# DEIK GLOBAL PRIVACY POLICY

**Last updated:** 17 March 2026

This Global Privacy Policy explains how **Ideus d.o.o.** processes personal data when users access and use the **DEIK Strategic Negotiation Simulator**.

This policy is designed to comply with major global privacy regulations including:

- GDPR (EU / EEA)
- CCPA / CPRA (California, USA)
- PDPA (Singapore)
- APPI (Japan)
- PIPA (South Korea)
- DPDP Act (India)
- Data Privacy Act (Philippines)

---

# 1. Data Controller

Ideus d.o.o.
Teslova 30
Slovenia

Email:
privacy@deik.ai

---

# 2. Categories of Personal Data

The platform may process the following data:

## Account Information

- name
- email address
- organization
- login credentials

## Simulation Data

- text responses
- negotiation inputs
- scenario interactions

## Voice Data (Optional)

- voice tone analysis
- speech timing indicators

Voice analysis is optional and activated only when enabled by the user.

---

## Behavioral Metrics

The platform may analyze:

- response timing
- negotiation patterns
- interaction dynamics

These metrics are used solely to generate training feedback.

---

### Technical Data

- IP address
- device information
- browser type
- session logs

**Voice Data & Biometric Processing:** If the User chooses to enable voice-based interaction, the Platform processes voice audio solely to derive communication metrics (e.g., tone, timing, stability). DEIK operates on a **"Zero-Storage"** principle for raw audio: all voice recordings are processed in real-time and are immediately and permanently deleted following the extraction of non-identifiable metrics. No raw voice recordings are stored on our servers or used for model training.

---

# 3. Purpose of Processing

Personal data is processed for the following purposes:

- providing the negotiation simulation platform
- generating performance feedback
- maintaining system security
- improving platform stability
- preventing misuse or security threats

**Important Notice on Employee Use:** The Platform is provided strictly for professional training and developmental purposes. The metrics and insights generated by the AI are intended to support the user's cognitive growth and are **not** designed, intended, or authorized

to be used as the sole basis for high-stakes HR decisions, such as performance reviews, promotions, or termination of employment.

---

# 4. Legal Basis (GDPR)

Processing is based on:

**Contractual necessity**

providing the platform services.

**Legitimate interest**

ensuring platform security and reliability.

**Consent**

for optional features such as voice analysis.

Users may withdraw consent at any time.

---

# 5. Artificial Intelligence Processing

The platform uses artificial intelligence to:

- simulate negotiation dialogue
- analyze interaction patterns
- generate training feedback

The system:

- does not make automated legal or financial decisions
- does not evaluate employment outcomes
- does not replace human judgment

AI-generated outputs are informational and intended for training purposes.

---

# 6. Data Retention

Data is retained only 12 months for analytics of trainings.

Typical retention periods:

| Data type | Retention |
|---|---|
| Account data | while account is active |
| Simulation metrics | up to 12 months |
| System logs | up to 90 days |
| Voice data | processed transiently |

Enterprise customers may configure custom retention policies.

---

# 7. Data Sharing

We may share data with trusted service providers for:

- infrastructure hosting
- security monitoring
- analytics services

All subprocessors operate under contractual data protection obligations.

We do **not sell personal data**.

---

# 8. International Data Transfers

Data may be transferred outside the European Economic Area when necessary to operate the platform.

Safeguards include:

- Standard Contractual Clauses
- equivalent security protections
- contractual obligations for processors

---

# 9. Security Measures

The platform uses industry-standard security controls including:

- TLS 1.3 encryption in transit
- AES-256 encryption at rest
- role-based access control
- tenant isolation
- infrastructure monitoring

---

# 10. Data Subject Rights

Users may request:

- access to personal data

- correction of inaccurate data
- deletion of personal data
- restriction of processing
- objection to processing
- data portability

Requests may be sent to:

privacy@deik.ai

---

# 11. Regional Privacy Rights

## European Union (GDPR)

Users in the EU have rights under the General Data Protection Regulation including:

- right to access
- right to erasure
- right to data portability

---

## United States (CCPA / CPRA)

California residents may have rights to:

- request disclosure of collected data
- request deletion of personal information

- opt out of sale of personal data

DEIK does **not sell personal data**.

Requests may be submitted via privacy@deik.ai.

---

## Asia-Pacific

Users in Asia-Pacific jurisdictions may have rights under local privacy regulations including:

- PDPA (Singapore)
- APPI (Japan)
- PIPA (South Korea)
- DPDP Act (India)

Users may request access, correction, or deletion of personal data.

---

# 12. China Safe Clause (PIPL)

The platform is not currently designed to host or process personal data subject to Chinese data localization requirements.

Organizations located in China should contact Ideus d.o.o. before deploying the platform to ensure compliance with applicable Chinese regulations.

---

# 13. Children's Data

The platform is not intended for users under 18 years of age.

---

# 14. Updates to this Policy

We may update this policy periodically.

Material changes will be communicated via the platform or email notification.