Rencore Governance

Your data is safe with Rencore Governance

Evaluating Rencore Governance

Before you make the decision to analyze your own tenant with Rencore Governance, you always have the option to sign up and use demo data to evaluate Rencore Governance. At this stage you do not need to connect your own tenant and we do not access any of your data.

Hosting

Infrastructure

Rencore Governance infrastructure is hosted on Microsoft Azure and passes all built-in automated regulatory compliance checks and security controls (Azure CIS 1.1.0, PCI DSS 3.2.1, SOC TSP, ISO 27001).

Self-hosting

Rencore Governance can also be hosted by yourself or your managed service provider (MSP) in your own Azure subscription. Self-hosting is only available in Enterprise plans and will require additional installation and onboarding efforts.

Authentication

Rencore Governance uses Azure AD applications. Customers consent to these AAD apps to grant the Rencore Platform access to the data required to perform analysis and monitoring. Customers can at any point revoke the App-Only or Delegated permissions granted to our applications. Rencore never asks for or stores any usernames or passwords.

Personal Identifiable Information (PII)

Rencore Governance collects usernames, e-mail addresses, URLs, title and other metadata of the collected data like Site Collections, Sites, Lists, Teams, etc. Collected customer data can be removed at any time by removing the encrypted storage tables belonging to the customer. Any PII information is also encrypted.

Rencore Governance does not monitor the activity of specific users (post messages in chats for example), but metadata. If users leave the organization, their data is removed by the next scan of the organization's tenant performed by Rencore Governance. Rencore Governance scans the tenant daily.

Your data is safe with Rencore Governance

Database

Rencore Governance uses Azure Storage Accounts. The storage accounts have strong built-in encryption in Azure, as well as firewalls and restricted network access. By using a no-SQL database, we eliminate the inherent risk of SQL injections as well as other OWASP TOP 10 risks posed by using SQL.

Data storage location

For US customers, data is stored in Azure Storage Accounts in one of the Microsoft US data centers. For European customers, data is stored in Azure Storage Accounts in the Microsoft West Europe data center.

Data and information encryption

All information is encrypted. Azure Storage Accounts have built-in support for encryption at rest, and in-transit. In addition to this, we add another layer of cryptographic AES 256-bit industry-standard encryption around the data before it is transmitted to the storage. All transmission from the application to the end-user are SSL encrypted.

Data types scanned and stored in Azure

Depending on the MS services you want to govern (Teams, SharePoint, Power Automate, Microsoft 365) Rencore Governance collects inventory data for these services that are used to build your reports with. Rencore Governance scans and stores Metadata like URLs, Title, Creation Date, Owner, Member, Last modification date etc.

Rencore Governance does not scan content (e.g. mails, documents, Teams messages, Teams attachments).

Data retention lifespan

Rencore Governance retains the collected data during your usage of our product, as it is required to build the dashboards, checks, and reports. Upon cancelling the subscription, or otherwise no longer being a customer of Rencore, we delete and purge the data used. Customers can also actively delete all the data by accessing their Rencore Governance account and clicking "Delete workspace".

If a user leaves the organization, their data is removed by the next scan of the organization's tenant performed by Rencore Governance. Rencore Governance scans the tenant daily.

Roles and Responsibilities

Data and system access permissions at Rencore

Rencore cannot access the data and systems if you host Rencore Governance in your own Azure subscription. If you use Rencore Governance as a Software-as-a-service (Saas) solution, only senior qualified staff in the Technical Operations team have access to our production cloud environments and subscriptions.

Zero access for subcontractors or third-party partners

Absolutely no subcontractors or third-party partners have access to your production or cloud environments.

Your data is safe with Rencore Governance

Services and Access Rights

Rencore Governance uses Azure Active Directory applications to access data in customer tenants.

In the list below, you can find all the services and the permissions used to collect information.

Permission	Type	Collected information
Azure Service Management		
User_impersonation	Delegated	▪ Power Automate Flows, Flow Runs etc.
Microsoft Graph		
Directory.Read.All	Delegated	▪ Groups, Users, Group Memberships ▪ Licenses ▪ Teams
Group.Read.All	Delegated	▪ Teams
Group.Read.All	Application	▪ Teams Activity (e.g., Messages)
Sites.Read.All	Delegated	▪ Site Collections
User.Read	Delegated	▪ Used for login into application
Office 365 Management		
ActivityFeed.Read		▪ AuditLog Events (e.g., Team Created)
ServiceHealth.Read		▪ Service Messages
SharePoint		
Sites.Read.All	Application	▪ Site Collections ▪ Sites ▪ Lists
Sites.FullControl.All	Application	▪ Site Collection Owner ▪ File Sharing Information ▪ Workflows, InfoPath Forms

Rencore Governance uses HTTP/SSL to access the data and store it directly encrypted in the backend storage. There is no other data transmission.