Dec 31, 2023

Keiji AI Security & Privacy Practice

Keiji is a secure platform that allows you to explore your data while considering all relevant legal, industry, and regulatory requirements. Our platform is cloud-hosted on Amazon Web Services, which is a highly secure and well-established environment. While many data and analytics platforms consider their cloud provider's security measures to be a comprehensive strategy, we at Keiji have taken additional steps to ensure the safety of our customers' data. We are building an information security system in accordance with ISO 27001, which is an industry gold standard. Our high bar of data protection and privacy controls are evident in our practice, and we also ensure our internal practices are secure and currently going through SOC 2 Type 1 and then Type 2 Certification.

Not only do we maintain secure practices and systems ourselves, but we also help our customers maintain their own compliance. Keiji is data neutral and agnostic, which means we provide you with privacy and control over the data you send to our platform. We also offer access control, data management, and other tools to help you comply with privacy regulations.

1. Certifications

SOC 2 Type 1 Certification (ongoing)

Keiji is currently undergoing a SOC2 (Service Organization Control 2) Type 1 review with a qualified auditor. This review covers all the trust principles (Security, Confidentiality, and Availability) that apply to our operations. This review aims to ensure that our practices across all aspects of the business maintain the security and confidentiality of customer data. Once the audit process is completed, we will make all our audit reports available to our customers under NDA.

ISO 27001 Certification (ongoing)

Keiji is currently considering obtaining an ISO certification. Our organization aims to adopt the ISO 27001 standard as the minimum requirement for security governance and our Information Security Management System (ISMS). By complying with ISO 27001,

we can assure our customers that we adhere to the highest standards of information security.

ISO 27018 Certification (ongoing)

Keiji is considering obtaining ISO 27018 certification to assure our customers that their personal data is handled securely and in accordance with internationally recognized high standards set by ISO. We are strongly committed to the privacy and protection of our customer's data, and this certification will demonstrate that we have a strong system of controls in place to specifically address the protection of customer data privacy.

2. Information Security

Keiji's security program governance aims to support ISO 27001/2 Information Security Management System (ISMS) requirements, as well as the needs and requirements of our customers. Our goal is to provide a secure platform while addressing all relevant legal, industry, and regulatory concerns.

Our core principles for information security are as follows:

- Maintaining a feature-rich, highly secure platform
- Addressing our customers' security needs and compliance mandates
- Operating our platform safely and reliably.

Principle 1: Empowering Our Customers with a Feature-rich and Secure Platform.

We take security very seriously in our product development process. We have strict procedures in place to ensure that all the code we write is reviewed for any potential security risks. We also provide training to our team on how to write secure code. We regularly retire old code to avoid any unnecessary risks to our platform's security.

We also have a program where we work with security researchers to identify any potential security issues in our system. This helps us stay on top of any new risks that may arise. We use a secure cloud environment to host our platform, and we have additional security measures in place to protect our users' data. These measures include things like strong encryption, automated security checks, and multi-factor authentication for all internal access.

Overall, we take every possible measure to ensure the security and reliability of our platform, so our users can feel confident when using our services.

Principle 2: Protecting Your Business, Ensuring Your Compliance is Our Priority

At Keiji AI, we understand that many of our customers have specific requirements related to rules, laws, and security standards that must be followed in their industry. Although our cloud provider, Amazon, has several compliance certifications that cover the network infrastructure and data centers, we know that it's not enough to meet the needs of our customers.

Therefore, we have adopted additional compliance programs that cover our own operations within the cloud. By doing this, we can ensure that your data and compliance requirements are always secure and protected while using Keiji's product.

Principle 3: Safety and reliability are the Operational Foundation of Our Platform

At Keiji AI, we deeply understand that security is more than just mere technical controls. It encompasses a holistic approach that covers secure environment management and the people involved. Our team strongly believes that security operations are critical to our security program's success.

To ensure that our controls are functioning optimally, we carry out a combination of internal and external audits, automated and manual in-depth testing, and a comprehensive approach to managing security alerts and events. We take data security very seriously and make sure that only necessary personnel have access to sensitive data by segregating roles. Our team also undergoes recurring, role-based training to maintain awareness of security within Keiji AI's culture.

We recognize that our customers want more than just certifications or the technology vendors we use. That's why, at Keiji AI, we are committed to providing not just top-notch technical controls but also a secure and reliable environment that you can trust. We are confident in our ability to deliver and are enthusiastic about the opportunity to work with you.

Shared Responsibility Model

As a responsible provider, Keiji takes the responsibility of maintaining a secure and reliable platform. However, as our customer, you also have a responsibility to use our AI platform in a legal and responsible manner.

It is important to understand that Keiji has certain attributes that users must take into account when using our platform. Firstly, Keiji is data-neutral, which means that we do not monitor or inspect the data that users choose to send to our platform. If our engine can process it, then it will, but Keiji does not make any data-based decisions. It only follows the queries given by users to perform specific operations. However, it is important to note that any Keiji service agreement includes restrictions on sending extremely sensitive data, such as social security numbers or bank account information, names, addresses, and medical record numbers to the Keiji platform.

Secondly, Keiji is data-agnostic, which means that it will take no action based on the nature of any particular data or its classification. All incoming data or user queries are treated similarly.

3. Data Protection Storage Policy

Data Storage and Segregation

Keiji ensures the safety of customer data by using various techniques to logically separate and encrypt it while storing it in their AWS environment. Customers can choose the geographical location for their data storage.

Data Encryption

TrialMind protects assets through encryption during transit and encryption at rest using AES-256 encryption.

4. Data Management and User Access Control

Data Governance

Our goal is to assist our customers in managing and regulating the data stored in Keiji. With our platform, users can establish their own rules for handling data and receive notifications in case of any concerns. By setting up specific ingestion guidelines, your organization can avoid accidentally storing confidential information like medical record numbers, patient names, and other identifiable data.

SSO

Our enterprise customers can access all our applications and services through Single Sign On (SSO).

Permission Levels

Keiji administrators have the minimal controls necessary to carry out their role in the organization. Customers can adjust data access for their users to specific data subsets.

5. Privacy

Data Ownership

Customers who use Keiji own the data they send to the Keiji platform for processing. Keiji collects and analyzes data about how its customers use Keiji's platform, but the data collected does not include the data sent by customers for analysis on their behalf.

For example, Keiji's platform allows customers to share clinical trial datasets for various analyses. Keiji collects usage patterns to understand how customers use their platform, but does not own or use the original clinical trial dataset for platform improvement purposes.

Personally Identifiable Information/Personal Data

Keiji customers have the flexibility to control what data is collected, processed, and stored in Keiji.

Keiji can help organizations customize our platform to minimize the personal identifiable information (PHI) sent to Keiji and reduce compliance processes by removing all HIPAA identifiers from the data.

GDPR

Keiji's privacy team is actively reviewing and improving our architecture, data flows, vendor capabilities, and agreements to ensure our platform will comply with GDPR regulations. Keiji's analytics platform does not directly interact with our customers' end-users, nor does it automatically collect personal data. However, our customers may collect and send personal data to Keiji accidentally. To ensure our customers remain compliant with privacy regulations, Keiji is evaluating and implementing procedures and upgrades.

The Keiji platform allows customers to upload and analyze their datasets. Keiji employees do not access customer datasets without customer instructions, and customer datasets are never shared or sold to third parties.

6. HIPAA and Business Associate Agreements (BAA)

For our customers who are considered covered entities or business associates under the Health Insurance Portability and Accountability Act (HIPAA), we understand that safeguarding protected health information is of utmost significance. Keiji can assist you in maintaining your HIPAA compliance through the execution of a Business Associates Agreement.

7. Contact

For questions about security and compliance, please contact support@keiji.ai
For privacy questions, please contact support@keiji.ai