AI RISK ASSESSMENT

(DEIK Strategic Negotiation Simulator)

Version: 1.0
Last Updated: [DATE]

---

1. Purpose of This Assessment

This document evaluates potential risks associated with the artificial intelligence systems used within the **DEIK Strategic Negotiation Simulator**.

The purpose of this assessment is to:

• identify potential risks arising from AI usage
• evaluate the likelihood and impact of those risks
• describe safeguards implemented to mitigate them
• align internal governance with the EU Artificial Intelligence Act

This assessment supports Ideus d.o.o. commitment to responsible AI deployment.

---

2. Description of the AI System

The DEIK Strategic Negotiation Simulator is an AI-assisted training platform designed to simulate negotiation scenarios and provide performance feedback.

The AI system performs the following functions:

• generation of simulated negotiation dialogue
• analysis of negotiation interaction patterns
• generation of training feedback
• optional analysis of voice interaction patterns

The system operates as an **interactive training environment** and does not autonomously execute real-world actions.

---

3. Intended Use

The platform is intended for:

• negotiation training
• professional development
• coaching environments
• internal corporate training programs

The system is not designed for:

• automated decision-making in business transactions
• legal advice
• financial decision automation
• personnel evaluation or hiring decisions

---

4. AI Risk Classification

Based on the current framework of the EU Artificial Intelligence Act, the DEIK Strategic Negotiation Simulator is expected to fall within the category of:

Limited Risk AI Systems

Reasons include:

• the system provides simulated training scenarios
• it does not determine access to employment, credit, or public services
• it does not perform biometric identification
• it does not autonomously execute decisions with legal consequences

Users are informed when interacting with AI-generated content, which satisfies transparency requirements.

---

5. Risk Identification

The following categories of risk were evaluated.

5.1 Data Privacy Risk

AI systems process user inputs which may include business information or communication patterns.

Potential risks include:

• unintended exposure of sensitive negotiation information
• improper handling of voice interaction data
• unauthorized access to simulation transcripts

5.2 Confidential Business Information Risk

Negotiation simulations may contain sensitive commercial strategies such as:

• pricing structures
• negotiation tactics
• business positioning

Exposure of this information could harm organizations.

5.3 AI Output Reliability Risk

AI-generated responses may:

• contain inaccuracies
• simplify complex negotiation dynamics
• fail to fully represent real-world negotiation behavior

Users may misinterpret simulation results if used outside their intended context.

5.4 Bias Risk

AI-generated responses could potentially reflect unintended patterns or biases originating from training data.

While negotiation simulations are not designed to evaluate individuals, bias in responses could affect the perceived realism of training scenarios.

5.5 Security Risk

AI systems processing user interaction data could become a target for unauthorized access attempts.

Risks include:

• unauthorized system access
• data exfiltration attempts
• infrastructure vulnerabilities

---

6. Risk Mitigation Measures

Ideus d.o.o. implements several safeguards to mitigate identified risks.

6.1 Privacy Safeguards

Privacy protections include:

• data minimization
• encryption of data in transit and at rest
• controlled access to production systems
• tenant isolation between organizations

Where possible, audio inputs are processed in real time and not permanently stored.

6.2 Data Isolation

Customer data remains isolated within tenant environments.

The platform enforces logical separation between organizations to ensure that:

• customer simulation data cannot be accessed by other organizations
• training interactions remain confidential

6.3 AI Model Data Policy

Customer simulation data is not used to train global AI models.

Negotiation strategies, transcripts, and voice interactions remain confined to the customer environment.

This safeguard prevents sensitive business knowledge from influencing shared AI systems.

6.4 Human Oversight

AI outputs are designed to support training rather than replace human decision-making.

Users maintain full responsibility for interpreting training results.

The system does not make automated decisions with legal or business consequences.

6.5 Security Controls

Technical safeguards include:

• encryption standards (TLS 1.3, AES-256)
• access control policies
• security monitoring and logging
• incident response procedures

These controls reduce the likelihood of unauthorized access.

---

7. Transparency Measures

To ensure transparency, Ideus d.o.o. provides the following documentation:

• Privacy Policy
• AI Processing Disclosure
• AI Model Transparency Sheet
• Security & Data Sovereignty documentation

Users interacting with the platform are informed that they are interacting with AI-generated simulations.

---

8. Residual Risk Assessment

After applying the safeguards described above, residual risk is assessed as:

Low to Moderate Risk

Primary residual risks relate to:

• user misinterpretation of simulation outputs
• potential exposure of confidential business content if users voluntarily input such data

These risks are mitigated through transparency, access controls, and data isolation mechanisms.

---

9. Monitoring and Review

Ideus d.o.o. periodically reviews AI system risks through:

• internal governance reviews
• updates to system architecture
• monitoring of emerging regulatory guidance

This risk assessment may be updated as regulatory frameworks evolve.

---

10. Governance

AI governance within Ideus d.o.o. is guided by the following principles:

• responsible AI deployment
• privacy protection
• transparency of AI behavior
• security of customer data

These principles support safe and trustworthy use of AI technology.

---

11. Contact

Questions regarding AI risk governance may be directed to:

ai-governance@deik.pro