datarails

# AI Security and Compliance

## Overview

At Datarails, we are committed to maintaining the highest standards of data security and regulatory compliance. Our AI tools, powered by OpenAI's GPT models, are integrated with Azure to provide industry-leading security measures. By deploying models within specific regional data centers in the US, UK, and Canada, we ensure compliance with local regulations and data residency requirements.

## Data Privacy and Security

**Regional Deployment:**
Our AI models are deployed in the same regions (US, UK, Canada) as your data, ensuring compliance with local data privacy laws, including adherence to GDPR.

**Azure Security Framework:**
Leveraging Azure's robust security protocols, including encryption at rest and in transit, network security groups, and access control policies.

**No Data Retention by AI Models:**
AI models do not retain any customer data. Every query or transaction is processed securely, and no customer information is stored or reused.

## Security Measures

**SOC 2 Certification:**
Datarails holds SOC 2 certification, ensuring we meet rigorous security and privacy standards for handling customer data.

**GDPR Compliance:**
We adhere to the GDPR standards, ensuring personal data is handled securely and transparently.

**Encryption:**
All data processed through our AI platform is encrypted using industry-standard AES-256 encryption.

**Role-Based Access Controls (RBAC):**
Access to sensitive data is controlled through strict identity and access management policies.

**Data Isolation:**
Customer data is isolated within secure environments to prevent unauthorized access or cross-tenant data sharing.

## Azure OpenAI Service Security

**Microsoft Compliance:**
Azure OpenAI services comply with a broad range of security standards, including SOC 2. Azure also adheres to many more standards, ensuring strong security measures across its platform. Full details can be found in Microsoft's compliance documentation.

**Data Residency:**
All data processed by OpenAI models is stored and processed in the same geographic region where your system is deployed.

## Continuous Monitoring and Updates

Our system undergoes continuous monitoring for vulnerabilities and threats. We regularly apply security patches and updates to ensure protection against emerging risks.