DATA PROCESSING AGREEMENT (DPA)

This Data Processing Agreement ("Agreement") forms part of the Service Agreement between:

Customer ("Controller")

and

Ideus d.o.o. ("Processor")

regarding the processing of personal data within the DEIK Strategic Negotiation Simulator.

---

1. Subject Matter

This Agreement governs the processing of personal data by Ideus on behalf of the Customer when providing the Platform.

---

2. Roles of the Parties

Customer acts as the **Data Controller**.

Ideus acts as the **Data Processor**.

Ideus processes personal data only according to documented instructions from the Customer.

---

3. Categories of Data Processed

The Platform may process the following categories of data:

- user account information
- simulation input data
- voice input streams
- behavioral performance metrics
- system usage logs

---

4. Categories of Data Subjects

Data subjects may include:

- employees
- consultants
- trainees
- authorized users of the Platform

---

5. Purpose of Processing

Data is processed solely for the purpose of:

- providing the negotiation simulator
- generating performance feedback
- maintaining system security and reliability

---

6. Processor Obligations

Ideus agrees to:

- process personal data only on documented instructions
- ensure confidentiality of personnel
- implement appropriate technical and organizational security measures
- assist the Controller in fulfilling GDPR obligations
- notify the Controller of data breaches without undue delay

---

7. Security Measures

Ideus maintains security measures including:

- encryption of data in transit and at rest
- logical tenant isolation
- role-based access control
- regular security audits
- vulnerability management processes

---

8. Subprocessors

Ideus may engage subprocessors to support service delivery, including:

- cloud infrastructure providers
- security monitoring services

All subprocessors are bound by equivalent data protection obligations.

Customers will be informed of material changes to subprocessors.

---

9. International Transfers

Where subprocessors process data outside the EEA, Ideus ensures:

- Standard Contractual Clauses
- appropriate security safeguards

---

10. Data Breach Notification

Ideus shall notify the Controller without undue delay after becoming aware of a personal data breach.

---

11. Data Subject Rights

Ideus will assist the Controller in responding to requests from data subjects exercising their GDPR rights.

---

12. Data Deletion

Upon termination of services, Ideus shall:

- delete personal data, or
- return personal data to the Controller

unless retention is required by law.

13. Audits

Upon reasonable request, the Controller may request documentation demonstrating Ideus's compliance with this Agreement.

Independent certifications and security reports may satisfy this requirement.

ANNEX I: DETAILS OF PROCESSING

1. Subject Matter and Duration: Provision of the DEIK Strategic Negotiation Simulator services for the duration of the Service Agreement.

2. Nature and Purpose: Processing personal data to provide simulated negotiation scenarios and generate training feedback.

3. Categories of Data Subjects: Employees, contractors, and authorized users of the Controller.

4. Categories of Personal Data: Name, email, job title, chat transcripts, negotiation inputs, and (optional) communication metrics.

ANNEX II: TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

1. Confidentiality: Data is hosted in AWS/Google Cloud (EU Region) with strict physical and system access controls (MFA, RBAC). All data is encrypted using TLS 1.3 (transfer) and AES-256 (at rest).

2. Integrity: Use of encrypted connections and audit logs to prevent and detect unauthorized data modification.

3. Availability & Resilience: Daily backups with Point-in-Time Recovery (PITR) and high-availability architecture to prevent service interruptions.

4. Testing & Assessment: Automated vulnerability scanning (CI/CD) and annual external penetration testing.

5. AI Safeguards: "Zero Retention" API policy with LLM providers (No Training clause) and data anonymization where feasible.

6. Ephemeral Audio Processing: Implementation of a volatile memory processing pipeline for voice data. Raw audio files are held only in temporary cache during inference and are automatically purged upon completion of the metric extraction, ensuring no biometric raw data persists at rest.

ANNEX III: LIST OF SUBPROCESSORS

Provider	Purpose	Data Location
AWS / Google Cloud	Infrastructure & Database	EU (Frankfurt / Ireland)
OpenAI / Anthropic	LLM Processing (via API)	EU / US (No-Training)
Cloudflare	DNS, WAF & Security	Global (Edge)
SendGrid	Transactional Emails	US / EU