Keeyns
info@keeyns.com
www.keeyns.com

Pettelaarpark 20
5216 PD 's-Hertogenbosch
The Netherlands

Keeyns Security Principles

At Keeyns, we strive to be as secure as possible for each individual customer. No exceptions and no additional premium packages required. We keep an eye out for the latest developments in security technologies and ensure the software has the latest patches and security updates. Keeyns is completely hosted in Azure, Microsoft's cloud platform, which currently consists of more than 200 services that integrate securely and easily together.

Each customer of Keeyns receives their own dedicated authentication tokens, credentials, encryption certificates, and Keeyns application instance. Each token expires after some time, which increases security. All the services of Keeyns always require authentication tokens, no exceptions. All data is encrypted in transit using TLS. Your documents that are uploaded are encrypted using AES with a unique key per file, accessible only using an RSA certificate. This certificate is safely stored in the Microsoft Azure Key Vault, and every customer has their own. The vault prevents anyone from extracting the certificate and decrypting the data.

For user authentication, Keeyns uses a third party: Auth0. This party provides features like OAuth2 authentication and SSO. By using this party, user passwords are not stored in the Keeyns platform.

Services we use from Microsoft Azure

As mentioned, Keeyns is hosted in Azure. Keeyns uses the following services from Azure:

1.1 **Key Vault**
Storage and protection of encryption certificates for each client. It is impossible to retrieve the certificate from this vault.

1.2 **App Service**
A service for hosting the web application of Keeyns. This service can be scaled up and deployed to any country supported by Microsoft Azure. The code running on this service is immutable. It provides access to databases and storage locations for documents. Each customer of Keeyns will get their own instance, ensuring that heavy usage by one customer does not affect others and that in-memory data remains for the intended customers.

1.3 **Function App**
The Function App is used for running the Keeyns Tax Engine and for scheduled work. Customers share these instances of services on the platform. The services do not have access to documents or other customer data.

1.4 Application Insights

Application Insights is a tool that Keeyns uses for logging. Every request is logged to this service with its timings and metadata. App Insights provides tools to monitor performance on services and requests and can send notifications on any abnormality. Keeyns will not log sensitive data.

1.5 Storage Account V2

Documents uploaded to Keeyns are stored in a service called Storage Account. This service supports large documents and encryption at rest by default. As Keeyns encrypts documents before they are sent to this storage account, it is not possible to recover documents without the decryption key and certificate from the Key Vault. No document is publicly available and requires service authentication before a document can be retrieved.

1.6 SQL Server + Database

A relational database to store customer data configured in Keeyns. The data includes dossiers, workflows, document metadata, discussions, and access rights for every user. Keeyns only has access to the data in this database, but not its structure. It is not possible to mutate the structure of the database. Any modification needed on this database structure will be performed during the upgrade of Keeyns to a newer version.

1.7 Cosmos DB

A non-relational database to store generated tax reports and results by the Tax Engine. It will also store any modifications that the user has applied.

1.8 MS Office 365

Keeyns seamlessly integrates with Microsoft Office 365, allowing users to create, edit, and collaborate on documents within the Keeyns platform using familiar Office applications such as Word, Excel, and PowerPoint. This integration enhances productivity by enabling direct access to Office tools for document management and collaboration, all within the secure environment of Azure services. Documents created or edited within Office 365 can be securely stored in the Keeyns platform, with all the encryption and security measures provided by Azure, ensuring that user data remains protected at all times.

The SLA of each Azure service can be found at: Azure Service Level Agreements

KEEYNS

Backup and Restore

To ensure that no data is lost, Keeyns applies certain backup strategies:

- A backup is created every day for documents. They are stored in a separate subscription in Azure with its own access policies. The documents are copied as is and are not decrypted.

- The database will have a Point-in-time recovery enabled for 7 days. In case anything happens, the database can be restored to the second when the event occurred.

- The data in Cosmos DB gets a backup every 12 hours. However, it is limited to two backups as this database can grow exponentially.

- The source code and binaries of Keeyns are kept indefinitely. This means that any version of the software can be installed at any time.

Frequently Asked Questions: Security & Privacy

- **Q: Where will the data be hosted (country)?**
  A: Keeyns is hosted in Azure. By default, we host our services in West Europe, which has a data center in Amsterdam. Therefore, we will store it in the Netherlands by default. On request, we can change this location to a different country.

- **Q: What is the data retention period?**
  A: Due to legal laws (WWFT), documents are never deleted. However, you could remove them to the Trash bin in the portal.

- **Q: What is the procedure for data deletion?**
  A: We will delete the encryption keys and the blob storage container in Azure to ensure all customer data is removed.

- **Q: What controls are in place to ensure data is deleted?**
  A: None, but we use the four-eye principle to ensure everything related to this specific customer is deleted in Azure.

- **Q: Is the vendor and/or data outside of the EEA?**
  A: No.

- **Q: Does the tool provide Single Sign-On (SSO)? What authentication method is being used?**
  A: Yes, we have SSO on our own environments. If you have rights to multiple client portals, you can switch between them without logging in again. For our authentication, we use Auth0 (https://auth0.com/) which implements OAuth2.

KEEYNS

- **Q: Does the vendor have any Security/Privacy/Compliance certifications?**
  A: We obtained the ISO27001 certificate – information security (the certificate is attached).

- **Q: Does the vendor have a security policy in place?**
  A: Attached is our privacy statement.

- **Q: Does the vendor have a vulnerability reporting & management program?**
  A: We comply with ISO27001 security standards. Additionally, we have a yearly external IT architect audit.

- **Q: Have there been any issues, scandals, negative publicity that we should be aware of?**
  A: There have not.

- **Q: Does the tool provide Single Sign-On (SSO)? If No, what authentication method is being used?**
  A: No, we don't. To log in, clients need an email address, password, and a two-factor authenticator app on their phone linked to their Keeyns account. The authenticator app is required because it reduces the chances of fraud, data loss, or identity theft. We recently disabled push notifications from Keeyns to the authenticator app after some recent news about confirmed risks regarding push notifications. You now manually need to start your authenticator app and confirm your identity by entering a six-digit number.

- **Q: Does the vendor have any Security/Privacy/Compliance certifications?**
  A: We obtained the ISO27001 certificate – information security.

- **Q: Does the vendor have a security policy in place?**
  A: See the principles above.

- **Q: Does the vendor have a vulnerability reporting & management program?**
  A: We run the ZAP vulnerability scanner at least twice a year. Additionally, we have a yearly external IT architect audit and our yearly ISO audit.

- **Q: Have there been any issues, scandals, negative publicity?**
  A: None.

- **Q: Who will administer access to the account, i.e., registering/setting up user access/logins, etc?**
  A: After implementation and go-live, portal management will be handed over to the end-users. As part of the implementation process, both user and administrator training will be provided by Keeyns. Typically, only 2 individuals will have administrative rights to avoid confusion in management. Keeyns is designed to be

KEEYNS

user-friendly, requiring no IT expertise to manage the portal. However, our support team can make changes as needed. It is worth mentioning that Keeyns will automatically update any changes to the standard processes we offer, such as the VAT return process and its associated deadlines, in the event of a legal amendment.

- **Q: Will the account have a single login, or will one login be required per user (I expect 2-3 people on the team will need access to the system)?**
  A: Every user is granted an individual account on Keeyns for two reasons:
  - o We place high significance on maintaining an accurate audit trail, which requires a record of who performed what action and when. This cannot be achieved with a shared account.

  - o From a security standpoint, it is designed to ensure the safety of the platform. Each user has their own account, secured by a unique password and a two-factor authenticator linked to their mobile device to verify the user's identity during login attempts, preventing unauthorized access. Please note that the number of users does not affect our pricing structure/your quote.

- **Q: Where is Keeyns hosted?**
  A: Keeyns is hosted on Microsoft Azure. All data is stored within the EU, in the Netherlands and Ireland.

- **Q: Details of the process for adding admin and standard users?**
  A: During the implementation of Keeyns, we work closely with our customer to set everything up as desired. Usually, one employee of the customer will be added and promoted to admin by us. This admin then has rights to create other users and promote them to admin if necessary.

- **Q: Can you please provide a link to the user policy (if any) that will need to be accepted by all users?**
  A: This is covered by the general terms and conditions that the customer signs upon purchasing Keeyns.

- **Q: Details of what, if any, user logging is done by the system, where those logs are stored, and who has access to them?**
  A: We have system logging stored on Azure, accessible only by Keeyns employees with specific rights. This logging does not contain sensitive information and is only used to analyze the operation of the platform. We also keep track of all logins of the users and the changes made by these users on the platform. This data is stored in our database on Azure. In the application, this data can be viewed by our customers' users (only those with sufficient rights) in the audit trail of dossiers. This is a useful

KEEYNS

feature that allows our customers to easily look up who performed which actions on a dossier.

- **Q: By default, does Keeyns allow for any integrations with other systems, and if so, what systems, and can this be disabled?**
  A: Keeyns has several integrations:
    - o **Auth0:** This service handles all authentication flows. This integration cannot be disabled.
    - o **Microsoft Office 365:** This service allows online editing of multitple type of documents. There is an option to enable or disable this integration.
    - o **SendGrid:** This service sends emails on behalf of Keeyns. Emails are composed in our services and only the email is transferred to this service. This integration cannot be disabled.

- **Q: Does Keeyns have any Privileged Utility Programs, and if so, what are they, why are they needed, who has access to them, and why?**
  A: Keeyns does not have any privileged utility programs. We run a backup tool to ensure backups of documents, but that runs without any user interaction in Azure. It has just enough privileges to perform this task.

- **Q: Is any source code stored within the Keeyns application?**
  A: No, all source code is safely stored in Microsoft Azure DevOps. Keeyns is not a tool to manage and collaborate on any source code.

KEEYNS