panagenda

iDNA Applications™

GL GreenLight™

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).

November 19, 2024, Version 1.01 EN

Contents

Foreword.......... 2

What is DORA? 4

Why is DORA Important?.......... 4

Why We Proactively Inform Our Customers About DORA Compliance Efforts 4

Obligations.......... 5

Service locations 5

Service Name 6

Service Scope.......... 6

Description of provided functions & services.......... 7

Group of Docker containers acting in concert 7

Container overview.......... 7

Update Server 8

Provisions on availability, authenticity, integrity, and confidentiality.......... 9

Agreed service levels.......... 9

Service Availability and SLA 9

Security and Risk Management 9

Compliance, Transparency and Audit Rights.......... 10

Obligation to support the financial entity in ICT incident management.......... 10

Termination rights and associated minimum notice periods.......... 10

Training and awareness of ICT third-party service providers on digital operational resilience 10

Participation in Training Programs.......... 10

Regular Updates and Education.......... 11

Post-Incident Learning.......... 11

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 GreenLight and panagenda iDNA Applications 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 GreenLight and panagenda iDNA Applications software delivery and update servers are hosted at

KeyCDN (keycdn.com).
proinity LLC
Reichenauweg 1
8272 Ermatingen
Switzerland

panagenda GreenLight and panagenda iDNA Applications 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 GreenLight and panagenda iDNA Applications

This applies to the entire panagenda iDNA Applications and panagenda GreenLight software stacks.

Service Scope

Provisioning and maintenance of components of the panagenda iDNA Applications and panagenda GreenLight software stacks.

Description of provided functions & services

Group of Docker containers acting in concert

The applications panagenda GreenLight and panagenda iDNA Applications are composed of a series of Docker containers that operate synergistically to deliver comprehensive web interfaces and a robust data collection backend. These containers facilitate seamless interaction and data integration, ensuring optimal performance and scalability within the customers' ICT infrastructure.

The deployment architecture leverages container orchestration to streamline processes, enhance resource utilization, and provide high availability. This modular approach not only simplifies maintenance but also allows for effortless scaling and updates, thereby aligning with advanced IT management practices.

Container overview

Component	Core Technologies	Link
End user web interfaces	Nginx Node.JS (React)	https://nginx.org/en/ https://nodejs.org/en
Admin & config interfaces	Nginx Node.JS (React) Apache Tomcat	https://nginx.org/en/ https://nodejs.org/en https://tomcat.apache.org/
Data collection backend	Apache Tomcat Hazelcast HCL Domino	https://tomcat.apache.org/ https://hazelcast.com/ https://www.hcl-software.com/domino/features
Data warehouse	PostgreSQL	https://www.postgresql.org/
Analytics & dashboarding interface	Metabase (Open Source)	https://www.metabase.com/start/oss/

These containers are operated on a Linux operating system, with Red Hat Linux or Red Hat-based Linux being recommended, using Docker and Docker Compose. To facilitate deployment and expedite evaluation installations, panagenda also offers pre-built virtual appliance images for VMWare vSphere and Microsoft Hyper-V. These virtual appliances utilize Alma Linux as the base operating system, which is a distribution built on Red Hat Linux.

If customers deploy these pre-built appliances, they assume full control and responsibility for the base operating system, including system updates. This enables customers to implement their own security policies in accordance with their internal guidelines.

panagenda GreenLight and panagenda iDNA Applications do not necessitate any installations on customer Domino servers, nor do they require the execution of additional server tasks or reconfiguration, assuming default Domino configurations are in place. This design choice significantly mitigates potential security risks by reducing the attack surface and ensuring that no additional vulnerabilities are introduced into the customer's IT environment.

Update Server

panagenda GreenLight and panagenda iDNA Applications software delivery and update servers are hosted on KeyCDN (keycdn.com).

KeyCDN is a high-performance content delivery network (CDN) designed to accelerate the delivery of web content by distributing it across a global network of servers. It enhances security through features like DDoS protection, secure token authentication, and TLS encryption, ensuring data integrity and protection against cyber threats. Additionally, KeyCDN offers high availability with its robust infrastructure, providing redundancy and failover mechanisms to ensure continuous and reliable access to content.

Provisions on availability, authenticity, integrity, and confidentiality

Both panagenda GreenLight and IDNA Applications 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: Imprint - panagenda | panagenda

Service Availability and SLA

panagenda guarantees a 99% availability of its software delivery and update servers, excluding scheduled maintenance windows. Since panagenda GreenLight and panagenda IDNA Applications 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 GreenLight and panagenda IDNA Applications 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 GreenLight and panagenda IDNA Applications. 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 GreenLight and panagenda IDNA Applications 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 GreenLight or panagenda IDNA Applications 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.