

panagenda OfficeExpert Privacy Policy

This article explains how panagenda OfficeExpert stores, uses and discloses the information it collects.

Data Collection

There are two primary ways in which OfficeExpert collects information:

- Secure calls (HTTPS) to Microsoft cloud services
- Secure calls (SSL) from OfficeExpert bots installed on-premises

Data Storage

All collected data is stored and processed within the OfficeExpert virtual appliance - **there is no external data processing!**

By default, all personal data is obfuscated, and therefore compliant with the EU's General Data Protection Regulation (GDPR). Obfuscation can only be disabled by applying a new license. Please refer to [Data Protection in User Profiles](#) for further details on that.

All passwords stored for OfficeExpert are either hashed or encrypted.

Usage Data

panagenda OfficeExpert **does not** collect any usage data and does not automatically send logs, configurations, statistics, benchmark data, or similar to panagenda.

Data Access

OfficeExpert is delivered as a virtual software appliance that supports VMWare ESX, Microsoft Hyper V and an Azure deployment . The customer installs OfficeExpert on-premises (or in their own Azure tenant) - thus the customer owns and controls the level of security such as where the virtual appliance is installed, as well as, who has which level of access to it.

OfficeExpert offers two different user roles:

- **Admin** with full access to configuration and data
- **Viewer** with limited access to data and no access to configuration