panagenda

MarvelClient™

SecurityInsider™

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).

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. Even though panagenda MarvelClient is pure on-premises software, we are still required to implement robust risk management practices. 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

panagenda MarvelClient and panagenda SecurityInsider software delivery and update servers are hosted in Austria (update.panagenda.com)

panagenda MarvelClient and panagenda SecurityInsider software is operated within each customers ICT network (on premises) by our customers themselves (the only exception being online software update provisioning services provided by panagenda)

Service Name

panagenda MarvelClient and panagenda SecurityInsider

This applies to the entire panagenda MarvelClient software stack and panagenda SecurityInsider

Service Scope

Provisioning and maintenance of components of the panagenda MarvelClient Software Stack and panagenda SecurityInsider

Description of provided MarvelClient functions & services

Two databases on HCL Domino Servers

- A **configuration database** which contains instructions for clients
- An **analyze database** storing detailed information about clients and their respective configuration

MarvelClient does not require any server tasks.

Typically, both above databases are replicated across all mail servers, which are assumed to be the servers that end-users can reach most efficiently. The databases scale along easily, even in large environments with several 100,000 users.

One local MarvelClient binary/file on HCL Notes Clients

MarvelClient runs as an extension in HCL Notes clients and in end user context, without administrative operating system permissions on modern operating systems. Once installed, the local MarvelClient file automatically creates and updates a couple of additional local files in the so called MarvelClient Working Directory.

No local file is required for HCL Nomad clients since panagenda MarvelClient is fully integrated into the Nomad app (starting with version 1.0.4).

- mc.dll or pmc.dll on Microsoft Windows, Citrix and Windows Terminal Server
- libmarvelclient.dylib or libpmc.dylib on Intel Mac OS X 64 bit

Additional component for MarvelClient Eclipse

MarvelClient Eclipse also includes a plugin which allows the binary to natively talk to Eclipse and vice versa. Installing and updating the plugin is automatically taken care of by the local MarvelClient file.

Additional component for MarvelClient Upgrade

MarvelClient Upgrade comes with an additional executable file which can be easily deployed to end users by MarvelClient itself.

Update Server

MarvelClient offers interactive automated online update. This service is provided through update.panagenda.com (URL: https://update.panagenda.com/pub/panaweb.nsf/GetLicenseInfo?openagent&key=YOURLICENSEKEY&product=MC).

Description of provided SecurityInsider functions & services

One database on HCL Domino Servers

- One **database** which contains both configuration for security scans and corresponding results

SecurityInsider does not require any server tasks or additional components on clients.

Update Server

SecurityInsider offers interactive automated online update. This service is provided through update.panagenda.com (URL: https://update.panagenda.com/pub/panaweb.nsf/GetLicenseInfo?openagent&key=YOURLICENSEKEY&product=SI).

Provisions on availability, authenticity, integrity, and confidentiality

Both panagenda MarvelClient and SecurityInsider do not collect or process any data or personal identifiable information (PII) outside of the customers ICT environment.

For legal reasons, access protocols to our online update service (update.panagenda.com) are stored for a minimum of 60 days (external IP address, time, event description).

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/download/legal/General-Terms-and-Conditions-of-Licence-and-Maintenance_2021-02_EN.pdf

Service Availability and SLA

panagenda guarantees a 99% availability of its software delivery and update servers, excluding scheduled maintenance windows. Since panagenda MarvelClient and SecurityInsider are hosted on premises within the customers ICT environment, panagenda cannot offer any availability SLA on their operation.

Monitoring and Reporting

As stated above, panagenda MarvelClient and SecurityInsider are hosted and operated within the customers ICT environment. Upon request, panagenda gladly provides its customers an offer to help ensure secure and compliant operations.

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.

Our customers are fully responsible for secure operations of panagenda MarvelClient and SecurityInsider. Key management, access rights and encryption of data in transfer and at rest must be managed within the customers HCL Dominio environment. panagenda can offer support on any aspect of administration for HCL Domino.

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 MarvelClient and panagenda SecurityInsider are not offered as a service but operated by the customer within the customer's ICT environment, no minimum notice period 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 MarvelClient or SecurityInsider 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.