panagenda

iDNA Applications™

GL GreenLight™

# Digital Operational Resilience Act Compliance-Dokument

# Vorwort

Florian Vogler
Geschäftsführer

In der heutigen sich schnell entwickelnden digitalen Landschaft ist die Sicherstellung der Widerstandsfähigkeit und Sicherheit von Finanzinstituten von größter Bedeutung. Als verantwortungs--bewusster Softwareanbieter sind wir bestrebt, unsere Kunden bei der Bewältigung der Komplexität der regulatorischen Compliance zu unterstützen. Dieses technische Papier skizziert unseren proaktiven Ansatz zur Erreichung der Compliance mit dem Digital Operational Resilience Act (DORA)

# Inhalt

# Was ist DORA?

Der Digital Operational Resilience Act (DORA) ist eine von der Europäischen Union erlassene Verordnung zur Verbesserung der digitalen operativen Widerstandsfähigkeit von Finanzinstituten. Ziel ist es sicherzustellen, dass Finanzinstitute in der Lage sind, allen Arten von IKT-bezogenen Störungen und Bedrohungen, einschließlich Cyberangriffen, standzuhalten, darauf zu reagieren und sich davon zu erholen.

# Warum ist DORA wichtig?

DORA ist von entscheidender Bedeutung, da es die zunehmende Abhängigkeit des Finanzsektors von digitalen Technologien und Drittanbietern von IKT-Dienstleistungen anspricht. Durch die Schaffung eines harmonisierten Rahmens für das IKT-Risikomanagement trägt DORA dazu bei, die mit digitalen Operationen verbundenen Risiken zu mindern und somit die Stabilität und Integrität des Finanzsystems in der gesamten EU zu schützen. Die Einhaltung von DORA schützt nicht nur einzelne Institutionen, sondern stärkt auch die Widerstandsfähigkeit des gesamten Finanzökosystems

# Warum wir unsere Kunden proaktiv über unsere DORA-Compliance-Bemühungen informieren

Unsere Kunden proaktiv über unsere DORA-Compliance-Bemühungen zu informieren, ist aus mehreren Gründen wesentlich:

- **Transparenz und Vertrauen**: Durch die offene Kommunikation unseres Compliance-Status bauen wir Vertrauen bei unseren Kunden auf und zeigen unser Engagement für ihre Sicherheit und operative Widerstandsfähigkeit.
- **Risikominderung**: Indem wir unsere Kunden informieren, helfen wir ihnen, die Maßnahmen zu verstehen, die wir zum Schutz ihrer Daten und Abläufe ergriffen haben, und reduzieren so ihre Risikobelastung.
- **Regulatorische Ausrichtung**: Wenn unsere Kunden über unsere Compliance-Bemühungen informiert sind, können sie ihre eigenen Praktiken besser an die regulatorischen Anforderungen anpassen, was reibungslosere Audits und Inspektionen erleichtert.
- **Wettbewerbsvorteil**: Proaktive Compliance kann ein Unterscheidungsmerkmal auf dem Markt sein und unser Engagement für die höchsten Standards in Bezug auf Sicherheit und Widerstandsfähigkeit hervorheben.

Wir sind bestrebt, unsere Praktiken kontinuierlich zu verbessern, um die Anforderungen von DORA zu erfüllen und zu übertreffen, damit unsere Kunden sich auf uns als vertrauenswürdigen Partner in ihren digitalen Abläufen verlassen können.

# Verpflichtungen

Gemäß dem EU Digital Operational Resilience Act (DORA) haben Drittanbieter von IKT-Dienstleistungen, wie unser Unternehmen, spezifische Verpflichtungen zur Sicherstellung der Widerstandsfähigkeit und Sicherheit ihrer Dienste. Obwohl panagenda GreenLight und panagenda iDNA Applications reine On-Premises-Software ist, sind wir dennoch verpflichtet, robuste Risikomanagementpraktiken umzusetzen. Dies umfasst regelmäßige Tests, Überwachung und Berichterstattung über die Leistung und Sicherheitsmaßnahmen unserer Software. Durch die Einhaltung dieser Verpflichtungen helfen wir unseren Kunden, die betriebliche Kontinuität und die Einhaltung der strengen DORA-Standards aufrechtzuerhalten und so die allgemeine Widerstandsfähigkeit ihrer digitalen Abläufe zu verbessern.

Verträge mit Drittanbietern von IKT-Dienstleistungen müssen die Rechte und Pflichten des Finanzunternehmens und des Dienstleisters klar zuweisen und schriftlich dokumentieren. Art. 30 DORA schreibt spezifische Aspekte für Dienstleisterverträge vor, einschließlich:

## Dienstleistungsstandorte

panagenda GmbH (Headquarters)
Sonnenfelsgasse 13/9
AT 1010 Wien
Österreich
Handelsregister: FN 293 516 t, HG Wien

panagenda GmbH
Lahnstrasse 17
DE 64646 Heppenheim
Deutschland
Handelsregister: Darmstadt HRB 88148

panagenda GreenLight und panagenda iDNA Applications Software Verteilungs- und Update-server werden gehostet bei:

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

**panagenda GreenLight und panagenda iDNA Applications wird innerhalb des IKT-Netzwerks jedes Kunden (vor Ort) von unseren Kunden selbst betrieben (die einzige Ausnahme sind Online-Software-Update-Dienste, die von panagenda bereitgestellt werden).**

# Dienstleistungsname

**panagenda GreenLight und panagenda iDNA Applications**

Dies behandelt die gesamte panagenda iDNA Applications und panagenda GreenLight  Software-Stacks.

# Leistungsumfang

Bereitstellung und Wartung der Komponenten des panagenda iDNA Applications und panagenda GreenLight  Software-Stacks.

# Beschreibung der bereitgestellten Funktionen und Dienste

## Gruppen von Docker-Containern, die zusammenarbeiten

Die Anwendungen panagenda GreenLight und panagenda iDNA Applications bestehen aus einer Reihe von Docker-Containern, die synergistisch zusammenarbeiten, um umfassende Webschnittstellen und ein robustes Datenerfassungs-Backend bereitzustellen. Diese Container ermöglichen eine nahtlose Interaktion und Datenintegration und gewährleisten so eine optimale Leistung und Skalierbarkeit innerhalb der IKT-Infrastruktur der Kunden.

Die Bereitstellungsarchitektur nutzt Container-Orchestrierung, um Prozesse zu optimieren, die Ressourcennutzung zu verbessern und hohe Verfügbarkeit zu gewährleisten. Dieser modulare Ansatz erleichtert nicht nur die Wartung, sondern ermöglicht auch müheloses Skalieren und Aktualisieren, wodurch er sich an fortschrittliche IT-Managementpraktiken anpasst.

## Übersicht der Container

| Component | Core Technologies | Link |
|---|---|---|
| End user web interfaces | Nginx<br>Node.JS (React) | https://nginx.org/en/<br>https://nodejs.org/en |
| Admin & config interfaces | Nginx<br>Node.JS (React)<br>Apache Tomcat | https://nginx.org/en/<br>https://nodejs.org/en<br>https://tomcat.apache.org/ |
| Data collection backend | Apache Tomcat<br>Hazelcast<br>HCL Domino | https://tomcat.apache.org/<br>https://hazelcast.com/<br>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/ |

Diese Container werden auf einem Linux-Betriebssystem betrieben, wobei Red Hat Linux oder Red Hat-basierte Linux-Distributionen empfohlen werden, unter Verwendung von Docker und Docker Compose. Um die Bereitstellung zu erleichtern und Evaluierungsinstallationen zu beschleunigen, bietet panagenda auch vorgefertigte virtuelle Appliance-Images für VMWare vSphere und Microsoft Hyper-V an. Diese virtuellen Appliances verwenden Alma Linux als Basisbetriebssystem, eine Distribution, die auf Red Hat Linux basiert.

Wenn Kunden diese vorgefertigten Appliances bereitstellen, übernehmen sie die volle Kontrolle und Verantwortung für das Basisbetriebssystem, einschließlich Systemupdates. Dies ermöglicht es den Kunden, ihre eigenen Sicherheitsrichtlinien gemäß ihren internen Richtlinien zu implementieren.

**panagenda GreenLight und panagenda iDNA Applications erfordern keine Installationen auf Kunden-Domino-Servern und auch keine Ausführung zusätzlicher Serveraufgaben oder Neukonfigurationen, vorausgesetzt, es sind Standard-Domino-Konfigurationen vorhanden.** Diese Designwahl verringert potenzielle Sicherheitsrisiken erheblich, indem die Angriffsfläche reduziert und sichergestellt wird, dass keine zusätzlichen Schwachstellen in die IT-Umgebung des Kunden eingeführt werden.

## Update-Server

Die Softwarebereitstellungs- und Update-Server von panagenda GreenLight und panagenda iDNA Applications werden auf KeyCDN (keycdn.com) gehostet.

KeyCDN ist ein leistungsstarkes Content Delivery Network (CDN), dass die Bereitstellung von Webinhalten beschleunigt, indem es sie über ein globales Netzwerk von Servern verteilt. Es erhöht die Sicherheit durch Funktionen wie DDoS-Schutz, sichere Token-Authentifizierung und TLS-Verschlüsselung, um die Datenintegrität und den Schutz vor Cyber-Bedrohungen zu gewährleisten. Darüber hinaus bietet KeyCDN eine hohe Verfügbarkeit mit seiner robusten Infrastruktur und stellt Redundanz- und Failover-Mechanismen bereit, um kontinuierlichen und zuverlässigen Zugriff auf Inhalte zu gewährleisten.

# Bestimmungen zur Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit

panagenda GreenLight und panagenda iDNA Applications sammeln oder verarbeiten keine Daten oder personenbezogenen Informationen (PII) außerhalb der IKT-Umgebung der Kunden.

Aus rechtlichen Gründen werden Zugriffsprotokolle auf unseren Online-Update-Dienst (update.panagenda.com) für mindestens 60 Tage gespeichert (externe IP-Adresse, Zeit, Ereignisbeschreibung).

# Vereinbarte Service-Level

Die aktuelle Version der allgemeinen Lizenz- und Wartungsbedingungen von panagenda finden Sie hier: Imprint - panagenda | panagenda

# Serviceverfügbarkeit und SLA

panagenda garantiert eine 99%ige Verfügbarkeit seiner Softwarebereitstellungs- und Update-Server, ausgenommen geplanter Wartungsfenster. Da panagenda GreenLight und panagenda iDNA Applications vor Ort in der IKT-Umgebung der Kunden gehostet werden, kann panagenda keine Verfügbarkeits-SLA für den Betrieb der Produkte anbieten.

## *Überwachung und Berichterstattung*

Wie oben erwähnt, wird panagenda GreenLight und panagenda iDNA Applications in der IKT-Umgebung der Kunden gehostet und betrieben. Auf Anfrage unterbreitet panagenda seinen Kunden gerne ein Angebot, um den sicheren und konformen Betrieb von panagenda GreenLight und panagenda iDNA Applications zu gewährleisten.

## *Kundensupport*

panagenda bietet eine Hotline für technischen Support während der Bürozeiten an Arbeitstagen in Österreich und/oder Deutschland (Montag bis Freitag, außer an Feiertagen) von 9.00 bis 17.00 Uhr MEZ. Zusätzlich können Sie uns per E-Mail (support@panagenda.com) in Österreich und Deutschland.

# Sicherheits- und Risikomanagement

## *Risikobewertung*

IKT-Risikobewertungen bei panagenda werden halbjährlich durchgeführt und sind Teil des Betriebs des Informationssicherheitsmanagementsystems (ISMS). Bei Bedarf können Risikoneubewertungen jederzeit durchgeführt werden.

## *Sicherheitsmaßnahmen*

panagenda hat das Prinzip der minimalen Rechtevergabe auf seine IKT-Umgebung angewendet, um die Zugangssicherheit zu gewährleisten. Wir haben auch einen robusten, aber leichtgewichtigen Secure Software Development Life Cycle (SSDLC) als Teil unserer ISO 27001:2022-Strategie etabliert.

Unsere Kunden sind vollständig verantwortlich für den sicheren Betrieb von panagenda GreenLight und panagenda iDNA Applications. Schlüsselverwaltung, Zugriffsrechte und Verschlüsselung von Daten während der Übertragung und im Ruhezustand müssen innerhalb der HCL Domino-

Umgebung der Kunden verwaltet werden. panagenda kann Unterstützung bei allen Aspekten der Verwaltung von HCL Domino anbieten.

### *Vorfallmanagement*

panagenda verfügt über einen unternehmensweiten Vorfallreaktionsplan. Dieser Plan umfasst Verfahren zur Erkennung, Meldung und Lösung von IKT-bezogenen Vorfällen. Wann immer ein Kunde von panagenda (direkt oder indirekt) von einem IKT-bezogenen Vorfall bei panagenda betroffen ist, halten wir uns an die durch die EU-Gesetzgebung vorgeschriebenen Benachrichtigungsfristen.

## Compliance, Transparenz und Prüfungsrechte

### *Regulatorische Compliance*

panagenda erfüllt alle relevanten DORA-Anforderungen und führt regelmäßige Updates durch, um die fortlaufende Compliance sicherzustellen.

### *Transparenz*

panagenda unterstützt und fördert die offene Kommunikation mit seinen Kunden in Bezug auf den Compliance-Status, Risikobewertungen und Vorfallberichte.

### *Prüfungsrechte*

Kunden haben das Recht, unsere Einhaltung der DORA-Anforderungen und Sicherheitsmaßnahmen zu prüfen. Die Kosten einer solchen Prüfung sind vollständig vom Kunden zu tragen.

# Verpflichtung zur Unterstützung der Finanzinstitute im IKT-Vorfallmanagement

Während eines IKT-Vorfalls spielen Drittanbieter von IKT-Dienstleistungen eine entscheidende Rolle bei der Unterstützung von Finanzinstituten, um eine schnelle Lösung und minimale Unterbrechungen sicherzustellen. panagenda verpflichtet sich, umfassende Unterstützung zu bieten, die eine sofortige Benachrichtigung des betroffenen Finanzinstituts einschließt. Wir bieten technische Unterstützung zur Diagnose und Behebung des Problems. Darüber hinaus arbeiten wir eng mit unseren Kunden zusammen, um Korrekturmaßnahmen umzusetzen und zukünftige Vorfälle zu verhindern. Dieser proaktive und reaktionsschnelle Ansatz trägt nicht nur zur Aufrechterhaltung der betrieblichen Kontinuität bei, sondern stärkt auch unser Engagement für den Schutz der digitalen Widerstandsfähigkeit unserer Kunden und die Einhaltung der DORA-Standards.

# Kündigungsrechte und zugehörige Mindestkündigungsfristen

panagenda respektiert das Kündigungsrecht gemäß den DORA-Anforderungen. Da panagenda GreenLight und panagenda iDNA Applications nicht als Dienstleistung angeboten wird, sondern vom Kunden innerhalb der IKT-Umgebung des Kunden betrieben wird, ist keine Mindestkündigungsfrist erforderlich.

# Schulung und Sensibilisierung von Drittanbietern von IKT-Dienstleistungen zur digitalen operativen Widerstandsfähigkeit

## Teilnahme an Schulungsprogrammen

panagenda freut sich darauf, an den Schulungsprogrammen zur IKT-Sicherheit und Widerstandsfähigkeit der Finanzinstitute teilzunehmen. Dies stellt sicher, dass alle Parteien auf Sicherheitsprotokolle und Verfahren zur Vorfallreaktion abgestimmt sind.

## Regelmäßige Updates und Weiterbildung

Kontinuierliche Weiterbildung und regelmäßige Updates zu IKT-Risikomanagementpraktiken sind unerlässlich. Dies umfasst das informieren über die neuesten Bedrohungen, Schwachstellen und regulatorischen Änderungen.

## Lernen nach Vorfällen

Nach jedem Vorfall im Zusammenhang mit panagenda GreenLight und panagenda iDNA Applications sollte panagenda in Nachbesprechungen einbezogen werden. panagenda wird die gewonnenen Erkenntnisse in ihre Schulungs- und Sensibilisierungsprogramme integrieren. Dies hilft, unsere Reaktionsstrategien zu verfeinern und die allgemeine Widerstandsfähigkeit zu verbessern.

DURCH DIE EINHALTUNG DIESER SERVICELEVEL-VERPFLICHTUNGEN STELLT PANAGENDA DIE WIDERSTANDSFÄHIGKEIT UND SICHERHEIT SEINER DIENSTLEISTUNGEN SICHER UND UNTERSTÜTZT SEINE KUNDEN BEI DER AUFRECHTERHALTUNG DER BETRIEBLICHEN KONTINUITÄT UND DER EINHALTUNG VON DORA.