Privacy Policy for OfficeExpert TrueDEM

Version 5 - April 8, 2021

Scope

This privacy policy describes panagenda's privacy practices for **OfficeExpert TrueDEM**

It only applies to the data collected and processed within the service. Any data in relation to the business transaction between panagenda and you (sales contacts, payment information, etc) is covered by our general privacy policy.

Who We Are

The panagenda group is made up of the following entities:

- panagenda GmbH, Austria
- panagenda GmbH, Germany
- panagenda Inc., USA
- Trust Factory B.V., The Netherlands

Contact details for the Data Protection Officer can be found in the "Contact Us" section at the end of this document.
General contact details for all entities can be found on our website: https://www.panagenda.com/imprint

What We Collect

The main function of OfficeExpert TrueDEM is to collect and analyze technical and usage information from a variety of devices and cloud services. As such, we collect a large range of data. To protect your privacy, we split this data into two parts that are processed and stored separately.

Core Data

Core Data is anonymized telemetry data. Core Data contains no Personally Identifiable Information (PII) of any kind.

Privileged Data

Privileged Data has the potential to contain information that may be covered by privacy laws or company policies. As a result, all Privileged Data is isolated and stored in customer-specific data structures.

The following information can be collected, depending on the chosen settings:

User Display Name, User Email Addresses, and UPN

These are collected to assist with reporting in user interfaces. For example, this would allow your help desk to identify data about a specific user. This is a cloud-only function, the agent never has access to this information.

IP Addresses

These are categorized into public and internal/private. They can be used to identify where people are, for example if you know the address ranges of your office locations. For each, you can choose to store the original or replace it with a cryptographic hash.

Host Names

The host names of users' devices, to assist with help desk activities.

WiFi Network Information

For identifying issues with networks and performance. This includes data like the SSID.

Microsoft Teams Presence History and Call Records

Metadata about the usage of Microsoft Teams for your analytics, reporting, and help desk.

Location Information

Used for analytics, reporting, and help desk activities. This data can be stored at the most accurate level, or get replaced with a circular reference approximating the location to about 160 km.

How and Why We Collect Information

There are two main sources of information: The agent that you install on your users' devices which then uploads information to us, and your Microsoft cloud services from which we pull information. Data from both is transmitted to and stored in our cloud services and is encrypted in transit and at rest.

Core Data (anonymized, no personally identifiable information) and Privileged Data (personally identifiable information) are stored separately, and Privileged Data can only be accessed by the accounts of your employees that you authorize to do so.

We use or access your data to:

- Carry out our obligations arising from any contracts entered into between you and us (Core and Privileged Data)
- Provide support and maintenance to you (Core and Privileged Data)
- Create benchmarks and draw insights from statistical analysis for the benefit of all customers (Core Data only)
- Operate a public web site providing aggregated information about the status of Microsoft cloud services (Core Data only)
- Operate, debug, test, improve our systems (Core and Privileged Data)

Where We Transfer and Store Your Data

To facilitate our operations, we utilize the cloud infrastructure by providers such as Microsoft. Microsoft's Privacy Policy can be found here: https://azure.microsoft.com/en-us/support/legal/

The jurisdiction can be chosen by you. Currently the choices are:

- US
- EU

Upon collection, data is transferred to the chosen location and stored there. Both Core Data and Privileged Data will remain in the chosen location unless a transfer to a different location is requested by you.

panagenda affiliated entities will have access to the data from the jurisdictions they operate in for the purposes described further above under the protections of this privacy policy. You will have access to the data from the jurisdictions your organization operates in.

For any transfer of data across jurisdictions we implement appropriate solutions as required by law (e.g. standard contractual clauses, privacy shield in accordance with Article 5 GDPR).

How We Protect Your Data

First things first: **Keeping your data safe is of paramount importance to us.**

You trust us with very sensitive information. That's why our service was built from the ground up with the safety of your data in mind:

- All data is encrypted in transport and at rest using state-of-the-art technology.
- Sensitive data can be obfuscated at the source. IP addresses can be replaced with a cryptographic hash, and geographic locations can be degraded to approximate locations, among other options.
- We separate the data into Core (=no personally identifiable information) and Privileged (personally identifiable) Data. Each is stored separately.
- Each customer's Privileged Data is stored separate from all others and is protected with customer-specific safeguards.
- You can choose to prevent any access to Privileged Data – even by us.

- You choose who at your organization gets access to the data.
- We follow best practices for security in cloud implementations as recommended by Microsoft.
- Access to our systems is tightly controlled and limited to employees and trusted partners that absolutely need to access them.
- Employees and trusted partners sign strict confidentiality and privacy agreements and undergo regular security and privacy training.

While we are committed to take all reasonable steps to protect and secure your data, we will not be held responsible for events arising from external parties gaining unauthorized access.

How Long We Store Your Data

Data is stored until it must be deleted in compliance with legal obligations.

More specifically:

- We may store Core Data indefinitely. Due to its anonymized nature, it cannot be traced back to the originating organization or users.
- We store Privileged Data until our contractual relationship with you is fulfilled, or until it must be deleted – either due to request by you or for other legal reasons.

Others Working for Us

To guarantee the highest level of security for our customers, it is of utmost importance that we emphasize the secure utilization of third-party software. Ensuring the safe deployment of such software is instrumental in safeguarding your data and systems against potential threats. When selecting third-party applications, it is vital to prioritize solutions with a proven track record of security and reliability, obtained from reputable sources. Regularly updating and patching these applications is critical to prevent exposure to emerging vulnerabilities. Additionally, exercise caution when granting permissions or sharing data with third-party software and always adhere to best practices outlined in our security guidelines.

Panagenda OfficeExpert TrueDEM uses third-party software in accordance with Art. 6(1) point f GDPR on the basis of our legitimate interest in improving the stability and functionality of our software-as-a-service offering. The data is to be passed on or used in any other way. However, we reserve the right to check the server log files subsequently, if there are any concrete indications of illegal use.

Who We Share Your Data With

Generally, we do not share your data with anyone, except for parties we are working with to provide this service, as outlined in the sections “Others Working for Us” and “Where We Transfer and Store Your Data” above.

This especially applies to Privileged Data.

However, Core Data may be used to draw insights, perform statistical analysis, and be aggregated to provide anonymized information to all our customers and to the public. Under no circumstance will information based on this data be traceable or identifiable as coming from your organization or a specific person at your organization.

Furthermore, we may be compelled to disclose your data (Core or Privileged):

- In response to a search warrant, court order, or similar legal request from a court, law enforcement, or other government agency
- Where required to do so by law
- To report a crime (such as suspected child exploitation)

Business Transfers

As we develop our business, we might be involved in a reorganization, merger, acquisition, or sale of our assets. Your information may be transferred as part of such a deal but will remain subject to the protections and promises made in any preexisting privacy policy (unless you consent otherwise). We will send you a notice and outline your options in this event via the contact information you have provided to us.

Rights

Data subjects have the right to lodge a complaint with a supervisory authority, the right to request access to and rectification or erasure of personal data, restriction of processing or to object to processing, as well as the right to data portability.

Where processing is based on freely given consent (Article 6 (1)(a) GDPR), data subjects have the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. With this notice we provide you with some general information regarding the processing of personal data in connection with our contractual relationship. Information about processing activities other than the ones associated with this service might be provided separately.

You have following specific rights when it comes to the processing of your personal data by us:

- Right to be informed: when your personal data is processed by us, you have the right to know about it (see further in Art 15 GDPR)
- Right to be correct or erase, access: you have the right to access the information and have it corrected without delay if it is inaccurate or incomplete.
- Right to object and restrict the data usage: You can ask to have your data blocked under certain circumstances. You can also object to it, in certain circumstances, on grounds relating to your specific situation.
- Right of portability: You have the right to receive your personal data in a standardized format in case you wish to transfer it to another controller (data portability). You can request that any of the above changes be communicated to other parties to whom your data have been disclosed.
- Right to withdrawal consent: Where the processing is based on your consent, you have the right to revoke the given consent at any time. Please keep in mind that your withdrawal does not affect the lawfulness of the processing prior to your withdrawal.
- Right to lodge a complaint: You have the right to complain at any time if you believe your data protection rights have been breached. For this purpose, please contact us directly. Of course, you have the right to file a complaint with the Austrian Data Protection Authority (or with another authority, in the country which is competent on your residence).

How to exercise your data protection rights

Please send us a written request to our Data Protection Officer (contact details can be found at the end of this document). We cannot accept verbal requests (via phone, chat) as we may not be able to deal with your identification. Therefore, your request should contain a detailed, accurate description of your data you want to access or corrected. In cases where we have a reasonable doubt about your person, we might ask to provide a copy of a document helping us verifying your identity (e.g. passport, please black out the information which are is not necessary thereof). We only use the information on your identification strictly for this purpose and the data will not be stored longer than needed.

Changes to This Policy

We may update this privacy policy from time to time by posting the updated document to our website. You acknowledge that it is your responsibility to review this policy periodically.

If we make changes to this policy that materially reduce your rights or protections, we will send you an update notice via the contact information you have provided to us.

Contact Us

We welcome questions, requests, and comments regarding this policy or any information we collect. They should be addressed to our Data Protection Officer.

Contact Details of Data Protection Officer

Michael Hafner
Schreyvogelgasse 3/10
AT-1010 Vienna, Austria
Cell: +43 699 18 99 18 09
email: michael.hafner@panagenda.com