Privacy Policy

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

Introduction

Evidia (**"we"**, **"us"**, or **"our"**) is committed to protecting your privacy and personal data. This Privacy Policy explains how we collect, use, store, and protect personal data when you use the Evidia Platform (the **"Service"**).

We provide an AI-assisted meeting analysis service designed with human oversight as a core principle. All AI outputs are advisory and require human review before action. We are committed to compliance with the General Data Protection Regulation (GDPR), the EU AI Act (Regulation 2024/1689), applicable financial services regulations, and other relevant data protection laws.

Data Controller

TODO COMPANY LEGAL NAME is the data controller for personal data processed in connection with the Service.

- **Registered address:** Laan van Chartroise 219
  3552ET Utrecht
  Netherlands
- **KVK number:** TODO KVK NUMBER
- **VAT number:** TODO VAT NUMBER
- **Contact:** privacy@evidia.ai

Privacy Contact

For privacy and data protection matters, including exercising your data subject rights, please contact:

- **Privacy Contact:** Liam Woodleigh-Hardinge
- **Email:** privacy@evidia.ai

Scope

This Privacy Policy applies to:

1. **Users** — Individuals who create accounts and use the Service (e.g., financial advisors, recruiters)
2. **Meeting participants** — Individuals whose meetings are recorded, transcribed, or analysed

3. **Clients** — Individuals who participate in meetings with users (e.g., insurance clients, candidates)
4. **Website visitors** — Individuals who visit our website at https://evidia.ai

Personal Data We Collect

Account Data

When you create an account, we collect:

- Name and email address
- Organisation and role information
- Authentication credentials (managed via OpenID Connect providers)
- Profile preferences and settings

Meeting Data

When meetings are recorded and analysed, we process:

- **Audio recordings** — Voice data from meeting participants
- **Transcripts** — Text representation of spoken content
- **Metadata** — Meeting date, duration, participants, calendar information
- **Analysis results** — Compliance scores, action items, summaries generated by our AI
- **Consent records** — Records of consent provided by advisors and clients

Usage Data

We automatically collect:

- Device and browser information
- IP address and approximate location (country level)
- Service usage patterns and feature interactions
- Performance and diagnostic data

Communication Data

When you contact us, we may collect:

- Email content and attachments
- Support ticket information
- Feedback and survey responses

Legal Basis for Processing

We process personal data under the following legal bases:

Data Category	Legal Basis	Purpose
Audio recordings	Art. 6(1)(a) — Consent	Transcription and compliance analysis
Transcripts	Art. 6(1)(a) — Consent	AI-powered analysis and reporting
Account data	Art. 6(1)(b) — Contract	Account management and service delivery
Meeting metadata	Art. 6(1)(f) — Legitimate interest	Service improvement and compliance
Usage data	Art. 6(1)(f) — Legitimate interest	Service reliability and security
Special category data (voice)	Art. 9(2)(a) — Explicit consent	Transcription functionality

Dual Consent Requirement

For meeting recordings, we implement a **dual consent flow**:

1. **Advisor consent** — The professional using our Service must provide explicit consent before recording begins
2. **Client consent** — The meeting participant (e.g., client, candidate) must provide explicit consent before being recorded

Both consents are recorded with timestamps, IP addresses, and the version of the privacy notice provided. Recording does not proceed without valid consent from all parties.

How We Use Personal Data

We use personal data for the following purposes:

Service Delivery

- Recording and transcribing meetings
- Generating compliance analysis and reports
- Creating meeting summaries and action items
- Providing conversational AI assistance

Account Management

- Authenticating users via OpenID Connect
- Managing multi-tenant organisation access
- Processing payments and subscriptions

Security and Compliance

- Maintaining audit trails (hash-chained, tamper-evident)
- Detecting and preventing fraud or misuse
- Complying with regulatory obligations
- Responding to legal requests

Improvement and Development

- Improving transcription accuracy
- Enhancing AI analysis quality
- Developing new features

AI Processing and Human Oversight

As an AI-assisted documentation and analysis tool, we implement the following transparency and human oversight measures regardless of final classification:

Transparency

- All AI-generated content is clearly labelled
- Users are informed when interacting with AI systems
- AI system limitations are disclosed

Human Oversight

- Compliance scores require human review before action
- Critical AI decisions cannot be fully automated
- Users can override or reject AI recommendations
- Human approval is required for adverse compliance findings

Accuracy and Quality

- Regular accuracy testing and benchmarking
- User feedback mechanisms for AI errors
- Continuous monitoring of AI output quality

Data Sharing and Disclosure

Within Your Organisation

Data is shared within your organisation based on the multi-tenant structure you configure. Organisation administrators control access permissions.

Sub-processors

We use the following categories of sub-processors:

Category	Provider	Purpose
Recording	Recall.ai	Meeting bot recording
Transcription	Deepgram, Soniox	Speech-to-text conversion
Infrastructure	Hetzner	Cloud hosting and compute
Storage	S3-compatible	Audio and document storage
Database	PostgreSQL	Application data storage

All sub-processors are bound by data processing agreements and process data only within the EU.

Legal Requirements

We may disclose data if required by law, regulation, or legal process, including:

- Court orders or subpoenas
- Regulatory authority requests
- Law enforcement requirements

No Sale of Data

We do not sell personal data to third parties.

International Data Transfers

EU Data Residency

All personal data is stored and processed within the European Union. We do not transfer personal data outside the European Economic Area (EEA).

Sub-processor Verification

We verify that all sub-processors maintain EU data residency and appropriate safeguards:

- Data processing agreements with EU Standard Contractual Clauses
- Technical measures ensuring data remains in the EU
- Regular audits of sub-processor compliance

Data Retention

We retain personal data for the following periods:

Data Type	Retention	Basis
Audio recordings	Tenant-configurable	Financial services regulations
Transcripts	Tenant-configurable	Financial services regulations
Consent records	Tenant-configurable, subject to applicable legal requirements	Legal requirement
Audit logs	Tenant-configurable, subject to security and compliance requirements	Security and compliance
Account data	For the duration of the customer relationship and thereafter as required by law, contract, or legitimate business purposes	User request

Deletion Process

When data reaches the end of its retention period or upon valid deletion request:

1. Audio files are securely deleted from object storage
2. Database records are permanently removed
3. Anonymised aggregates may be retained for analytics
4. Deletion is logged in our audit system

Your Rights

Under the GDPR, you have the following rights:

Right to Access (Article 15)

You may request a copy of the personal data we hold about you. We will respond within 1 month.

Right to Rectification (Article 16)

You may request correction of inaccurate personal data. For transcripts, corrections are possible through our human review process.

Right to Erasure (Article 17)

You may request deletion of your personal data, subject to:

- Legal retention requirements (e.g., financial regulations)
- Ongoing legal proceedings
- Legitimate business interests

Right to Restrict Processing (Article 18)

You may request that we restrict processing of your data in certain circumstances.

Right to Data Portability (Article 20)

You may request your data in a portable format (JSON, PDF, or CSV).

Right to Object (Article 21)

You may object to processing based on legitimate interests.

Right to Withdraw Consent (Article 7)

Where processing is based on consent, you may withdraw consent at any time. Withdrawal does not affect the lawfulness of prior processing.

Exercising Your Rights

To exercise your rights:

1. Email privacy@evidia.ai with "Data Subject Request" in the subject line
2. Provide sufficient information to verify your identity
3. Specify which right(s) you wish to exercise

We will respond within 1 month (extendable by two months for complex requests).

Data Security

We implement comprehensive security measures:

Encryption

- **At rest:** AES-256 for all stored data
- **In transit:** TLS 1.3 for all data transfers

Access Control

- Multi-factor authentication (MFA) available
- Role-based access control (RBAC)
- Row-level security (RLS) for tenant isolation
- Regular access reviews

Audit Logging

- Comprehensive audit trail with integrity verification
- Security-relevant events logged
- Audit logs retained for Tenant-configurable, subject to security and compliance requirements

Infrastructure Security

- Regular security assessments
- Automated vulnerability scanning
- Incident response procedures

See Chapter **??** for detailed security information.

Data Breach Notification

In the event of a personal data breach:

1. We will assess the breach and associated risks
2. We will notify the supervisory authority within 72 hours (if required)
3. We will notify affected individuals without undue delay (if high risk)
4. We will document the breach and remediation measures

Children's Privacy

Our Service is not intended for children under 16 years of age. We do not knowingly collect personal data from children. If you believe we have collected data from a child, please contact privacy@evidia.ai.

Changes to This Policy

We may update this Privacy Policy from time to time. Material changes will be:

- Notified via email to registered users
- Posted on our website with an updated date
- Subject to re-consent where required by law

Right to Complain

If you believe we have not adequately addressed your privacy concerns, you have the right to lodge a complaint with a supervisory authority in your jurisdiction.

In the Netherlands, the supervisory authority is:

- **Autoriteit Persoonsgegevens**
- **Website:** https://autoriteitpersoonsgegevens.nl

Contact Us

For any questions about this Privacy Policy or our data practices:

- **Email:** privacy@evidia.ai
- **Address:** Laan van Chartroise 219
  3552ET Utrecht
  Netherlands