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. This infrastructure 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, including additional infrastructure requirements on the customer's part.

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, either globally or on a per-service basis. Rencore never asks for or stores any usernames or passwords used to authenticate in Rencore Governance.

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. Customers can request the removal of PII at any time. Any PII information is encrypted.

Rencore Governance does not monitor the activity of specific users (post messages in chats for example), but does process 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 or at another frequency determined by the customer or as required by the nature of the items being scanned. Provisioning features may allow the customer to edit PII in the Microsoft 365 tenant through the use of Rencore Governance; however, the customer remains in full control of the PII within their Microsoft 365 tenant throughout this process, and may refrain from using provisioning features at all if preferred.

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. This uses a no-SQL database, eliminating the inherent risk of SQL injections as well as other OWASP TOP 10 risks posed by using SQL. Rencore also uses PostgreSQL and modern security coding methods to protect against the risk of SQL injections.

Data storage location

The customer selects the location of data storage upon connecting Rencore Governance to their Microsoft 365 tenant. The customer has a choice between three Azure data centres: West Europe (Netherlands); Central US (Iowa), Australia East (New South Wales). Rencore recommends that customers in the EU/EFTA region use the West Europe data centre, that customers in the Americas use the Central US data centre, and that customers in the APAC region use the Australia East data centre; however, this choice remains fully up to the customer.

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, Rencore Governance adds 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 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. 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. emails, 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". Data is marked for deletion and held for a period of 30 days before it is permanently deleted (in order to allow for a restore in the event of accidental deletion); customers can request immediate and permanent deletion of their data at any time.

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 or at another frequency determined by the customer or as required by the nature of the items being scanned.

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 (self-hosting). If you use Rencore Governance as a Software-as-a-service (SaaS) solution, senior qualified staff in the Technical/Product Operations or Customer Success teams have access to information on inventory counts and the names of data segments/dashboards – this does not include any information on the contents of Rencore Governance environments and/or Microsoft 365 tenants, and this information is only accessed for troubleshooting purposes. Nobody else at Rencore has access to this information.

Services and Access Rights

Zero access for subcontractors or third-party partners

Absolutely no subcontractors or third-party partners have access to your production or cloud environments; while subprocessors are used within Rencore Governance (please refer to the Data Processing Agreement for a full list), they do not process data from a connected Microsoft 365 tenant, but rather data that passes through their APIs in the course of using their services (e.g. by providing feedback to a feature in the product).

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

You can find all the services and the permissions used to collect information here:

https://url.rencore.com/gov-permissions

Rencore Governance uses HTTP/SSL to access the data and store it directly encrypted in the backend storage.