panagenda

OfficeExpert™ TrueDEM

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 verantwortungsbewusster 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

Zusätzliche Standorte:

Microsoft Azure Datenzentren

panagenda betreibt derzeit zwei SaaS-Instanzen von panagenda OfficeExpert TrueDEM. Eine Instanz läuft innerhalb von Microsoft Azure West Europe, wobei Kundendaten in Westeuropa / Amsterdam gespeichert werden. Die andere Instanz läuft in Microsoft Azure East US2, wobei Kundendaten in Virginia / USA gespeichert werden.

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

panagenda empfiehlt dringend Microsoft Azure Westeuropa für Kunden innerhalb der EU und der EFTA. Microsoft garantiert branchenführenden Datenschutz für Kunden in Europa mit seiner EU-Datenrichtlinie für die Microsoft Cloud-Initiative.

MaxMind

MaxMind stellt Standortdaten und zusätzliche Informationen zu IP-Adressen bereit.

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

Es werden keine weiteren Informationen als eine öffentliche IP-Adresse verwendet, um die von MaxMind bereitgestellten Informationen abzufragen.

panagenda OfficeExpert TrueDEM

panagenda OfficeExpert TrueDEM umfasst zwei Komponenten: die TrueDEM Client-Software (Agent-Anwendung) und das TrueDEM-Portal.

TrueDEM Client-Software

> Die Software wird lokal auf Endgeräte der Benutzer installiert und automatisch aktualisiert.
>
> Sie nutzt **blazingCDN**, um die panagenda OfficeExpert TrueDEM Client-Software Bereitstellung und Updates für die Kund zu liefern. Nur das Agenten-Anwendungspaket befindet sich auf diesem Content-Delivery-Netzwerk. Die Anwendung ist digital von panagenda (GlobalSign-Zertifikat) signiert.

TrueDEM-Portal

> Das OfficeExpert TrueDEM-Portal und die Daten werden in den Microsoft Azure-Regionen EU und US gehostet. Westeuropa / Amsterdam für die EU und East US2 / Virginia für die USA.

Dienstleistungsname

panagenda OfficeExpert TrueDEM

Dies betrifft die gesamte panagenda OfficeExpert TrueDEM Software-Stack.

Leistungsumfang

Bereitstellung, Hosting und Verwaltung von Daten und Komponenten von panagenda OfficeExpert TrueDEM.

Beschreibung der bereitgestellten TrueDEM-Funktionen und -Dienste

Microsoft Entra ID Enterprise Applications für OfficeExpert TrueDEM

OfficeExpert TrueDEM API

Microsoft Entra ID Enterprise-Anwendung mit dem einzigen Zweck, Agent-APIs sicher zu exponieren. Die Bereiche werden von der Entra ID Enterprise-Anwendung OfficeExpert TrueDEM Agent verwendet. **Mit dieser Anwendung werden keine Daten gesammelt.**

OfficeExpert TrueDEM Agent

Dies ist die Entra ID Enterprise-Anwendung, die den panagenda OfficeExpert TrueDEM Agent (auf Endbenutzer-Computern bereitgestellt) autorisiert, Tests im Namen des angemeldeten Benutzers durchzuführen. Diese Anwendung verwendet delegierte Berechtigungen, was bedeutet, dass jede einzelne Operation im Namen des Benutzers durchgeführt wird und nur auf Ressourcen zugreift, auf die der Benutzer auch zugreifen kann. Der **panagenda OfficeExpert TrueDEM Agent liest oder verwendet niemals Inhalte** wie Teams-Chats, OneDrive-Dateien oder E-Mails – die Berechtigungen sind erforderlich, damit der panagenda OfficeExpert TrueDEM Agent die Verfügbarkeit von M365-Diensten genau (d.h. speziell für den angemeldeten Benutzer) messen kann.

Die Entra ID Enterprise-App ist erforderlich, damit der panagenda OfficeExpert TrueDEM Agent Daten im Namen des angemeldeten Benutzers abrufen kann. Eine einmalige globale Admin-Zustimmung ist erforderlich.

Welche Daten werden gesammelt:

> Verschiedene Arten von technischen System-Metriken für Gerät, Netzwerk, Anwendungen.

Mögliche PII-Elemente:

> Wi-Fi-SSID, Wi-Fi-BSSID, gehashte öffentliche IP-Adresse, Gerätename

OfficeExpert TrueDEM Call und Health

Diese Entra ID Enterprise-Anwendung wird von der Backend-Engine panagenda OfficeExpert TrueDEM genutzt, um Anrufdatensätze von Kunden zu sammeln – eine wichtige Metadatenquelle, die von Microsofts APIs bereitgestellt wird. Die hier gesammelten Metadaten entsprechen denen, die Microsoft speichert und im Call Quality Dashboard verfügbar macht. Dies sind die Daten, die später mit denen ergänzt werden, die vom panagenda OfficeExpert TrueDEM Agent auf dem Endgerät erfasst wurden.

Diese Anwendung ist erforderlich, um anruf- und systemgesundheitsbezogene Daten von Microsoft abzurufen. Dies ist ein Teil der Daten, die später mit den vom Endgerät abgerufenen Daten kombiniert werden. Eine einmalige globale Admin-Zustimmung ist erforderlich.

Welche Daten werden gesammelt:

> Metriken zu jedem Microsoft Teams-Anruf und Metriken sowie Statusinformationen zur Systemgesundheit aus der M365-Cloud.

Mögliche PII-Elemente:

Benutzer-ID, Benutzer-Hauptname, Benutzername, E-Mail-Adresse, Nachname, Vorname, Berufsbezeichnung, Altersgruppe, EntraID-Erweiterungsattribute 1 bis 15

OfficeExpert TrueDEM Portal & Daten

Cloud-basierte Umgebung, die von Kunden genutzt wird, um analytische- und Leistungsdaten in proprietären Berichten und Insight-Seiten abzurufen. Für jeden Kunden existiert eine separate Instanz von panagenda OfficeExpert TrueDEM. Die Instanz befindet sich entweder in den EU- oder US-Azure-Region-Datenzentren, je nach Anforderung des Kunden.

Daten werden in der gleichen Region gespeichert und nicht zwischen Regionen ausgetauscht.

Das panagenda TrueDEM-Portal ermöglicht den Zugriff auf die Daten. Benutzerdefinierte Berichte können erstellt und in der Instanz des Kunden gespeichert und verwaltet werden.

Alle API-Kommunikationen erfüllen die folgenden Standards:

- Die Kommunikation erfolgt nur über SSL/TLS (TLS 1.2) gesicherte Verbindungen
- Für die Kommunikation ist eine authentifizierte Verbindung vom Agenten auf dem Client-Gerät erforderlich
- Der Payload für alle Kommunikationen ist separat oder zusätzlich zur SSL/TLS-Schicht verschlüsselt

Updates des Portals und seines Inhalts werden regelmäßig von panagenda initiiert.

Das Grafana-Framework ist die Softwareschicht, die zur Darstellung und zum Zugriff auf die Daten verwendet wird. Die Datenschicht ist ein Microsoft Azure Data Explorer Cluster.

TrueDEM Manager

Der TrueDEM Manager ist eine von panagenda erstellte und digital signierte Support-App, die den sicheren Aktualisierungsprozess des TrueDEM-Agenten auf Benutzergeräten orchestriert. Der TrueDEM Manager wird nach dem Login ausgeführt und stellt eine Verbindung zum Autodiscover-Dienst her, um den Agententyp und die Version zu überprüfen sowie den Update-Kanal zu bestimmen.

Für die Installation der Anwendung sind Administratorrechte erforderlich. Für die Funktionsweise der App sind keine Administratorrechte erforderlich.

Die App speichert Installationsdateien lokal auf dem Gerät des Benutzers und protokolliert die Logs auf dem Gerät unter: %localappdata%\panagenda\TrueDEM Manager\logs

TrueDEM Agent

Leichte Softwareanwendung, die Daten vom Endgerät sammelt. Die Anwendung läuft im Benutzerkontext und erfordert keine Administratorrechte. Es benötigt jedoch delegierte Berechtigungen in Microsoft Entra ID Enterprise Applications (siehe oben).

Der Agent ist nicht dafür ausgelegt, Daten unter normalen Bedingungen lokal zu speichern. Er kann jedoch temporäre Dateien auf dem Computer des Benutzers speichern, wenn die Konnektivität zu

Microsoft Azure eingeschränkt ist. Diese temporären Daten enthalten keine Anzeigennamen, Benutzernamen, E-Mail-Adressen, Passwörter oder andere sensible Informationen.

Alle vom Agenten gesammelten Daten werden verschlüsselt, von der lokalen Zwischenspeicherung bis zur erfolgreichen Übertragung an unsere SaaS-Plattform. Dies umfasst die lokale Pufferung, die Übertragung und die Speicherung im Ruhezustand.

TrueDEM Teams-Plugin

Plugin, das als Teil des TrueDEM-Agenten installiert ist und während Anrufen aktiv Metriken aus dem Teams-Client abruft:

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

Bestimmungen zur Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit

OfficeExpert TrueDEM erkennt und sammelt zwei Arten von Informationen:

- **Kerndaten:** Anonymisierte Telemetriedaten, die keine persönlich identifizierbaren Informationen enthalten.

- **Privilegierte Daten:** Daten, die potenziell Daten enthalten können, die unter Datenschutzgesetze oder Unternehmensrichtlinien fallen.

Die folgenden privilegierten Daten werden, je nach gewählten Einstellungen, gesammelt:

- **Benutzeranzeigennamen, Benutzer-E-Mail-Adressen und UPN**
  Diese werden gesammelt, um Berichte in Benutzeroberflächen zu unterstützen. Beispielsweise kann dies Ihrem Helpdesk ermöglichen, Daten zu einem bestimmten Benutzer zu identifizieren. Dies ist eine reine Cloud-Funktion, der Agent hat keinen Zugriff auf diese Informationen.
- **IP-Adressen**
  Diese werden in öffentliche und interne/private kategorisiert. Sie können verwendet werden, um zu ermitteln, wo sich Personen befinden, beispielsweise wenn Sie die Adressbereiche Ihrer Bürostandorte kennen. Für jede können Sie wählen, ob die ursprüngliche Adresse gespeichert oder durch einen kryptografischen Hash ersetzt wird.
- **Hostnamen**
  Die Hostnamen der Benutzergeräte, um den Helpdesk zu unterstützen.
- **Wi-Fi-Netzwerkinformationen**
  Zur Identifizierung von Netzwerk- und Leistungsproblemen. Dazu gehören Daten wie die SSID.
- **Microsoft Teams Anwesenheitsverlauf und Anrufaufzeichnungen**
  Metadaten über die Nutzung von Microsoft Teams für Ihre Analysen, Berichte und den Helpdesk.
- **Standortinformationen**
  Wird für Analysen, Berichte und Helpdesk-Aktivitäten verwendet. Diese Daten können auf der genauesten Ebene gespeichert oder durch eine kreisförmige Referenz ersetzt werden, die den Standort auf etwa 160 km genau annähert.

Daten auf Clients:

Wie bereits erwähnt, kann der lokale TrueDEM-Agent nicht privilegierte Informationen lokal speichern sowie Installations-, Leistungs- und Ereignisprotokolle. Alle vom Agenten gesammelten Daten werden von der Erfassung bis zur erfolgreichen Übertragung auf unsere SaaS-Plattform verschlüsselt. Dazu gehört die In-Memory-Speicherung, die Übertragung und die Speicherung im Ruhezustand.

Die Logs werden gespeichert unter

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

und nach 7 Tagen überschrieben. Sie enthalten FEHLER- und WARN-Meldungen, einschließlich Zeitstempeln mit grundlegender Ereignisbeschreibung.

Verwaltungsdaten:

panagenda protokolliert und speichert erfolgreiche und fehlgeschlagene OfficeExpert TrueDEM-Manager-Installationen innerhalb von Azure AppInsights. Protokolle werden für 30 Tage gespeichert.

Verfügbarkeit:

panagenda wird sicherstellen, dass die SaaS-Lösung dem Kunden mindestens 99% der Betriebszeit des jeweiligen Azure-Datacenter-Uptime während eines Kalenderjahres zur Verfügung steht, ausgenommen geplante und im Voraus kommunizierte Wartungsfenster.

Authentizität:

Die Daten des Kunden werden sicher von den Endgeräten der Benutzer an die dedizierte OfficeExpert TrueDEM-Instanz gesendet. Der TrueDEM-Agent initiiert eine Verbindung zum Autoconfig-Dienst unter Verwendung des Tokens des Endbenutzers, um die spezifische TrueDEM-Konfiguration abzurufen. Dies stellt sicher, dass die Daten der Endbenutzer an die richtige Instanz geleitet werden. Folglich ist der Datenfluss exklusiv und sicher, da jeder EventHub nur mit seiner entsprechenden Kundendatenbank interagiert. Anschließend bittet der TrueDEM-Agent den SaaS-Anbieter, eine Verbindung zum EventHub herzustellen.

Integrität:

Sie vertrauen uns sehr sensible Informationen an. Deshalb wurde unser Service von Grund auf mit der Sicherheit Ihrer Daten im Hinterkopf entwickelt:

- Alle Daten werden während des Transports und im Ruhezustand unter Verwendung modernster Technologie verschlüsselt.
- Sensible Daten können an der Quelle obfuskiert werden. IP-Adressen können durch einen kryptografischen Hash ersetzt und geografische Standorte auf ungefähre Standorte reduziert werden.
- panagenda trennt die Daten in Kerndaten, die keine persönlich identifizierbaren Informationen enthalten, und privilegierte Daten, die möglicherweise persönlich identifizierbare Informationen enthalten. Jede wird separat gespeichert.
- Die privilegierten Daten jedes Kunden werden getrennt von allen anderen gespeichert und durch kundenspezifische Schutzmaßnahmen geschützt.
- Sie können wählen, jeglichen Zugriff auf privilegierte Daten zu verhindern – auch durch panagenda.

- Sie entscheiden, wer in Ihrer Organisation mit Hilfe des Microsoft Entra ID des Kunden Zugriff auf die Daten erhält.
- panagenda folgt den bewährten Sicherheitspraktiken für Cloud-Implementierungen, wie sie von Microsoft empfohlen werden.
- Der Zugang zu unseren Systemen ist streng kontrolliert und auf Mitarbeiter und vertrauenswürdige Partner beschränkt, die absolut Zugang zu ihnen benötigen.
- Mitarbeiter und vertrauenswürdige Partner unterzeichnen strenge Vertraulichkeits- und Datenschutzvereinbarungen und absolvieren regelmäßige Schulungen zu Sicherheit und Datenschutz.

Vertraulichkeit:

Um unsere Betriebsabläufe zu erleichtern, nutzen wir die Cloud-Infrastruktur von Anbietern wie Microsoft. Die Datenschutzrichtlinie von Microsoft finden Sie hier: https://azure.microsoft.com/en-us/support/legal/

Die Gerichtsbarkeit kann von Ihnen gewählt werden. Derzeit stehen folgende Optionen zur Verfügung:

- Vereinigte Staaten von Amerika (USA)
- Europäische Union (EU)

Nach der Erfassung werden die Daten an den gewählten Standort übertragen und dort gespeichert. Sowohl Kerndaten als auch privilegierte Daten verbleiben am gewählten Standort, es sei denn, eine Übertragung an einen anderen Standort wird von Ihnen angefordert.

Mit panagenda verbundene Unternehmen haben unter dem Schutz der Datenschutzrichtlinie von panagenda Zugriff auf die Daten aus den Gerichtsbarkeiten, in denen sie tätig sind, für die oben beschriebenen Zwecke. Der Kunde hat Zugriff auf die Daten aus den Gerichtsbarkeiten, in denen seine Organisation tätig ist.

Für jegliche Übertragung von Daten über Gerichtsbarkeiten hinweg implementieren wir geeignete Lösungen, wie gesetzlich vorgeschrieben (z.B. Standardvertragsklauseln gemäß Artikel 5 DSGVO).

Kerndatenverarbeitung:

Nicht privilegierte vollständig anonymisierte Daten können von panagenda verwendet werden, um Trends zu erkennen und allgemeine Microsoft-Verfügbarkeitsinformationen bereitzustellen. Diese Daten sind in keiner Weise auf eine Person oder Organisation zurückführbar.

Software von Drittanbietern:

panagenda OfficeExpert TrueDEM verwendet Software von Drittanbietern gemäß Art. 6(1)-Punkt f DSGVO auf der Grundlage unseres berechtigten Interesses an der Verbesserung der Stabilität und Funktionalität unseres Software-as-a-Service-Angebots. Die Daten werden nicht weitergegeben oder in anderer Weise genutzt. Wir behalten uns jedoch das Recht vor, die Server-Logdateien nachträglich zu überprüfen, falls konkrete Hinweise auf eine rechtswidrige Nutzung vorliegen.

Vereinbarte Service-Level

Die aktuelle Version der allgemeinen Lizenz- und Wartungsbedingungen von panagenda finden Sie hier: https://www.panagenda.com/legal

Serviceverfügbarkeit und SLA

panagenda stellt sicher, dass die SaaS-Lösung dem Kunden mindestens 99% der Zeit der jeweiligen Verfügbarkeit des Azure-Rechenzentrums im Kalenderjahr zur Verfügung steht, ausgenommen geplante und im Voraus kommunizierte Wartungsfenster.

Überwachung und Berichterstattung

Überwachung und Berichterstattung über die Betriebszeit, Nutzung und Leistung der Umgebung erfolgen durch die panagenda OfficeExpert TrueDEM Unternehmensanwendung.

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 erreichen.

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 des geringsten Privilegs auf seine IKT-Umgebung angewendet, um die Zugriffssicherheit zu gewährleisten. Wir haben auch einen robusten, aber leichten Secure Software Development Life Cycle (SSDLC) als Teil unserer ISO 27001:2022-Strategie etabliert.

Daten und Anwendungen werden in Microsoft Azure-Rechenzentren gespeichert. Informationen zur Sicherheit von Microsoft Azure-Rechenzentren finden Sie hier: https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security

Unsere Kunden sind vollständig verantwortlich für die sichere Bereitstellung des panagenda OfficeExpert TrueDEM Agents.

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 Recht auf Kündigung gemäß den DORA-Anforderungen. Da panagenda OfficeExpert TrueDEM als Dienstleistung angeboten und von panagenda betrieben wird, ist eine Mindestkündigungsfrist von 60 Tagen vor dem Verlängerungsdatum 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 die Information über die neuesten Bedrohungen, Schwachstellen und regulatorischen Änderungen.

Lernen nach Vorfällen

Nach jedem Vorfall im Zusammenhang mit panagenda OfficeExpert TrueDEM 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.