panagenda

OfficeExpert™ TrueDEM

Digital Operational Resilience Act Compliance Paper

Foreword

Florian Vogler
Chief Executive Officer

In today's rapidly evolving digital landscape, ensuring the resilience and security of financial institutions is paramount. As a responsible software provider, we are committed to supporting our clients in navigating the complexities of regulatory compliance. This technical paper outlines our proactive approach to achieving compliance with the Digital Operational Resilience Act (DORA).

April 10th, 2025, Version 1.1 EN

Contents

What is DORA?

The Digital Operational Resilience Act (DORA) is a regulation enacted by the European Union to enhance the digital operational resilience of financial entities. It aims to ensure that financial institutions can withstand, respond to, and recover from all types of ICT-related disruptions and threats, including cyberattacks.

Why is DORA Important?

DORA is crucial because it addresses the increasing dependency of the financial sector on digital technologies and third-party ICT service providers. By establishing a harmonized framework for ICT risk management, DORA helps mitigate the risks associated with digital operations, thereby safeguarding the stability and integrity of the financial system across the EU. Compliance with DORA not only protects individual institutions but also enhances the resilience of the entire financial ecosystem.

Why We Proactively Inform Our Customers About DORA Compliance Efforts

Proactively informing our customers about our DORA compliance efforts is essential for several reasons:

- **Transparency and Trust:** By openly communicating our compliance status, we build trust with our clients, demonstrating our commitment to their security and operational resilience.
- **Risk Mitigation:** Keeping our customers informed helps them understand the measures we have in place to protect their data and operations, thereby reducing their risk exposure.
- **Regulatory Alignment:** Ensuring our clients are aware of our compliance efforts helps them align their own practices with regulatory requirements, facilitating smoother audits and inspections.
- **Competitive Advantage:** Demonstrating proactive compliance can be a differentiator in the market, highlighting our dedication to maintaining the highest standards of security and resilience.

We are dedicated to continuously improving our practices to meet and exceed the requirements set forth by DORA, ensuring that our clients can rely on us as a trusted partner in their digital operations.

Obligations

Under the EU Digital Operational Resilience Act (DORA), third-party ICT service providers, such as our company, have specific obligations to ensure the resilience and security of their services. panagenda OfficeExpert TrueDEM is a hosted software solution. This means that strict and robust risk management practices are in place to ensure the resilience and security of the solution and data. This includes regular testing, monitoring, and reporting of our software's performance and security measures. By adhering to these obligations, we help our clients maintain operational continuity and compliance with DORA's stringent standards, thereby enhancing the overall resilience of their digital operations.

Contracts with ICT third-party service providers must clearly assign the rights and obligations of the financial company and the service provider and document them in writing. Art. 30 DORA prescribes specific aspects for service provider contracts, including:

Service locations

panagenda GmbH (Headquarters)
Sonnenfelsgasse 13/9
AT 1010 Vienna
Austria
Comm. Register: FN 293 516 t, HG Wien

panagenda GmbH
Lahnstrasse 17
DE 64646 Heppenheim
Germany
Comm. Register: Darmstadt HRB 88148

Additional locations:

Microsoft Azure Datacenters

panagenda currently operates two SaaS instances of panagenda OfficeExpert TrueDEM. One instance is running within Microsoft Azure West Europe where customer data is stored in West Europe / Amsterdam. The other instance is running in Microsoft Azure East US2 where customer data is stored in Virginia / US.

Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA
Phone: +1 (425) 882-8080

panagenda strongly recommends Microsoft Azure West Europe for customers within the EU and EFTA. Microsoft guarantees industry-leading data protection for customers in Europe with its EU Data Boundary for the Microsoft Cloud initiative.

MaxMind

MaxMind provides location data and additional information on IP addresses.

> *MaxMind Inc., 51 Pleasant Street #1020, Malden, MA 02148 USA*

No information other than a public IP address is used to query the information provided by MaxMind.

panagenda OfficeExpert TrueDEM

panagenda OfficeExpert TrueDEM includes two components: the TrueDEM Client Software (Agent Application) and the TrueDEM Portal.

TrueDEM Client Software

> The Software is installed locally on end-user devices and is automatically updated
>
> It utilizes blazingCDN to provide panagenda OfficeExpert TrueDEM Client software delivery and updates to customers. Only the Agent application package is located on that Content delivery network. The application is digitally signed by panagenda (GlobalSign certificate).

TrueDEM Portal

> OfficeExpert TrueDEM portal and data is hosted on Microsoft Azure in the EU and US regions. West Europe / Amsterdam for EU and East US2 / Virginia for US

Service Name

panagenda OfficeExpert TrueDEM

This applies to the entire panagenda OfficeExpert TrueDEM solution stack

Service Scope

Provisioning, hosting and management of data and components of panagenda OfficeExpert TrueDEM.

Description of provided TrueDEM functions & services

Microsoft Entra ID Enterprise Applications for OfficeExpert TrueDEM

OfficeExpert TrueDEM API

Microsoft Entra ID Enterprise application with the sole purpose to expose Agent APIs securely. The scopes are used by the Entra ID Enterprise Application: OfficeExpert TrueDEM Agent. **No Data is collected with this Application**.

OfficeExpert TrueDEM Agent

This is the Entra ID Enterprise application that authorizes the panagenda OfficeExpert TrueDEM Agent (deployed to end-users) to perform tests on behalf of the logged-in user. This application uses delegated permissions, which means that every single operation is carried out on behalf of the user, and only on resources that the user can access as well. The **panagenda OfficeExpert TrueDEM Agent never reads or consumes any content** such as Teams chats, OneDrive files or emails – these permissions are required so that the panagenda OfficeExpert TrueDEM Agent can accurately (i.e., for the logged in user specifically) measure the availability of M365 services.

This Entra ID Enterprise App is required for the panagenda OfficeExpert TrueDEM Agent to be able to retrieve data on behalf of the logged in user. A one-time, global admin consent is required.

Which data is collected:

Different types of technical system metrics for Device, Network, Applications.

Possible PII items:

Wi-Fi SSID, Wi-Fi BSSID, hashed public IP address, Device Name

OfficeExpert TrueDEM Call and Health

This Entra ID Enterprise Application is leveraged by the backend panagenda OfficeExpert TrueDEM engine to retrieve client's call records data – a critical source of metadata offered by Microsoft's APIs. The metadata collected here is the equivalent of what Microsoft stores and makes available as part of the Call Quality Dashboard. This is the data that is later augmented with what was recorded by the panagenda OfficeExpert TrueDEM Agent on the endpoint.

This Application is required for retrieving call and system health-related data from Microsoft. This is part of the data which is later combined with data retrieved from the endpoint. A one-time, global admin consent is required.

Which data is collected:

Metrics about every Microsoft Teams Call and Metrics and Status information about the System Health Data from the M365 Cloud.

Possible PII items?

Users Id, Users Principal Name, Username, Mail Address, Surname, Given Name, Job Title, Age Group, EntraID Extension Attributes 1 to15

OfficeExpert TrueDEM Portal & Data

Cloud based environment used by customers to access analytical and performance data delivered in proprietary reports and insight pages. A separate instance of panagenda OfficeExpert TrueDEM exists for each customer. The instance resides on either the EU or US Azure region datacenters depending on the customer's requirement.

Data is stored in the same region and is not exchanged between regions.

panagenda TrueDEM portal provides access to the data. Custom reports can be created and are stored and maintained in the customer's instance.

All communications with our API maintain the following standards:

- Communications only take place over SSL/TLS (TLS 1.2) secured connections
- Communications require an authenticated connection from the agent on the client machine
- The payload for all communications is encrypted separately from, or in addition to, the SSL/TLS layer

Updates to the Portal and its content are initiated by panagenda on a regular basis.

Grafana Framework is the Software layer used to depict and access the data. The Data layer is a Microsoft Azure Data Explorer Cluster

TrueDEM Manager

The TrueDEM Manager is a support app created and digitally signed by panagenda that orchestrates the secure update process of the TrueDEM Agent on user devices. TrueDEM Manager is executed post-login and establishes a connection with the Autodiscover service. This is to verify the agent type and version as well as to determine the update channel.

Administrative privileges are required to install the application. No administrative privileges are required for the functioning of the app.

The app stores installation files locally on the user's device and maintains logs on the device at: *%localappdata%\panagenda\TrueDEM Manager\logs*

TrueDEM Agent

Lightweight software application responsible for collecting data from the endpoint device. The application runs in the user's context and does not require admin rights. It does require delegated permissions in Microsoft Entra ID Enterprise Applications (see above).

The agent is not designed to store data locally under normal operation. However, it can store temporary files on a user's machine if connectivity to Microsoft Azure is limited. This temporary data does not contain display names, usernames, email addresses, passwords, or any other sensitive information.

All data gathered by the agent is encrypted, from local storage caching to successful transmission to our SaaS platform. This includes local storage buffering, transmission, and while at rest.

TrueDEM Teams plugin

Plugin installed as part of the TrueDEM Agent that actively retrieves metrics from within the Teams client during calls

%localappdata%\Packages\PerfraxInc.OfficeExpertEPM_wmk1sxh3zvv7j\LocalCache\Plugins\TeamsPlugin

Provisions on availability, authenticity, integrity, and confidentiality

OfficeExpert TrueDEM recognizes and collects two types of information:

- **Core Data:** Anonymized telemetry data that does not contain Personally Identifiable Information of any kind.

- **Privileged data**: Data that has the potential to contain data that may be covered by privacy laws or company policies.

The following privileged data is collected, depending on 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.
- **Wi-Fi 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.

Data on clients:

As stated earlier, the local TrueDEM Agent can temporarily store non-privileged information locally as well as installation, performance and events logs. All data gathered by the agent is encrypted from inception until successful transmission to our SaaS platform. This includes in-memory, during transmission, and while at rest.

Logs are stored at

%localappdata% \Packages\PerfraxInc.OfficeExpertEPM_wmk1sxh3zvv7j\LocalCache\Logs

and overwritten after 7 days. They contain ERROR and WARN indications including timestamps with basic event description.

Management data:

panagenda logs and stores successful and unsuccessful OfficeExpert TrueDEM Manager installations within Azure AppInsights. Logs are kept for 30 days.

Availability:

panagenda will ensure that the SaaS solution shall be available to Customer at least 99% of the time of the respective Azure Datacenter uptime during any calendar year excluding planned and communicated in advance maintenance windows.

Authenticity:

Customer's data is securely sent from end user devices to the dedicated OfficeExpert TrueDEM instance. The TrueDEM Agent initiates a connection to the autoconfig service utilizing the end-user's token to retrieve the specific TrueDEM configuration. This ensures that the end-users' data is directed to the correct Instance. Consequently, data flow is exclusive and secure as each EventHub is designated to interact with only its corresponding customer database. Afterwards the TrueDEM Agent asks the SaaS Provider to connect to EventHub.

Integrity:

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.
- panagenda separates the data into core data, which holds no personally identifiable information, and privileged data, which might include personally identifiable information. 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 panagenda.
- You choose who at your organization gets access to the data by using the customers Microsoft Entra ID.
- panagenda follows 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.

Confidentiality:

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:

- United States of America (US)
- European Union (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 above under the protection of the panagenda privacy policy. The customer will have access to the data from the jurisdictions their organization operates in.

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

Core data processing:

Non-privileged fully anonymized data can be used by panagenda to detect trends and provide general Microsoft availability information. This data is in no way traceable to an individual or organization.

Third party software:

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 not 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.

Agreed service levels

The most current version of panagenda's general terms and conditions of license and maintenance can be found here: https://www.panagenda.com/legal

Service Availability and SLA

panagenda ensures that the SaaS solution shall be available to Customer at least 99% of the time of the respective Azure Datacenter uptime during any calendar year excluding planned and communicated in advance maintenance windows.

Monitoring and Reporting

Monitoring and reporting on the uptime, usage and performance of the environment is done through the panagenda OfficeExpert TrueDEM enterprise application.

Client Support

panagenda offers a hotline for technical support during office hours, on working days in Austria and/or Germany (Monday to Friday, excluding holidays) from 9.00 – 17.00 CET. Additionally, you can contact us by e-mail (support@panagenda.com) in German or English.

Security and Risk Management

Risk Assessment

ICT risk assessments at panagenda are performed on a bi-annual basis and are part of its Information Security Management System (ISMS) operation. If required, reassessments of risk can be performed at any time.

Security Measures

panagenda has applied the principle of least privilege to its ICT environment to ensure access security. We also established a robust but lightweight Secure Software Development Life Cycle (SSDLC) as part of our ISO 27001:2022 strategy.

Data and application are stored in Microsoft Azure datacenters. Microsoft Azure datacenter security information can be found here: https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security

Our customers are fully responsible for secure deployment of the panagenda OfficeExpert TrueDEM Agent.

Incident Management

panagenda has a company-wide incidence response plan in place. This plan includes procedures for detection, reporting and resolution of ICT-related incidents. Whenever a customer of panagenda is affected (directly or indirectly) by an ICT-related incident happening at panagenda, we comply to required notification periods applied through EU legislation.

Compliance, Transparency and Audit Rights

Regulatory Compliance

panagenda obeys all relevant DORA requirements and regular updates to ensure ongoing compliance.

Transparency

panagenda supports and promotes open communication with its customers regarding compliance status, risk assessments, and incident reports.

Audit Rights

Customers have the right to audit our compliance with DORA requirements and security measures. The costs of such an audit are to be borne entirely by the customer.

Obligation to support the financial entity in ICT incident management

During an ICT incident, third-party ICT service providers play a crucial role in supporting financial entities to ensure swift resolution and minimal disruption. panagenda is committed to providing

comprehensive support, which includes immediate notification to the affected financial entity. We offer technical assistance to diagnose and mitigate the issue. Additionally, we collaborate closely with our customers to implement corrective actions and prevent future occurrences. This proactive and responsive approach not only helps in maintaining operational continuity but also reinforces our commitment to safeguarding our clients' digital resilience and compliance with DORA standards.

Termination rights and associated minimum notice periods

panagenda respects the right of termination according to DORA requirements. Since panagenda OfficeExpert TrueDEM is offered as a service and operated by panagenda, a minimum notice period of 60 days before the renewal date is required.

Training and awareness of ICT third-party service providers on digital operational resilience

Participation in Training Programs

panagenda is looking forward to participating in the financial entity's ICT security awareness and resilience training programs. This ensures that all parties are aligned on security protocols and incident response procedures.

Regular Updates and Education

Continuous education and regular updates on ICT risk management practices are essential. This includes staying informed about the latest threats, vulnerabilities, and regulatory changes.

Post-Incident Learning

After any panagenda OfficeExpert TrueDEM related incident, panagenda should be involved in post-incident reviews. panagenda will integrate the lessons learned into their training and awareness programs. This helps in refining our response strategies and improving overall resilience

BY ADHERING TO THESE SERVICE LEVEL COMMITMENTS, PANAGENDA ENSURES THE RESILIENCE AND SECURITY OF ITS SERVICES, SUPPORTING ITS CLIENTS IN MAINTAINING OPERATIONAL CONTINUITY AND COMPLIANCE WITH DORA.