DEIK ENTERPRISE SECURITY & DATA SOVEREIGNTY WHITEPAPER

Version: 1.0
Last Updated: 17th of March, 2026

---

1. Introduction

This document describes the security architecture, data protection practices, and data sovereignty principles implemented within the **DEIK Strategic Negotiation Simulator** (the "Platform").

The platform is designed for organizations that require a secure environment for training strategic negotiation capabilities using artificial intelligence.

Given the sensitive nature of negotiation simulations—which may include pricing strategies, commercial positioning, and negotiation tactics—DEIK has implemented security practices aligned with modern enterprise SaaS standards.

The security framework of the platform is based on the following principles:

• Security by Design
• Privacy by Design
• Data Minimization
• Tenant Isolation
• Confidentiality of Strategic Data

This whitepaper provides transparency into the technical and operational safeguards that protect customer data.

---

2. Platform Overview

The DEIK Strategic Negotiation Simulator is an AI-assisted training environment that allows users to practice negotiation scenarios through interactive simulations.

The platform includes the following core components:

• Scenario simulation engine
• AI response generation systems
• Voice interaction analysis
• Behavioral performance analytics
• User management and enterprise administration

The system may process various forms of data during simulations including:

• textual responses
• voice input streams
• behavioral timing data
• performance metrics

The platform is intended solely for training and performance analysis purposes.

---

3. Security Architecture

The platform is built using a layered security architecture designed to protect data at every stage of processing.

The architecture consists of the following layers:

Infrastructure Layer

Secure cloud infrastructure provides:

• network segmentation
• firewall protection
• distributed availability
• automated scaling
• DDoS mitigation

Application Layer

Application-level protections include:

• authentication controls
• access control enforcement
• API protection
• request validation

Data Protection Layer

Data security mechanisms include:

• encryption of data in transit and at rest
• secure storage services
• controlled database access
• internal audit logging

Monitoring Layer

Continuous monitoring systems detect:

• anomalous traffic patterns
• potential intrusion attempts
• unauthorized access attempts
• infrastructure instability

This layered architecture ensures that multiple independent safeguards protect the platform.

---

4. Encryption and Data Protection

All sensitive data handled by the platform is protected through modern cryptographic standards.

Encryption in Transit

All network communications between users and the platform are encrypted using:

TLS 1.3

This ensures that data transmitted across public networks cannot be intercepted or modified.

Encryption at Rest

Stored data is protected using:

AES-256 encryption

This applies to:

• databases
• storage systems
• backups

Encryption keys are managed using secure key management systems with strict access controls.

---

5. Tenant Isolation

Enterprise customers operate within logically isolated environments.

Tenant isolation ensures that:

• customer data is separated at the application layer
• database access is restricted per tenant
• user permissions are scoped to their organization

This architecture prevents data from one organization from being visible to another organization.

Isolation mechanisms include:

• tenant-scoped database queries
• tenant access identifiers
• permission-based data access

This approach ensures strong separation between enterprise customers.

---

6. AI Model Data Policy

The DEIK platform includes artificial intelligence systems that generate simulation responses and analyze negotiation behavior.

To protect customer confidentiality, the following policy applies:

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

Customer data remains confined to:

• the customer tenant environment
• simulation session analysis systems

Simulation content—including negotiation strategies, pricing information, and business scenarios—remains private to the customer organization.

This policy ensures that strategic negotiation insights are not incorporated into shared models.

---

7. Voice Data Processing

The platform may analyze voice input during negotiation simulations in order to provide feedback on communication patterns and stress indicators.

Voice processing is designed according to data minimization principles.

Where possible:

• voice input is processed in real time
• raw audio is not permanently stored
• only derived behavioral indicators are retained

Examples of derived indicators include:

• speech stability metrics
• response timing patterns
• vocal intensity indicators

Enterprise customers may configure retention policies for simulation data.

---

8. Access Control

Access to the platform and internal systems is restricted through multiple control mechanisms.

Authentication

User access requires authenticated accounts.

Security controls include:

• strong password policies
• optional multi-factor authentication
• session management controls

Role-Based Access Control (RBAC)

Users are assigned roles that determine the level of access to platform features.

Roles may include:

• standard users
• training administrators
• enterprise administrators

Access privileges are granted according to the principle of **least privilege**.

Internal Access Controls

Access to production infrastructure is limited to authorized personnel and is monitored through audit logging.

---

9. Monitoring and Logging

Security monitoring systems continuously analyze system activity in order to detect anomalies or potential threats.

Monitoring capabilities include:

• infrastructure health monitoring
• authentication event tracking
• suspicious activity detection
• log aggregation and analysis

Audit logs may include:

• login activity
• administrative actions
• system access events

Logs are retained for a limited period for security analysis and incident investigation.

---

10. Incident Response

DEIK maintains internal procedures for responding to security incidents.

The incident response process includes the following stages:

1. Detection
2. Investigation
3. Containment
4. Remediation
5. Notification (when required)

In the event of a confirmed data breach involving personal data, DEIK will follow applicable legal requirements regarding notification.

---

11. Infrastructure Security Standards

The platform is hosted on secure cloud infrastructure providers that maintain industry-recognized security certifications such as:

• ISO 27001
• SOC 2 Type II (or equivalent)

These standards require strict operational controls including:

• physical data center security
• access monitoring
• redundancy and disaster recovery procedures

Using certified infrastructure helps ensure strong baseline security practices.

---

12. Data Retention

DEIK follows the principle of retaining data only for as long as necessary.

Typical retention guidelines include:

Account data
Retained while the account is active.

Simulation metrics
Retained for performance analytics and training history.

System logs
Retained for security monitoring purposes for a limited period.

Audio streams
Processed transiently unless explicit storage is enabled.

Enterprise customers may configure custom retention policies depending on their organizational requirements.

---

13. Data Sovereignty

Organizations using the DEIK platform retain control over their negotiation simulation data.

DEIK does not claim ownership over customer simulation inputs or outputs.

Customer data remains:

• isolated within the platform environment
• protected through encryption
• accessible only to authorized users

The platform is designed so that strategic negotiation knowledge remains under the control of the organization that generated it.

14. Continuous Security Improvement

Security is an ongoing process.

DEIK regularly reviews and improves its security practices through:

• infrastructure updates
• vulnerability monitoring
• internal security reviews
• updates to platform architecture

Our objective is to maintain a secure environment that organizations can trust when training sensitive strategic capabilities.

---

15. Contact

Security questions or vulnerability reports may be directed to:

security@deik.pro

DEIK encourages responsible disclosure of security issues so they can be addressed promptly.