

# Evidia

Trust Centre

Legal and Compliance Documentation

Version 1.0.0

2026-07-07

TODO COMPANY LEGAL NAME

Laan van Chartroise 219  
3552ET Utrecht  
Netherlands

KVK: TODO KVK NUMBER

VAT: TODO VAT NUMBER

# Contents

---

|                                                  |          |
|--------------------------------------------------|----------|
| <b>Introduction</b>                              | <b>7</b> |
| <b>1 Privacy Policy</b>                          | <b>9</b> |
| 1.1 Introduction                                 | 9        |
| 1.1.1 Data Controller                            | 9        |
| 1.1.2 Privacy Contact                            | 9        |
| 1.2 Scope                                        | 10       |
| 1.3 Personal Data We Collect                     | 10       |
| 1.3.1 Account Data                               | 10       |
| 1.3.2 Meeting Data                               | 10       |
| 1.3.3 Usage Data                                 | 10       |
| 1.3.4 Communication Data                         | 11       |
| 1.4 Legal Basis for Processing                   | 11       |
| 1.4.1 Dual Consent Requirement                   | 11       |
| 1.5 How We Use Personal Data                     | 11       |
| 1.5.1 Service Delivery                           | 11       |
| 1.5.2 Account Management                         | 12       |
| 1.5.3 Security and Compliance                    | 12       |
| 1.5.4 Improvement and Development                | 12       |
| 1.6 AI Processing and Human Oversight            | 12       |
| 1.6.1 Transparency                               | 12       |
| 1.6.2 Human Oversight                            | 12       |
| 1.6.3 Accuracy and Quality                       | 12       |
| 1.7 Data Sharing and Disclosure                  | 13       |
| 1.7.1 Within Your Organisation                   | 13       |
| 1.7.2 Sub-processors                             | 13       |
| 1.7.3 Legal Requirements                         | 13       |
| 1.7.4 No Sale of Data                            | 13       |
| 1.8 International Data Transfers                 | 13       |
| 1.8.1 EU Data Residency                          | 13       |
| 1.8.2 Sub-processor Verification                 | 13       |
| 1.9 Data Retention                               | 14       |
| 1.9.1 Deletion Process                           | 14       |
| 1.10 Your Rights                                 | 14       |
| 1.10.1 Right to Access (Article 15)              | 14       |
| 1.10.2 Right to Rectification (Article 16)       | 15       |
| 1.10.3 Right to Erasure (Article 17)             | 15       |
| 1.10.4 Right to Restrict Processing (Article 18) | 15       |
| 1.10.5 Right to Data Portability (Article 20)    | 15       |

|          |                                       |           |
|----------|---------------------------------------|-----------|
| 1.10.6   | Right to Object (Article 21)          | 15        |
| 1.10.7   | Right to Withdraw Consent (Article 7) | 15        |
| 1.10.8   | Exercising Your Rights                | 15        |
| 1.11     | Data Security                         | 15        |
| 1.11.1   | Encryption                            | 15        |
| 1.11.2   | Access Control                        | 16        |
| 1.11.3   | Audit Logging                         | 16        |
| 1.11.4   | Infrastructure Security               | 16        |
| 1.12     | Data Breach Notification              | 16        |
| 1.13     | Children's Privacy                    | 16        |
| 1.14     | Changes to This Policy                | 16        |
| 1.15     | Right to Complain                     | 17        |
| 1.16     | Contact Us                            | 17        |
| <b>2</b> | <b>Terms and Conditions</b>           | <b>18</b> |
| 2.1      | Definitions                           | 18        |
| 2.2      | Agreement Formation                   | 18        |
| 2.2.1    | Acceptance of Terms                   | 18        |
| 2.2.2    | Order of Precedence                   | 18        |
| 2.2.3    | Changes to Terms                      | 19        |
| 2.3      | Service Description                   | 19        |
| 2.3.1    | Overview                              | 19        |
| 2.3.2    | AI Transparency and Human Oversight   | 19        |
| 2.3.3    | Service Availability                  | 19        |
| 2.3.4    | Service Changes                       | 19        |
| 2.4      | Subscriptions and Fees                | 20        |
| 2.4.1    | Subscription Terms                    | 20        |
| 2.4.2    | Fees and Payment                      | 20        |
| 2.4.3    | Taxes                                 | 20        |
| 2.4.4    | Price Changes                         | 20        |
| 2.5      | Use of Service                        | 20        |
| 2.5.1    | Permitted Use                         | 20        |
| 2.5.2    | Usage Limits                          | 20        |
| 2.5.3    | Acceptable Use Policy                 | 21        |
| 2.5.4    | Consent Obligations                   | 21        |
| 2.5.5    | User Responsibilities                 | 21        |
| 2.6      | Customer Data                         | 21        |
| 2.6.1    | Ownership                             | 21        |
| 2.6.2    | Processing                            | 21        |
| 2.6.3    | Data Security                         | 22        |
| 2.6.4    | Data Retention and Deletion           | 22        |
| 2.6.5    | Data Residency                        | 22        |
| 2.7      | Intellectual Property                 | 22        |
| 2.7.1    | Our IP                                | 22        |
| 2.7.2    | Feedback                              | 22        |
| 2.7.3    | AI-Generated Content                  | 22        |
| 2.8      | Confidentiality                       | 22        |
| 2.8.1    | Definition                            | 22        |
| 2.8.2    | Obligations                           | 23        |
| 2.8.3    | Exceptions                            | 23        |
| 2.9      | Warranties                            | 23        |

|          |                                              |           |
|----------|----------------------------------------------|-----------|
| 2.9.1    | Our Warranties . . . . .                     | 23        |
| 2.9.2    | Your Warranties . . . . .                    | 23        |
| 2.9.3    | Disclaimer . . . . .                         | 23        |
| 2.9.4    | AI Limitations . . . . .                     | 24        |
| 2.10     | Limitation of Liability . . . . .            | 24        |
| 2.10.1   | Exclusion of Consequential Damages . . . . . | 24        |
| 2.10.2   | Liability Cap . . . . .                      | 24        |
| 2.10.3   | Exceptions . . . . .                         | 24        |
| 2.11     | Indemnification . . . . .                    | 24        |
| 2.11.1   | Our Indemnity . . . . .                      | 24        |
| 2.11.2   | Your Indemnity . . . . .                     | 25        |
| 2.12     | Term and Termination . . . . .               | 25        |
| 2.12.1   | Term . . . . .                               | 25        |
| 2.12.2   | Termination for Convenience . . . . .        | 25        |
| 2.12.3   | Termination for Cause . . . . .              | 25        |
| 2.12.4   | Effects of Termination . . . . .             | 25        |
| 2.13     | General Terms . . . . .                      | 26        |
| 2.13.1   | Governing Law . . . . .                      | 26        |
| 2.13.2   | Dispute Resolution . . . . .                 | 26        |
| 2.13.3   | Assignment . . . . .                         | 26        |
| 2.13.4   | Force Majeure . . . . .                      | 26        |
| 2.13.5   | Entire Agreement . . . . .                   | 26        |
| 2.13.6   | Severability . . . . .                       | 26        |
| 2.13.7   | No Waiver . . . . .                          | 26        |
| 2.13.8   | Notices . . . . .                            | 26        |
| 2.14     | Contact . . . . .                            | 26        |
| <b>3</b> | <b>Data Processing Agreement</b>             | <b>27</b> |
| 3.1      | Definitions . . . . .                        | 27        |
| 3.2      | Scope and Roles . . . . .                    | 27        |
| 3.2.1    | Roles . . . . .                              | 27        |
| 3.2.2    | Scope . . . . .                              | 28        |
| 3.2.3    | Duration . . . . .                           | 28        |
| 3.3      | Details of Processing . . . . .              | 28        |
| 3.3.1    | Subject Matter . . . . .                     | 28        |
| 3.3.2    | Duration of Processing . . . . .             | 28        |
| 3.3.3    | Nature and Purpose of Processing . . . . .   | 28        |
| 3.3.4    | Categories of Personal Data . . . . .        | 28        |
| 3.3.5    | Special Categories of Data . . . . .         | 29        |
| 3.3.6    | Categories of Data Subjects . . . . .        | 29        |
| 3.4      | Controller Obligations . . . . .             | 29        |
| 3.4.1    | Lawful Processing . . . . .                  | 29        |
| 3.4.2    | Dual Consent . . . . .                       | 29        |
| 3.4.3    | Instructions . . . . .                       | 29        |
| 3.4.4    | Data Minimisation . . . . .                  | 30        |
| 3.5      | Processor Obligations . . . . .              | 30        |
| 3.5.1    | Process Only on Instructions . . . . .       | 30        |
| 3.5.2    | Confidentiality . . . . .                    | 30        |
| 3.5.3    | Security Measures . . . . .                  | 30        |
| 3.5.4    | Staff Training . . . . .                     | 30        |
| 3.5.5    | Conditions for Sub-processing . . . . .      | 30        |

|          |                                               |           |
|----------|-----------------------------------------------|-----------|
| 3.5.6    | Assistance . . . . .                          | 31        |
| 3.5.7    | Deletion and Return . . . . .                 | 31        |
| 3.6      | Sub-processors . . . . .                      | 31        |
| 3.6.1    | Authorised Sub-processors . . . . .           | 31        |
| 3.6.2    | Changes to Sub-processors . . . . .           | 31        |
| 3.6.3    | Sub-processor Agreements . . . . .            | 31        |
| 3.7      | Data Subject Rights . . . . .                 | 32        |
| 3.7.1    | Assistance . . . . .                          | 32        |
| 3.7.2    | Response Timeframe . . . . .                  | 32        |
| 3.8      | Security Measures . . . . .                   | 32        |
| 3.8.1    | Technical Measures . . . . .                  | 32        |
| 3.8.2    | Organisational Measures . . . . .             | 33        |
| 3.8.3    | Security Certifications . . . . .             | 33        |
| 3.9      | Personal Data Breaches . . . . .              | 33        |
| 3.9.1    | Notification . . . . .                        | 33        |
| 3.9.2    | Notification Contents . . . . .               | 33        |
| 3.9.3    | Assistance . . . . .                          | 33        |
| 3.9.4    | Costs . . . . .                               | 33        |
| 3.10     | International Data Transfers . . . . .        | 33        |
| 3.10.1   | EU Data Residency . . . . .                   | 33        |
| 3.10.2   | Sub-processor Transfers . . . . .             | 34        |
| 3.11     | Audit Rights . . . . .                        | 34        |
| 3.11.1   | Information . . . . .                         | 34        |
| 3.11.2   | Audits . . . . .                              | 34        |
| 3.11.3   | Third-Party Certifications . . . . .          | 34        |
| 3.12     | Liability . . . . .                           | 34        |
| 3.12.1   | Processor Liability . . . . .                 | 34        |
| 3.12.2   | Controller Liability . . . . .                | 34        |
| 3.13     | Deletion and Return of Data . . . . .         | 35        |
| 3.13.1   | Upon Termination . . . . .                    | 35        |
| 3.13.2   | Legal Retention . . . . .                     | 35        |
| 3.13.3   | Certification . . . . .                       | 35        |
| 3.14     | General Terms . . . . .                       | 35        |
| 3.14.1   | Amendments . . . . .                          | 35        |
| 3.14.2   | Order of Precedence . . . . .                 | 35        |
| 3.14.3   | Governing Law . . . . .                       | 35        |
| 3.14.4   | Contact . . . . .                             | 35        |
| 3.15     | Standard Contractual Clauses . . . . .        | 36        |
| <b>4</b> | <b>AI Disclosure and EU AI Act Compliance</b> | <b>37</b> |
| 4.1      | Introduction . . . . .                        | 37        |
| 4.2      | AI System Classification . . . . .            | 37        |
| 4.2.1    | EU AI Act Position . . . . .                  | 37        |
| 4.2.2    | Risk Classification Assessment . . . . .      | 37        |
| 4.2.3    | Transparency Obligations . . . . .            | 38        |
| 4.3      | AI Components in the Service . . . . .        | 38        |
| 4.3.1    | AI Functions . . . . .                        | 38        |
| 4.3.2    | Important Limitations . . . . .               | 38        |
| 4.4      | Human Oversight . . . . .                     | 39        |
| 4.4.1    | Design Principles . . . . .                   | 39        |
| 4.4.2    | User Responsibilities . . . . .               | 39        |

|          |                                       |           |
|----------|---------------------------------------|-----------|
| 4.5      | Transparency . . . . .                | 39        |
| 4.5.1    | Labelling . . . . .                   | 39        |
| 4.5.2    | User Notifications . . . . .          | 40        |
| 4.6      | Data and Privacy . . . . .            | 40        |
| 4.6.1    | Data Use . . . . .                    | 40        |
| 4.6.2    | Processing Location . . . . .         | 40        |
| 4.7      | Quality and Monitoring . . . . .      | 40        |
| 4.7.1    | Quality Practices . . . . .           | 40        |
| 4.7.2    | User Feedback . . . . .               | 40        |
| 4.8      | User Rights . . . . .                 | 41        |
| 4.8.1    | Right to Human Review . . . . .       | 41        |
| 4.8.2    | Right to Explanation . . . . .        | 41        |
| 4.8.3    | Right to Contest . . . . .            | 41        |
| 4.9      | Third-Party AI Providers . . . . .    | 41        |
| 4.10     | Contact . . . . .                     | 41        |
| <b>5</b> | <b>Security Architecture</b>          | <b>42</b> |
| 5.1      | Introduction . . . . .                | 42        |
| 5.2      | Security Governance . . . . .         | 42        |
| 5.2.1    | Security Leadership . . . . .         | 42        |
| 5.2.2    | Security Policies . . . . .           | 42        |
| 5.2.3    | Compliance Framework . . . . .        | 43        |
| 5.3      | Infrastructure Security . . . . .     | 43        |
| 5.3.1    | Hosting Environment . . . . .         | 43        |
| 5.3.2    | Network Security . . . . .            | 43        |
| 5.3.3    | Server Hardening . . . . .            | 43        |
| 5.4      | Data Security . . . . .               | 44        |
| 5.4.1    | Data Classification . . . . .         | 44        |
| 5.4.2    | Encryption . . . . .                  | 44        |
| 5.4.3    | Data Residency . . . . .              | 44        |
| 5.4.4    | Data Retention and Deletion . . . . . | 44        |
| 5.5      | Access Control . . . . .              | 45        |
| 5.5.1    | Authentication . . . . .              | 45        |
| 5.5.2    | Authorisation . . . . .               | 45        |
| 5.5.3    | Administrative Access . . . . .       | 46        |
| 5.6      | Application Security . . . . .        | 46        |
| 5.6.1    | Secure Development . . . . .          | 46        |
| 5.6.2    | Input Validation . . . . .            | 47        |
| 5.6.3    | API Security . . . . .                | 47        |
| 5.6.4    | Webhook Security . . . . .            | 47        |
| 5.7      | Audit Logging . . . . .               | 47        |
| 5.7.1    | Audit Trail Architecture . . . . .    | 47        |
| 5.7.2    | Logged Events . . . . .               | 47        |
| 5.7.3    | Audit Log Protection . . . . .        | 48        |
| 5.8      | Monitoring and Detection . . . . .    | 48        |
| 5.8.1    | Infrastructure Monitoring . . . . .   | 48        |
| 5.8.2    | Security Monitoring . . . . .         | 49        |
| 5.8.3    | Distributed Tracing . . . . .         | 49        |
| 5.8.4    | Alerting . . . . .                    | 49        |
| 5.9      | Incident Response . . . . .           | 49        |
| 5.9.1    | Incident Classification . . . . .     | 49        |

|          |                                           |           |
|----------|-------------------------------------------|-----------|
| 5.9.2    | Response Process . . . . .                | 49        |
| 5.9.3    | Communication . . . . .                   | 50        |
| 5.10     | Business Continuity . . . . .             | 50        |
| 5.10.1   | Backup Strategy . . . . .                 | 50        |
| 5.10.2   | Disaster Recovery . . . . .               | 50        |
| 5.10.3   | High Availability . . . . .               | 50        |
| 5.11     | Vendor Security . . . . .                 | 51        |
| 5.11.1   | Vendor Assessment . . . . .               | 51        |
| 5.11.2   | Vendor Requirements . . . . .             | 51        |
| 5.11.3   | Ongoing Monitoring . . . . .              | 51        |
| 5.12     | Physical Security . . . . .               | 51        |
| 5.12.1   | Data Centre Security . . . . .            | 51        |
| 5.12.2   | Office Security . . . . .                 | 51        |
| 5.13     | Security Certifications . . . . .         | 52        |
| 5.14     | Security Contact . . . . .                | 52        |
| <b>6</b> | <b>Sub-processor List</b>                 | <b>53</b> |
| 6.1      | Introduction . . . . .                    | 53        |
| 6.2      | Sub-processor Categories . . . . .        | 53        |
| 6.3      | Current Sub-processors . . . . .          | 53        |
| 6.3.1    | Infrastructure and Hosting . . . . .      | 53        |
| 6.3.2    | Meeting Recording . . . . .               | 54        |
| 6.3.3    | Transcription Services . . . . .          | 54        |
| 6.3.4    | AI and Language Services . . . . .        | 54        |
| 6.3.5    | Authentication Services . . . . .         | 55        |
| 6.3.6    | Payment Processing . . . . .              | 55        |
| 6.4      | Sub-processor Updates . . . . .           | 55        |
| 6.4.1    | Notification of Changes . . . . .         | 55        |
| 6.4.2    | Objection Process . . . . .               | 56        |
| 6.5      | Verification . . . . .                    | 56        |
| 6.5.1    | Due Diligence . . . . .                   | 56        |
| 6.5.2    | Contractual Requirements . . . . .        | 56        |
| 6.5.3    | EU Standard Contractual Clauses . . . . . | 56        |
| 6.6      | Contact . . . . .                         | 56        |
| 6.7      | Change History . . . . .                  | 57        |
|          | <b>Document History</b>                   | <b>58</b> |

# Introduction

---

## About This Document

This Trust Centre contains the legal and compliance documentation for Evidia. It is designed to provide transparency about how we handle data, maintain security, and comply with applicable regulations.

## Document Structure

This document includes:

- **Privacy Policy** — How we collect, use, and protect personal data
- **Terms and Conditions** — The legal agreement for using our services
- **Data Processing Agreement** — GDPR-compliant terms for data processing
- **AI Disclosure** — Transparency about our AI systems under the EU AI Act
- **Security Architecture** — Technical and organisational security measures
- **Sub-processor List** — Third parties who process data on our behalf

## Regulatory Framework

Evidia provides an AI-assisted meeting analysis service designed with human oversight as a core principle. We comply with:

- EU AI Act (Regulation 2024/1689) — Transparency and human oversight requirements
- General Data Protection Regulation (GDPR)
- Aligned with ISO/IEC 27001 security controls
- Applicable financial services regulations

## Contact Information

For questions about any document in this Trust Centre:

- **General enquiries:** [contact@evidia.ai](mailto:contact@evidia.ai)
- **Privacy and data protection:** [privacy@evidia.ai](mailto:privacy@evidia.ai)

- **Security:** [security@evidia.ai](mailto:security@evidia.ai)
- **Legal:** [legal@evidia.ai](mailto:legal@evidia.ai)

## Chapter 1

# Privacy Policy

---

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

### 1.1 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.

#### 1.1.1 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](mailto:privacy@evidia.ai)

#### 1.1.2 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](mailto:privacy@evidia.ai)

## 1.2 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>

## 1.3 Personal Data We Collect

### 1.3.1 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

### 1.3.2 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

### 1.3.3 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

### 1.3.4 Communication Data

When you contact us, we may collect:

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

## 1.4 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             |

### 1.4.1 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.

## 1.5 How We Use Personal Data

We use personal data for the following purposes:

### 1.5.1 Service Delivery

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

### 1.5.2 Account Management

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

### 1.5.3 Security and Compliance

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

### 1.5.4 Improvement and Development

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

## 1.6 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:

### 1.6.1 Transparency

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

### 1.6.2 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

### 1.6.3 Accuracy and Quality

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

## 1.7 Data Sharing and Disclosure

### 1.7.1 Within Your Organisation

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

### 1.7.2 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.

### 1.7.3 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

### 1.7.4 No Sale of Data

We do not sell personal data to third parties.

## 1.8 International Data Transfers

### 1.8.1 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).

### 1.8.2 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

## 1.9 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                   |

### 1.9.1 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

## 1.10 Your Rights

Under the GDPR, you have the following rights:

### 1.10.1 Right to Access (Article 15)

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

### 1.10.2 Right to Rectification (Article 16)

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

### 1.10.3 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

### 1.10.4 Right to Restrict Processing (Article 18)

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

### 1.10.5 Right to Data Portability (Article 20)

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

### 1.10.6 Right to Object (Article 21)

You may object to processing based on legitimate interests.

### 1.10.7 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.

### 1.10.8 Exercising Your Rights

To exercise your rights:

1. Email [privacy@evidia.ai](mailto: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).

## 1.11 Data Security

We implement comprehensive security measures:

### 1.11.1 Encryption

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

### 1.11.2 Access Control

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

### 1.11.3 Audit Logging

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

### 1.11.4 Infrastructure Security

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

See Chapter 5 for detailed security information.

## 1.12 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

## 1.13 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](mailto:privacy@evidia.ai).

## 1.14 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

## 1.15 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>

## 1.16 Contact Us

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

- **Email:** [privacy@evidia.ai](mailto:privacy@evidia.ai)
- **Address:** Laan van Chartroise 219  
3552ET Utrecht  
Netherlands

## Chapter 2

# Terms and Conditions

---

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

## 2.1 Definitions

In these Terms and Conditions:

Means a user account created to access the Service. Means these Terms and Conditions, the Privacy Policy, the Data Processing Agreement, and any other policies incorporated by reference. Means individuals authorised by Customer to use the Service under Customer's subscription. Means the organisation or individual that has subscribed to the Service. Means all data, including personal data, that Customer or Authorised Users upload, transmit, or process through the Service. Means the user guides, technical specifications, and other materials provided by Evidia regarding the Service. Means the date on which Customer accepts these Terms or first uses the Service. Means the subscription fees and any additional charges for the Service. Means Customer's order for subscriptions, whether via online signup, written agreement, or other ordering process. Means the Evidia Platform provided by Evidia, including all features, functionality, and associated services. Means Customer's subscription to the Service for a specified term. Means services, software, or content provided by third parties that integrate with or are accessible through the Service. Means TODO COMPANY LEGAL NAME. Means Customer.

## 2.2 Agreement Formation

### 2.2.1 Acceptance of Terms

By accessing or using the Service, you agree to be bound by this Agreement. If you are accepting on behalf of an organisation, you represent that you have authority to bind that organisation.

### 2.2.2 Order of Precedence

In the event of conflict between documents, the following order of precedence applies:

1. Any written agreement signed by both parties
2. The Data Processing Agreement

3. These Terms and Conditions
4. The Privacy Policy
5. Other policies referenced herein

### 2.2.3 Changes to Terms

We may update these Terms from time to time. We will notify you of material changes via email or through the Service. Continued use after changes become effective constitutes acceptance.

## 2.3 Service Description

### 2.3.1 Overview

The Service is an AI-powered meeting analysis and compliance platform designed for financial services professionals, providing:

- Automatic meeting recording and transcription
- AI-powered compliance analysis and scoring
- Meeting summaries and action item extraction
- Conversational AI assistance for meeting queries
- Calendar integration and meeting scheduling
- Audit trail and compliance reporting

### 2.3.2 AI Transparency and Human Oversight

The Service is an AI-assisted documentation and analysis tool designed with human oversight as a core principle. AI outputs are advisory and require human review before action. This approach includes:

- Human oversight for critical AI outputs
- Transparency about AI capabilities and limitations
- Comprehensive audit logging
- Regular accuracy testing and monitoring

For detailed information about our AI systems and EU AI Act compliance, see Chapter 4.

### 2.3.3 Service Availability

We aim to provide the Service with high availability. Specific uptime commitments, if any, are set forth in your Order or a separate service level agreement.

### 2.3.4 Service Changes

We may modify, suspend, or discontinue features of the Service with reasonable notice. We will not materially reduce core functionality during your Subscription term without providing an alternative or refund.

## 2.4 Subscriptions and Fees

### 2.4.1 Subscription Terms

1. Subscriptions are purchased for a specified term (e.g., monthly or annual)
2. Subscriptions automatically renew unless terminated in accordance with these Terms
3. Renewal pricing may change with 30 days' notice

### 2.4.2 Fees and Payment

1. You agree to pay the Fees for your Subscription
2. Fees are billed in advance unless otherwise specified
3. Payment is due within 30 days of invoice
4. We may suspend the Service for non-payment with 10 days' notice
5. Overdue amounts accrue interest at the statutory rate

### 2.4.3 Taxes

Fees are exclusive of taxes unless otherwise stated. You are responsible for all applicable taxes, except for taxes based on our net income.

### 2.4.4 Price Changes

We may increase Fees upon renewal with 60 days' notice. You may terminate before the renewal date if you do not accept the new pricing.

## 2.5 Use of Service

### 2.5.1 Permitted Use

Subject to this Agreement, we grant you a limited, non-exclusive, non-transferable right to:

1. Use the Service for your internal business purposes
2. Permit Authorised Users to access the Service
3. Use the Documentation in connection with the Service

### 2.5.2 Usage Limits

1. Subscriptions are subject to usage limits (e.g., number of users, meetings, storage)
2. Exceeding limits may result in additional charges or service restrictions
3. We will notify you when approaching usage limits

### 2.5.3 Acceptable Use Policy

You agree not to:

1. Use the Service for any unlawful purpose
2. Upload malicious code or attempt to compromise Service security
3. Reverse engineer, decompile, or disassemble the Service
4. Resell or redistribute the Service without authorisation
5. Use the Service to process data of competitors
6. Record meetings without proper consent from all participants
7. Use the Service in a manner that violates applicable laws or regulations

### 2.5.4 Consent Obligations

You are solely responsible for:

1. Obtaining consent from all meeting participants before recording
2. Informing participants of the privacy implications of AI analysis
3. Ensuring your use of the Service complies with applicable data protection laws
4. Maintaining records of consent obtained

### 2.5.5 User Responsibilities

You agree to:

1. Keep account credentials secure
2. Promptly notify us of unauthorised access
3. Ensure Authorised Users comply with this Agreement
4. Use strong passwords and enable multi-factor authentication

## 2.6 Customer Data

### 2.6.1 Ownership

You retain all right, title, and interest in Customer Data. We acquire no rights in Customer Data except as necessary to provide the Service.

### 2.6.2 Processing

We will process Customer Data only:

1. As necessary to provide the Service
2. In accordance with your instructions
3. As required by applicable law

### 2.6.3 Data Security

We will implement appropriate technical and organisational measures to protect Customer Data as described in the Data Processing Agreement and Chapter 5.

### 2.6.4 Data Retention and Deletion

1. We will retain Customer Data during your Subscription
2. Upon termination, you may request export of Customer Data
3. We will delete Customer Data within 90 days of termination, subject to legal retention requirements

Tenant-configured retention periods apply during the active subscription. Upon termination, any remaining data will be deleted within 90 days, regardless of configured retention, unless export is requested or legal requirements apply.

### 2.6.5 Data Residency

All Customer Data is stored and processed within the European Union. We will not transfer Customer Data outside the EEA without your prior written consent.

## 2.7 Intellectual Property

### 2.7.1 Our IP

We retain all right, title, and interest in:

1. The Service and all software, technology, and content therein
2. Our trademarks, trade names, and branding
3. Improvements, enhancements, and derivatives of the Service

### 2.7.2 Feedback

If you provide feedback or suggestions regarding the Service, we may use such feedback without obligation to you.

### 2.7.3 AI-Generated Content

1. AI-generated content (transcripts, summaries, analyses) is provided for informational purposes
2. You retain ownership of your Customer Data and meeting content
3. We may use aggregated, anonymised data to improve our AI models
4. You acknowledge that AI-generated content may contain errors

## 2.8 Confidentiality

### 2.8.1 Definition

“Confidential Information” means information disclosed by one party to the other that is marked confidential or would reasonably be understood as confidential.

### 2.8.2 Obligations

Each party agrees to:

1. Protect Confidential Information with reasonable care
2. Use Confidential Information only for purposes of this Agreement
3. Not disclose Confidential Information to third parties without consent

### 2.8.3 Exceptions

These obligations do not apply to information that:

1. Is or becomes publicly available without breach
2. Was already known to the receiving party
3. Is independently developed
4. Must be disclosed by law (with notice to the other party)

## 2.9 Warranties

### 2.9.1 Our Warranties

We warrant that:

1. The Service will perform substantially as described in the Documentation
2. We will not introduce malicious code into the Service
3. We will process Customer Data in accordance with the Data Processing Agreement

### 2.9.2 Your Warranties

You warrant that:

1. You have the right to upload and process Customer Data through the Service
2. Your use of the Service will not violate applicable laws
3. You will obtain necessary consents from meeting participants

### 2.9.3 Disclaimer

EXCEPT AS EXPRESSLY PROVIDED HEREIN, THE SERVICE IS PROVIDED “AS IS” AND “AS AVAILABLE.” WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

## 2.9.4 AI Limitations

YOU ACKNOWLEDGE THAT:

1. AI-generated content may contain errors or inaccuracies
2. AI should not be the sole basis for legal or compliance decisions
3. Human review is required for critical compliance findings
4. AI capabilities and accuracy may vary over time

## 2.10 Limitation of Liability

### 2.10.1 Exclusion of Consequential Damages

NEITHER PARTY WILL BE LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, INCLUDING LOSS OF PROFITS, DATA, OR BUSINESS OPPORTUNITY.

### 2.10.2 Liability Cap

EACH PARTY'S TOTAL LIABILITY UNDER THIS AGREEMENT IS LIMITED TO THE GREATER OF:

1. The Fees paid or payable in the 12 months preceding the claim
2. **[TODO: Liability cap amount to be determined]**

### 2.10.3 Exceptions

These limitations do not apply to:

1. Breach of confidentiality obligations
2. Your payment obligations
3. Data protection violations caused by our gross negligence or wilful misconduct
4. Liability that cannot be limited by law

## 2.11 Indemnification

### 2.11.1 Our Indemnity

We will indemnify you against claims that the Service infringes any patent, copyright, or trademark, provided you:

1. Notify us promptly of the claim
2. Allow us to control the defence
3. Cooperate reasonably in the defence

If the Service becomes or may become infringing, we may:

1. Modify the Service to make it non-infringing
2. Obtain a licence for continued use
3. Terminate this Agreement and refund prepaid Fees

### **2.11.2 Your Indemnity**

You will indemnify us against claims arising from:

1. Your Customer Data
2. Your breach of this Agreement
3. Your violation of applicable law
4. Alleged infringement by your use of the Service

## **2.12 Term and Termination**

### **2.12.1 Term**

This Agreement begins on the Effective Date and continues until terminated.

### **2.12.2 Termination for Convenience**

Either party may terminate:

1. At the end of a Subscription term with 30 days' notice
2. For annual Subscriptions, with 60 days' notice before renewal

### **2.12.3 Termination for Cause**

Either party may terminate:

1. Upon material breach that is not cured within 30 days' notice
2. Immediately if the other party becomes insolvent or files for bankruptcy

### **2.12.4 Effects of Termination**

Upon termination:

1. Your access to the Service will cease
2. You may request export of Customer Data within 30 days
3. We will delete Customer Data in accordance with Section 5.4
4. Provisions that by nature survive will remain in effect
5. No refund of prepaid Fees for partial periods (unless termination by us for cause)

## 2.13 General Terms

### 2.13.1 Governing Law

This Agreement is governed by Dutch law, without regard to conflict of law principles.

### 2.13.2 Dispute Resolution

Any dispute arising from this Agreement will be submitted to the exclusive jurisdiction of the courts of Amsterdam, Netherlands.

### 2.13.3 Assignment

You may not assign this Agreement without our prior written consent. We may assign to an affiliate or successor in connection with a merger or acquisition.

### 2.13.4 Force Majeure

Neither party is liable for delays or failures due to circumstances beyond reasonable control, including natural disasters, war, terrorism, or government actions.

### 2.13.5 Entire Agreement

This Agreement constitutes the entire agreement between the parties and supersedes all prior agreements and understandings.

### 2.13.6 Severability

If any provision is found unenforceable, the remaining provisions will continue in full force.

### 2.13.7 No Waiver

Failure to enforce any provision does not constitute a waiver.

### 2.13.8 Notices

Notices must be in writing and sent to:

- **To us:** legal@evidia.ai or Laan van Chartroise 219  
3552ET Utrecht  
Netherlands
- **To you:** The email address associated with your account

## 2.14 Contact

For questions about these Terms and Conditions:

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

## Chapter 3

# 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.

### 3.1 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.

### 3.2 Scope and Roles

#### 3.2.1 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

### 3.2.2 Scope

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

### 3.2.3 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.

## 3.3 Details of Processing

### 3.3.1 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.

### 3.3.2 Duration of Processing

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

### 3.3.3 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                 |

### 3.3.4 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

### 3.3.5 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.

### 3.3.6 Categories of Data Subjects

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

## 3.4 Controller Obligations

Controller warrants and undertakes that:

### 3.4.1 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

### 3.4.2 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

### 3.4.3 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

### 3.4.4 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.

## 3.5 Processor Obligations

Processor agrees to:

### 3.5.1 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

### 3.5.2 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

### 3.5.3 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 5 for detailed security information.

### 3.5.4 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

### 3.5.5 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

### 3.5.6 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

### 3.5.7 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

## 3.6 Sub-processors

### 3.6.1 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                              |

### 3.6.2 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

### 3.6.3 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

## 3.7 Data Subject Rights

### 3.7.1 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

### 3.7.2 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.

## 3.8 Security Measures

### 3.8.1 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

### 3.8.2 Organisational Measures

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

### 3.8.3 Security Certifications

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

## 3.9 Personal Data Breaches

### 3.9.1 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.

### 3.9.2 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

### 3.9.3 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

### 3.9.4 Costs

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

## 3.10 International Data Transfers

### 3.10.1 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.

### 3.10.2 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

## 3.11 Audit Rights

### 3.11.1 Information

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

### 3.11.2 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

### 3.11.3 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.

## 3.12 Liability

### 3.12.1 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

### 3.12.2 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

## 3.13 Deletion and Return of Data

### 3.13.1 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)

### 3.13.2 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

### 3.13.3 Certification

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

General Terms

## 3.14 General Terms

### 3.14.1 Amendments

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

### 3.14.2 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

### 3.14.3 Governing Law

This DPA is governed by Dutch law.

### 3.14.4 Contact

- **Privacy Contact:** [privacy@evidia.ai](mailto:privacy@evidia.ai)

Appendix: Standard Contractual Clauses

### 3.15 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]**

## Chapter 4

# AI Disclosure and EU AI Act Compliance

---

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

### 4.1 Introduction

This document provides transparency information about the artificial intelligence systems used in the Evidia Platform (the “Service”).

Evidia uses AI to assist with meeting transcription, summarisation, and compliance analysis. All AI outputs are provided as decision-support tools; they do not constitute automated decision-making and require human review before action.

AI System Classification

### 4.2 AI System Classification

#### 4.2.1 EU AI Act Position

The Service is designed as an **assistive AI tool** with the following characteristics:

- AI outputs are advisory and require human review
- No automated decisions are made without human approval
- Users can override, modify, or reject all AI recommendations
- The system does not profile individuals or make decisions about legal rights

#### 4.2.2 Risk Classification Assessment

Based on the EU AI Act framework, we assess the Service as follows:

| Annex III Category           | Assessment                                                                      |
|------------------------------|---------------------------------------------------------------------------------|
| Critical infrastructure (5a) | Not applicable — the Service does not manage or operate critical infrastructure |
| Employment (4)               | Not applicable — the Service is not used for recruitment decisions              |

| Annex III Category     | Assessment                                                                   |
|------------------------|------------------------------------------------------------------------------|
| Access to services (6) | Not applicable — the Service does not determine access to essential services |
| Creditworthiness (7)   | Not applicable — the Service does not evaluate creditworthiness              |

The Service functions as a documentation and analysis support tool. Final decisions regarding compliance, client advice, or other matters remain with qualified human professionals.

4.2.3 Transparency Obligations

Regardless of classification, we voluntarily apply transparency best practices:

- Clear labelling of AI-generated content
- Disclosure of AI capabilities and limitations
- Human oversight mechanisms
- Audit logging of AI operations

AI Components Overview

4.3 AI Components in the Service

4.3.1 AI Functions

The Service incorporates AI for the following **assistive** functions:

| Function               | Technology           | Purpose                                |
|------------------------|----------------------|----------------------------------------|
| Speech Recognition     | Deepgram, Soniox     | Convert audio to text transcripts      |
| Speaker Diarisation    | Soniox               | Identify speakers in transcripts       |
| Summarisation          | Large Language Model | Generate meeting summaries             |
| Action Item Extraction | Large Language Model | Identify potential action items        |
| Compliance Analysis    | Large Language Model | Flag potential compliance topics       |
| Conversational AI      | Large Language Model | Answer questions about meeting content |

4.3.2 Important Limitations

All AI outputs are advisory only. Users should be aware that:

1. **Transcription accuracy:** May be affected by audio quality, accents, background noise, technical terminology, and overlapping speech.

2. **Analysis accuracy:** AI-generated summaries, action items, and compliance flags may contain errors, omissions, or misinterpretations. They should not be treated as legal or compliance advice.
3. **No legal advice:** The Service does not provide legal advice. Compliance analysis is a support tool to help professionals identify topics that may require review.
4. **Context limitations:** AI may miss contextual nuances, implicit meanings, or domain-specific knowledge that a human would recognise.
5. **Language support:** Primary support for Dutch and English; other languages may have reduced accuracy.

Human Oversight

## 4.4 Human Oversight

### 4.4.1 Design Principles

The Service is designed with human oversight as a core principle:

1. **AI assists, humans decide:** AI outputs support but do not replace professional judgment
2. **Override capability:** Users can modify or reject any AI-generated content
3. **No automated adverse actions:** The system cannot take adverse actions without human approval
4. **Full transparency:** Users can see which content is AI-generated

### 4.4.2 User Responsibilities

Users of the Service are responsible for:

1. Reviewing AI outputs before relying on them
2. Applying professional judgment to compliance analysis
3. Verifying transcripts against source material where accuracy is critical
4. Ensuring that final decisions are appropriate for their context

Transparency

## 4.5 Transparency

### 4.5.1 Labelling

AI-generated content is identified through:

- Visual indicators distinguishing AI-generated from user-created content
- Timestamps showing when content was generated
- Ability to view original source material (transcript or audio)

### 4.5.2 User Notifications

Users are informed about:

1. When AI is being used to process their data
2. The purpose of each AI component
3. Known limitations and potential for errors
4. Their right to human review of AI outputs

Data and Privacy

## 4.6 Data and Privacy

### 4.6.1 Data Use

- Customer data is processed to provide the Service
- Customer data is not used to train AI models
- AI providers are contractually bound not to retain or train on customer data

### 4.6.2 Processing Location

AI processing occurs within the European Union. See Chapter 6 for details on sub-processors.  
Quality and Monitoring

## 4.7 Quality and Monitoring

### 4.7.1 Quality Practices

We maintain AI quality through:

1. Monitoring of user feedback on AI outputs
2. Regular review of error patterns
3. Updates to improve accuracy where feasible
4. Clear user guidance on interpreting AI outputs

### 4.7.2 User Feedback

Users can report AI errors through:

- In-app feedback mechanisms
- Contact with support team

Reported issues are used to improve the Service and, where appropriate, communicated to AI providers.

User Rights

## 4.8 User Rights

### 4.8.1 Right to Human Review

Users can request human review of any AI output by escalating to their organisation administrator or contacting support.

### 4.8.2 Right to Explanation

Upon request, we will provide information about:

1. Which AI components processed their data
2. The general nature of the processing
3. How to interpret AI outputs

### 4.8.3 Right to Contest

Users may contest AI-generated content by:

1. Modifying or rejecting the content within the Service
2. Requesting review by their organisation administrator
3. Contacting support for assistance

Third-Party AI Providers

## 4.9 Third-Party AI Providers

We engage established AI providers subject to:

1. Data processing agreements
2. EU data residency requirements
3. Contractual prohibitions on training on customer data
4. Security and compliance assessments

See Chapter 6 for the current list of sub-processors.  
Contact

## 4.10 Contact

For questions about AI use in the Service:

- **General enquiries:** [contact@evidia.ai](mailto:contact@evidia.ai)
- **Privacy:** [privacy@evidia.ai](mailto:privacy@evidia.ai)

## Chapter 5

# Security Architecture

---

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

Introduction

### 5.1 Introduction

This document describes the technical and organisational security measures implemented by Evidia to protect the Evidia Platform (the “Service”) and customer data.

Security is a foundational principle of our platform design. We implement defence-in-depth strategies, zero-trust principles, and continuous monitoring to protect against threats.

Security Governance

### 5.2 Security Governance

#### 5.2.1 Security Leadership

- Security oversight is provided by senior leadership
- Security responsibilities are defined for all personnel
- Regular security training is mandatory for all staff

#### 5.2.2 Security Policies

We maintain documented policies covering:

1. Information security policy
2. Access control policy
3. Data classification policy
4. Incident response policy
5. Business continuity policy
6. Vendor management policy

### 5.2.3 Compliance Framework

Our security controls align with:

- ISO/IEC 27001 control framework
- EU AI Act security requirements
- GDPR security requirements
- Industry best practices

Infrastructure Security

## 5.3 Infrastructure Security

### 5.3.1 Hosting Environment

| Component          | Details                                       |
|--------------------|-----------------------------------------------|
| Cloud provider     | Hetzner                                       |
| Region             | European Union (EU-only)                      |
| Network isolation  | Virtual private cloud with restricted access  |
| Load balancing     | Application-level load balancing              |
| Container security | Docker containers with minimal attack surface |

### 5.3.2 Network Security

#### Network Architecture

1. Private network with controlled ingress/egress
2. Firewall rules restricting traffic to necessary ports
3. TLS termination at the application layer
4. No direct database access from public networks

#### DDoS Protection

1. Rate limiting on API endpoints
2. Traffic analysis and anomaly detection
3. Graceful degradation under attack

### 5.3.3 Server Hardening

1. Minimal base images with regular security updates
2. Unnecessary services and packages removed
3. Host-based firewalls
4. Regular vulnerability scanning

Data Security

## 5.4 Data Security

### 5.4.1 Data Classification

| Classification | Examples                | Handling                     |
|----------------|-------------------------|------------------------------|
| Confidential   | Audio, transcripts, PII | Encrypted, access-controlled |
| Internal       | Configuration, logs     | Access-controlled            |
| Public         | Marketing content       | Standard handling            |

### 5.4.2 Encryption

#### Encryption at Rest

- **Algorithm:** AES-256
- **Scope:** All stored data including databases, object storage, and backups
- **Key management:** Secure key storage with regular rotation

#### Encryption in Transit

- **Protocol:** TLS 1.3
- **Scope:** All network communications
- **Certificate management:** Automated certificate renewal

#### Secrets Management

- **Approach:** Self-hosted secrets management infrastructure
- **Scope:** API keys, database credentials, encryption keys
- **Practices:** Secrets never logged, rotated regularly, least-privilege access

### 5.4.3 Data Residency

- All customer data is stored and processed within the European Union
- No cross-border data transfers without explicit consent
- Sub-processors verified for EU data residency

### 5.4.4 Data Retention and Deletion

| Data Type        | Retention           | Deletion Method                     |
|------------------|---------------------|-------------------------------------|
| Audio recordings | Tenant-configurable | Secure deletion from object storage |
| Transcripts      | Tenant-configurable | Database record deletion            |

| Data Type       | Retention                                                            | Deletion Method             |
|-----------------|----------------------------------------------------------------------|-----------------------------|
| Consent records | Tenant-configurable, subject to applicable legal requirements        | Database record deletion    |
| Audit logs      | Tenant-configurable, subject to security and compliance requirements | Anonymisation then deletion |
| Account data    | Until request                                                        | Full account deletion       |

Access Control

## 5.5 Access Control

### 5.5.1 Authentication

#### User Authentication

- **Method:** OpenID Connect (OIDC)
- **Providers:** OpenID Connect (Google, Microsoft 365)
- **MFA:** Multi-factor authentication available and recommended
- **Session management:** Secure session tokens with automatic expiration

#### Service Authentication

- Internal service-to-service authentication
- API key rotation for external integrations
- Mutual TLS for sensitive internal communications

### 5.5.2 Authorisation

#### Role-Based Access Control (RBAC)

| Role   | Permissions                                            |
|--------|--------------------------------------------------------|
| Owner  | Full organisation management, billing, user management |
| Admin  | User management, settings, integrations                |
| Member | Meeting access, analysis review                        |
| Viewer | Read-only access to assigned meetings                  |

## Row-Level Security (RLS)

We implement database-level row-level security for multi-tenant isolation:

1. All tenant-scoped tables have RLS enabled
2. RLS policies enforce `app.current_tenant_id` filtering
3. Session-scoped database context prevents cross-tenant access
4. Defence-in-depth: application queries also include explicit tenant filters

## Principle of Least Privilege

1. Users granted minimum permissions necessary
2. Regular access reviews and certification
3. Time-limited elevated access where required

### 5.5.3 Administrative Access

1. Separate administrative accounts
2. MFA required for all administrative access
3. All administrative actions logged
4. Break-glass procedures for emergency access

Application Security

## 5.6 Application Security

### 5.6.1 Secure Development

#### Development Practices

1. Secure coding guidelines and training
2. Code review required for all changes
3. Automated security scanning in CI/CD pipeline
4. Dependency vulnerability monitoring

#### Security Testing

1. Static application security testing (SAST)
2. Dynamic application security testing (DAST)
3. Dependency vulnerability scanning
4. Periodic penetration testing

### 5.6.2 Input Validation

1. All user input validated and sanitised
2. Parameterised queries prevent SQL injection
3. Output encoding prevents XSS attacks
4. File upload validation and scanning

### 5.6.3 API Security

1. Rate limiting on all endpoints
2. Authentication required for protected endpoints
3. Input validation on all parameters
4. CORS policies restrict cross-origin requests
5. Content Security Policy (CSP) headers

### 5.6.4 Webhook Security

1. HMAC-SHA256 signature verification
2. Timestamp validation to prevent replay attacks
3. Idempotency keys for deduplication
4. Secure endpoint URLs

Audit Logging

## 5.7 Audit Logging

### 5.7.1 Audit Trail Architecture

We maintain comprehensive audit logging with integrity measures:

1. **Event chaining:** Audit events are linked to enable integrity verification
2. **Comprehensive coverage:** Security-relevant events are logged
3. **Append-only storage:** Audit logs cannot be modified after creation

### 5.7.2 Logged Events

#### Authentication Events

- Login success/failure
- Logout
- Session creation/revocation
- MFA enrolment/removal

**Authorisation Events**

- Role grants/revocations
- Permission changes
- API key creation/rotation/revocation
- Policy changes

**Data Access Events**

- Transcript viewed
- Audio downloaded
- Report exported
- Data exports

**AI System Events**

- AI inference requested/completed
- Human approval granted/denied
- AI output overridden
- Quality issues reported

**Administrative Events**

- Configuration changes
- Integration setup/modification
- Security setting changes

**5.7.3 Audit Log Protection**

1. Logs stored separately from application data
2. Access restricted to authorised personnel
3. Log access itself is audited
4. Retained for Tenant-configurable, subject to security and compliance requirements

Monitoring and Detection

**5.8 Monitoring and Detection****5.8.1 Infrastructure Monitoring**

1. Real-time metrics collection
2. Resource utilisation monitoring
3. Automated alerting for anomalies
4. Centralised log aggregation

### 5.8.2 Security Monitoring

1. Failed authentication attempt monitoring
2. Unusual access pattern detection
3. Privilege escalation monitoring
4. Data exfiltration detection

### 5.8.3 Distributed Tracing

1. OpenTelemetry-based distributed tracing
2. Request correlation across services
3. Performance monitoring
4. Error tracking and alerting

### 5.8.4 Alerting

1. 24/7 monitoring and alerting
2. Severity-based escalation procedures
3. On-call rotation for critical alerts
4. Regular alert review and tuning

Incident Response

## 5.9 Incident Response

### 5.9.1 Incident Classification

| Severity | Examples                        | Response Time |
|----------|---------------------------------|---------------|
| Critical | Data breach, system compromise  | Immediate     |
| High     | Security vulnerability, outage  | 1 hour        |
| Medium   | Performance degradation, errors | 4 hours       |
| Low      | Minor issues, cosmetic bugs     | 24 hours      |

### 5.9.2 Response Process

1. **Detection:** Automated monitoring or user report
2. **Triage:** Severity assessment and team notification
3. **Containment:** Isolate affected systems

4. **Eradication:** Remove threat and patch vulnerabilities
5. **Recovery:** Restore services and verify integrity
6. **Post-incident:** Root cause analysis and documentation

### 5.9.3 Communication

1. Internal stakeholders notified per severity
2. Affected customers notified without undue delay
3. Regulatory notification within 72 hours where required
4. Post-incident report provided to affected parties

Business Continuity

## 5.10 Business Continuity

### 5.10.1 Backup Strategy

1. Regular automated backups of all data
2. Encrypted backup storage
3. Off-site backup replication
4. Regular backup restoration testing

### 5.10.2 Disaster Recovery

1. Documented disaster recovery procedures
2. Recovery time objective (RTO): **[TODO: RTO]**
3. Recovery point objective (RPO): **[TODO: RPO]**
4. Regular disaster recovery testing

### 5.10.3 High Availability

1. Redundant infrastructure components
2. Automatic failover for critical services
3. Load balancing across multiple instances
4. Geographic redundancy where applicable

Vendor Security

## 5.11 Vendor Security

### 5.11.1 Vendor Assessment

Before engaging vendors, we assess:

1. Security certifications and practices
2. Data processing locations
3. Compliance with relevant regulations
4. Incident response capabilities

### 5.11.2 Vendor Requirements

All vendors processing customer data must:

1. Sign data processing agreements
2. Maintain appropriate security controls
3. Process data only within the EU
4. Notify us of security incidents

### 5.11.3 Ongoing Monitoring

1. Regular vendor security reviews
2. Monitoring of vendor security announcements
3. Contractual right to audit

Physical Security

## 5.12 Physical Security

### 5.12.1 Data Centre Security

Our cloud provider (Hetzner) maintains physical security including:

1. 24/7 security personnel and surveillance
2. Biometric access controls
3. Environmental controls (fire, flood, temperature)
4. Uninterruptible power supply and generators

### 5.12.2 Office Security

1. Physical access controls
2. Clean desk policy
3. Secure disposal of physical media

Security Certifications

## 5.13 Security Certifications

[**TODO: List current security certifications, e.g.:**]

- ISO/IEC 27001:2013 (planned)
- SOC 2 Type II (planned)

Contact

## 5.14 Security Contact

For security concerns or to report a vulnerability:

- **Security team:** security@evidia.ai
- **Responsible disclosure:** We appreciate responsible disclosure of security vulnerabilities

## Chapter 6

# Sub-processor List

---

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

Introduction

### 6.1 Introduction

This document lists the sub-processors that Evidia (“**we**”, “**us**”) engages to process personal data on behalf of our customers in connection with the Evidia Platform (the “Service”).

By using the Service, you authorise us to engage these sub-processors as described in the Data Processing Agreement (Chapter 3).

Sub-processor Categories

### 6.2 Sub-processor Categories

We engage sub-processors in the following categories:

1. **Infrastructure providers** — Cloud computing, hosting, and storage
2. **Meeting recording providers** — Bot services for meeting recording
3. **Transcription providers** — Speech-to-text services
4. **AI providers** — Large language model and AI services
5. **Payment providers** — Billing and payment processing

Current Sub-processors

### 6.3 Current Sub-processors

#### 6.3.1 Infrastructure and Hosting

| Provider | Purpose                   | Location | DPA |
|----------|---------------------------|----------|-----|
| Hetzner  | Cloud infrastruc-<br>ture | EU       | Yes |

| Provider      | Purpose           | Location | DPA               |
|---------------|-------------------|----------|-------------------|
| PostgreSQL    | Database services | EU       | N/A (self-hosted) |
| S3-compatible | Object storage    | EU       | N/A (self-hosted) |

### 6.3.2 Meeting Recording

| Provider       | Purpose                    | Location | DPA |
|----------------|----------------------------|----------|-----|
| Recall.ai Inc. | Meeting bot, calendar sync | EU       | Yes |

**Data processed:**

- Meeting audio and video
- Calendar information
- Meeting metadata (participants, duration)

**Retention:** Audio deleted after processing; metadata retained per agreement.

### 6.3.3 Transcription Services

| Provider       | Purpose                     | Location | DPA |
|----------------|-----------------------------|----------|-----|
| Deepgram, Inc. | Speech-to-text              | EU       | Yes |
| Soniox d.o.o.  | Speech-to-text, diarisation | EU       | Yes |

**Data processed:**

- Audio recordings for transcription
- Voice data for speaker identification

**Retention:** Audio deleted immediately after transcription; no training on customer data.

### 6.3.4 AI and Language Services

| Provider          | Purpose                          | Location | DPA |
|-------------------|----------------------------------|----------|-----|
| Scaleway SAS      | AI analysis, summarisation (LLM) | EU       | Yes |
| OpenAI (optional) | Embeddings for help search       | EU/US    | Yes |

**Data processed:**

- Meeting transcripts for analysis

- Generated text for summaries and compliance analysis
- Help content for semantic search (OpenAI only)

**Retention:** Transcripts not retained by provider; no training on customer data.

### 6.3.5 Authentication Services

| Provider        | Purpose             | Location | DPA |
|-----------------|---------------------|----------|-----|
| Google LLC      | OpenID Connect auth | Global   | N/A |
| Microsoft Corp. | OpenID Connect auth | Global   | N/A |

**Data processed:**

- Authentication tokens
- Basic profile information (name, email)

**Note:** These are data controllers for their own services. We only receive authentication assertions.

### 6.3.6 Payment Processing

| Provider     | Purpose            | Location | DPA |
|--------------|--------------------|----------|-----|
| Stripe, Inc. | Payment processing | EU       | Yes |

**Data processed:**

- Billing information
- Payment card data (tokenised)

Sub-processor Updates

## 6.4 Sub-processor Updates

### 6.4.1 Notification of Changes

We will notify customers of additions or replacements to this list at least 30 days before the change takes effect. Notifications will be sent to the email address associated with your account.

### 6.4.2 Objection Process

If you object to a new or replacement sub-processor on reasonable data protection grounds:

1. Contact us at [privacy@evidia.ai](mailto:privacy@evidia.ai) within 15 days of receiving notification
2. Provide specific reasons for your objection
3. We will work with you to address concerns
4. If concerns cannot be resolved, you may terminate the affected services

Verification

## 6.5 Verification

### 6.5.1 Due Diligence

We conduct due diligence on all sub-processors including:

1. Security practices and certifications
2. Data protection compliance
3. Data residency verification
4. Contractual protections

### 6.5.2 Contractual Requirements

All sub-processors are bound by agreements requiring:

1. Processing only on our instructions
2. Confidentiality obligations
3. Appropriate security measures
4. Assistance with data subject requests
5. Notification of data breaches
6. Audit rights
7. Deletion of data upon termination

### 6.5.3 EU Standard Contractual Clauses

For sub-processors established outside the EEA (if any), we ensure EU Standard Contractual Clauses or equivalent safeguards are in place.

Contact

## 6.6 Contact

For questions about sub-processors:

- **Email:** [privacy@evidia.ai](mailto:privacy@evidia.ai)

Change History

## 6.7 Change History

| Date       | Change       | Details                                 |
|------------|--------------|-----------------------------------------|
| 2026-07-07 | Initial list | First publication of sub-processor list |

# Document History

---

| Version | Date       | Description     |
|---------|------------|-----------------|
| 1.0.0   | 2026-07-07 | Initial release |

*End of Trust Centre Documentation*