chained audit trail
- All security-relevant events logged
- Tamper-evident storage

4. Network Security:

- Firewall protection
- Network segmentation
- DDoS protection

Organisational Measures

1. Security policies and procedures
2. Staff training and awareness
3. Background checks for personnel with access
4. Vendor security assessments

Security Certifications

[TODO: List any security certifications (e.g., ISO 27001, SOC 2)]

Personal Data Breaches

Notification

Processor will notify Controller without undue delay (and in any event within 48 hours) after becoming aware of a Personal Data Breach affecting Controller Personal Data.

Notification Contents

Notification will include:

1. Nature of the breach including categories and approximate number of Data Subjects
2. Name and contact details of the data protection officer
3. Likely consequences of the breach
4. Measures taken or proposed to address the breach

Assistance

Processor will:

1. Cooperate with Controller in investigating the breach
2. Take reasonable steps to contain, mitigate, and remediate
3. Provide information reasonably required for Controller's supervisory authority notification

Costs

Processor will bear its own costs of investigating and remediating breaches caused by Processor's failure to meet its obligations under this DPA.

International Data Transfers

EU Data Residency

Processor stores and processes all Controller Personal Data within the European Union. Processor will not transfer Controller Personal Data outside the EEA without Controller's prior written consent.

Sub-processor Transfers

Processor ensures that all Sub-processors either:

1. Process data within the EEA, or
2. Provide appropriate safeguards (Standard Contractual Clauses, Binding Corporate Rules, or equivalent)

Audit Rights

Audit Rights

Information

Processor will make available to Controller all information reasonably necessary to demonstrate compliance with this DPA and Article 28 GDPR.

Audits

1. Controller may conduct audits or inspections with reasonable notice
2. Audits must be conducted during normal business hours
3. Controller will bear its own audit costs unless a material breach is discovered
4. Processor may require a confidentiality agreement before providing access

Third-Party Certifications

Processor may demonstrate compliance through third-party audit reports (e.g., SOC 2, ISO 27001) where such reports address Controller's reasonable requirements.

Liability

Processor Liability

Processor is liable only for damages caused by Processing where Processor:

1. Has not followed Controller's documented instructions, or
2. Has acted in breach of this DPA or Applicable Law

Controller Liability

Controller is liable for damages caused by:

1. Unlawful or unclear instructions
2. Failure to comply with Controller's own GDPR obligations
3. Failure to obtain necessary consents

Deletion and Return

Deletion and Return of Data

Upon Termination

Upon termination of the main Agreement or this DPA:

1. Controller may request export of Controller Personal Data within 30 days
2. Processor will delete all Controller Personal Data within 90 days
3. Deletion will include backups (subject to technical constraints)

Legal Retention

Processor may retain Controller Personal Data where required by Applicable Law, provided that:

1. Processor informs Controller of the retention requirement
2. Processor continues to protect the data in accordance with this DPA
3. Processor deletes the data as soon as retention is no longer required

Certification

Upon Controller's written request, Processor will provide written certification of deletion.
General Terms

General Terms

Amendments

This DPA may only be amended in writing signed by both parties.

Order of Precedence

In the event of conflict:

1. This DPA prevails over the main Terms and Conditions regarding Processing
2. Controller's written instructions prevail over this DPA
3. Applicable Law prevails over this DPA

Governing Law

This DPA is governed by Dutch law.

Contact

- **Privacy Contact:** privacy@evidia.ai

Appendix: Standard Contractual Clauses

Standard Contractual Clauses

Where required for international transfers, the parties agree to be bound by the Standard Contractual Clauses approved by the European Commission (Decision 2021/914), with the following specifications:

- **Module:** Module Two (Controller to Processor)
- **Clause 7 (Docking clause):** Not applicable
- **Clause 9 (Use of sub-processors):** Option 2 (general written authorisation)
- **Clause 11 (Redress):** Not applicable

- **Clause 17 (Governing law):** Dutch law
- **Clause 18 (Choice of forum):** courts of Amsterdam, Netherlands

[TODO: Attach full text of Standard Contractual Clauses if required]