

# Security & Compliance with Rheo AI

Since its inception, Rheo AI has been developed with a strong emphasis on data protection and security. The platform adheres to the '**Secure by Design**' principles and utilizes a contemporary technology stack to provide the highest levels of security, privacy and compliance standards required to meet our customers expectations.

As a consequence of this focus on security, Rheo is **ISO 27001:2022** certified, the international standard for Information Security Management Systems (ISMS). This certification demonstrates our commitment to data security and comprehensive approach to managing sensitive information.

# Application Security

## A How is your data protected?

1. Data is encrypted in transit using Transport Layer Security (TLS) 1.2
2. Data is encrypted at rest using 256-bit AES, one of the strongest block ciphers available
3. We use versioning and never delete any of your data
4. We protect your data from unauthorised access using multiple access management controls
5. Your data is backed-up every hour and copied off-site



## B How is your data isolated from other customers?

To ensure data and process isolation, each customer gets dedicated instances of the Rheo AI application, segregated database and data stores. You can choose between 2 identity models and authentication options.



### SAML-based Single Sign-On (SSO)

You can integrate Rheo AI with your corporate credential directories using Security Assertion Markup Language (SAML v2.0) to retain full control of the authentication process. You can also automatically provision and deprovision your users in Rheo AI with Single Sign-On (SSO) services to manage user accounts across SaaS providers, including Rheo AI.



### Rheo AI Cloud Accounts

You can also manage user accounts directly in Rheo AI.

- › Configurable Password Policy
- › Credentials are never stored in human readable format. We use a secure one-way hash algorithm with a salt.

## C User Permissions and Access Control

Rheo provides complete transparency through ensuring that access to your Rheo AI instances are governed by user roles and access rights configured by your designated Rheo AI Administrators.

## Where will our data be hosted?

We host Rheo AI in Amazon Web Services (AWS) data centers (the leading Infrastructure as a Service (IaaS) cloud provider) in the United States. AWS maintains multiple certifications and attestations for its hosting operations. For more information about their certification and compliance program, please visit the AWS website links on [security](#) and [compliance](#).



## Privacy

Rheo AI is committed to protecting your data including the personal information of your employees. As a result we help your organization remain and demonstrate compliance with Privacy Laws and Regulations.

## Data Ownership And Control



### Who owns the data we store in your service?

You maintain full ownership and control of your data uploaded or created in Rheo AI.



### What happens to our data if we cancel our subscription to Rheo AI?

Rheo AI makes your data accessible for retrieval at any time during the term of your subscription and for a period of 60 days after the termination of your subscription. After 60 days, Rheo AI will disable the account and will securely delete your data.