Planisware

Stand: 12. Februar 2026

ANHANG II – SICHERHEITSMASSNAHMEN

Dieser Anhang stellt die Architektur, die Infrastruktur sowie die Sicherheitsrichtlinien und -standards der Planisware-Lösungen dar, die alle für SaaS-Services gelten. Die Sicherheitsmaßnahmen, die auch für On-Premise-Produkte gelten, sind in einem eigenen Abschnitt am Ende dieses Anhangs ausdrücklich aufgeführt. Zur Vermeidung von Zweifeln gelten Bestimmungen, die nicht ausdrücklich als auch für On-Premise-Produkte anwendbar gekennzeichnet sind, ausschließlich für SaaS-Services.

BESTIMMUNGEN, DIE NUR FÜR SAAS-PRODUKTE GELTEN

1. LÖSUNGSARCHITEKTUR

MANAGEMENT DER RECHENZENTREN

Planisware besitzt und verwaltet die physischen Komponenten im Zusammenhang mit seinem Planisware-SaaS-Service in Rechenzentren. Die Rechenzentren von Planisware werden als „Planisware Ping Power Pipe“- oder „4P“-Rechenzentren bezeichnet, die Fernzugriff zu Servern, Stromversorgung und Internetverbindungen bieten.

Planisware nutzt private Flächen in Host-Colocation-Zentren, die eine physische Umgebung und grundlegende Dienstleistungen bereitstellen, wie zum Beispiel:

- Verwaltung der physischen Sicherheit (Perimeter-Sicherheit, physische Zugangskontrolle)
- Energieversorgung
- Klimatisierung
- Verwaltung der Netzwerkverbindungen zwischen den Planisware-Computerarrays
- Bereitstellung von WAN-Verbindungen (Internetzugang, spezialisierte Verbindungen)

Planisware 4P ermöglicht die allgemeine Serververwaltung und die direkte Bereitstellung aller SaaS-Services durch Planisware.

Kunden können wählen, an welchem der von Planisware angebotenen Standorte ihre Daten gespeichert werden sollen. Standardmäßig werden die Daten wie folgt gespeichert:

Standort des Kunden	Datenspeicherung
Europa	Europäische Union
Schweiz	Schweiz
Afrika	Europäische Union
Naher Osten	Schweiz
Vereinigte Staaten	Vereinigte Staaten
Asien	Singapur
Sonstige	An einem von Planisware ausgewählten Standort und in Übereinstimmung mit allen geltenden Gesetzen zum Schutz von personenbezogenen Daten

Die Rechenzentren sind nach SSAE16 und/oder ISO 27001 zertifiziert. Die Lösungen werden von Vollzeit-Ingenieuren vor Ort betreut und rund um die Uhr an 365 Tagen im Jahr durch geprüftes Sicherheitspersonal, Zugangskontrollen mittels Ausweis/Lichtbildausweis, biometrische Zugangskontrollen, Bewegungssensoren und Alarme bei Sicherheitsverletzungen geschützt. Der Zugang zu Server-Systemen ist ausschließlich über interne IPSec-VPNs von Planisware möglich. Zusätzlich zum VPN verfügen autorisierte Mitarbeiter von Planisware über Netzwerk- und Anmeldedaten für den Zugang zu Produktionsserver-Systemen.

ENDBENUTZER-GERÄTE UND DATENAUSTAUSCH

Der Datenverkehr zwischen Planisware-Servern und externen Systemen wird je nach Unterstützung der Verschlüsselungssuiten durch den Browser des Endbenutzers mittels TLS (HTTPS) verschlüsselt. Planisware unterstützt Site-to-Site-IPsec-VPNs für die Integration mit externen Systemen auf gemeinsam genutzten Netzwerkgeräten und bietet AES-256-Verschlüsselung für Data-in-Transit zwischen Standorten.

2. SICHERHEITSMASSNAHMEN

SICHERHEIT IM PERSONALBEREICH

Ein oberflächlicher Hintergrundcheck ist Teil des Einstellungsprozesses bei Planisware. Vorbehaltlich der vor Ort geltenden Gesetze kann Planisware weitere Hintergrundchecks durchführen. Alle Mitarbeiter werden regelmäßig in Sicherheitsmaßnahmen und -verfahren geschult.

IP-BASIERTE ZUGRIFFSBESCHRÄNKUNG

Sofern in den Kommerziellen Bedingungen oder einer speziellen Bestellung festgelegt, kann der Zugang des Kunden zu der Anwendung auf Firewall-Ebene verwaltet werden, um den Kreis der Endbenutzer, die auf die Anwendung zugreifen können, auf ein bestimmtes IP-Subnetz zu beschränken.

VERSCHLÜSSELUNG

Planisware verwendet kryptografische Algorithmen, die der Sensibilität der zu schützenden Daten, den jeweils geltenden Vorschriften zur Verschlüsselung der einzelnen Länder sowie den Empfehlungen staatlicher Sicherheitsbehörden entsprechen.

Data-in-Transit

Der Webdatenverkehr zwischen Endbenutzern und Servern wird je nach Unterstützung der Verschlüsselungssuiten durch den Browser des Endbenutzers mittels TLS (HTTPS) verschlüsselt.

Der Dateiaustausch mit externen Systemen kann ebenfalls mit PGP oder gemäß anderen vom Kunden gewünschten Standards verschlüsselt werden. Für nicht sichere Protokolle unterstützt das Planisware SaaS-Produkt Site-to-Site-IPsec-VPN zur Integration mit externen Systemen.

Data-at-Rest

Planisware bietet zwei Stufen der Verschlüsselung der Daten. Die Verschlüsselung von Datenbankpartitionen ist die Standardeinstellung unserer SaaS-Plattform:

- Die Datenbankdatei wird auf einer Partition mit Verschlüsselung gemountet.
- Die Verschlüsselung und Entschlüsselung der Partition erfolgen durch Planisware beim Start der Anwendung.

- Der Schlüssel für die Verschlüsselung befindet sich ausschließlich im Arbeitsspeicher des Planisware-Servers und wird niemals auf der Festplatte des Anwendungsservers gespeichert, sodass es unmöglich ist, die Partition zu entschlüsseln, wenn der Planisware-Server angehalten wird.
- Der Schlüssel wird verschlüsselt und von einem Schlüsselserver, der sich in einem anderen Rechenzentrum befindet, mit dem Anwendungsserver ausgetauscht.
- Die Verschlüsselung der Datenbankpartition erfolgt mittels symmetrischer AES-XTS-Verschlüsselung mit einer Schlüsselgröße von 512 Bit.

Verschlüsselung der Daten in der Datenbank: Je nach Verwendung der Attribute in der Datenbank erfolgt die Verschlüsselung entweder mit symmetrischer AES-ECB-Verschlüsselung mit einer Schlüsselgröße von 256 Bit oder mit symmetrischer AES-CBC-Verschlüsselung mit einer Schlüsselgröße von 128 Bit.

ZUGRIFFSPROTOKOLLIERUNG

Planisware führt eine mit Zeitstempeln versehene Protokolldatei über die folgenden Aktivitäten:

- Wenn ein Endbenutzer verbunden ist
- Von Endbenutzern besuchte Seiten der Anwendung

Von Endbenutzern vorgenommene Aktualisierungen der Kundendaten werden ebenfalls nachverfolgt und stehen für forensische Analysen zur Verfügung. Kunden können zudem durch die Konfiguration von Protokollen in der Anwendung ihren eigenen Audit-Trail erstellen. Auf diese Weise können sie Berichte in Echtzeit verfolgen und abrufen, z. B. wer ein bestimmtes Attribut wann geändert hat.

Zusätzlich können Kunden Workflows in der Anwendung konfigurieren, die sicherstellen, dass wichtige Datenaktualisierungen durch einen RACI-definierten Genehmigungsprozess kontrolliert werden.

DATENTRENNUNG

Unsere Planisware-SaaS-Lösungen nutzen eine Kombination aus verschiedenen Komponenten, darunter eine PostgreSQL-Datenbank, einen Apache-Webserver und das Betriebssystem Linux. Planisware SaaS ist eine Single-Tenant-Lösung. Kundendaten werden durch folgende Maßnahmen isoliert und von einem Kunden zum anderen getrennt:

- Dedizierte VM(s), die alle Komponenten enthalten
- Eine dedizierte Datenbank mit dedizierten Zugangsdaten
- Ein dediziertes VLAN

FUNKTIONSTRENNUNG

Planisware folgt dem Prinzip der Funktionstrennung und erstellt abhängig von Rolle und Verantwortungsbereich ein Endbenutzerprofil. Die Produktionsumgebung des Kunden ist nur zugänglich für:

- das Incident Response Team (ohne Zugang zu Kundendaten),
- Support-Team, um ein Problem zu bearbeiten (ohne Zugriff auf Kundendaten, sofern nicht anderweitig vom Kunden autorisiert),
- der Planisware Delivery Manager, um eine Änderung wie vom Kunden gewünscht in der Produktionsumgebung zu übernehmen
- der Technical Delivery Manager (ohne Zugang zu den Kundendaten), für die Serverkonfiguration
- die Planisware-Systemadministratoren, falls erforderlich, um unerwartete schwerwiegende Vorfälle zu bewältigen.

Diese Zugangsberechtigungen werden regelmäßig überprüft und jede Erstellung, Erweiterung oder Aufhebung werden in einem Ticketingsystem verfolgt.

SCHUTZ VOR VIREN UND MALWARE

Es wurde ein mehrschichtiger Sicherheitsansatz nach dem Prinzip der „Defense in Depth“ implementiert:

- Kundenumgebungen befinden sich auf Linux-Servern mit einem Antivirenprogramm.
- Auf den Planisware-Workstations, die Zugang zu Planisware SaaS haben, ist ein Antivirenprogramm installiert.
- Im Rahmen des Alarm- und Vorfallmanagementprozesses werden Malware-Risiken regelmäßig überwacht.
- Planisware trennt Infrastruktur und Anwendungen voneinander. Firewalls filtern die Kommunikation zwischen Komponenten in verschiedenen Zonen. Alle Komponenten werden regelmäßig aktualisiert und überwacht, um sicherzustellen, dass sie auf dem neuesten Update-Stand sind.

SOFTWARE- UND SYSTEM-PATCHES

Kundenumgebungen erhalten automatische Linux-Updates für Betriebssystem-Sicherheitspatches. Im Rahmen des Alarm- und Vorfallmanagementprozesses überprüfen der Chief Information Security Officer (CISO), die Asset-Manager und der Infrastrukturmanager für Planisware SaaS regelmäßig die Sicherheitsrisiken und stützen sich dabei auf die folgenden Sicherheitswarnungen:

- Vom CERT-FR (ANSSI), CERT-US;
- Von Herausgebern, Entwicklern und Subunternehmern;
- Von den Administratoren erkannt (über Ereignisse in Protokollen und Warnmeldungen des Planisware SaaS-Infrastrukturteams);
- Von Cybersicherheitsbehörden, Verbänden und Medien;
- Veröffentlicht von den Rechenzentrumsanbietern von Planisware SaaS Hosting;
- Identifiziert während der Ausführung des Sicherheitskontrollplans.
- Identifiziert während der Durchführung externer Audits

Nach der Ermittlung und Bewertung der Risiken, die sich aus dem Überwachungs- und Warnsystem ergeben, werden Sicherheitspatches so schnell wie möglich (nach Validierung des Aktionsplans) angewendet oder je nach Schweregrad des Risikos bereitgestellt.

NETZWERKSICHERHEIT

Planisware konfiguriert die gesamte Netzwerkinfrastruktur nach dem Prinzip des „Least Access“, indem Filter integriert werden, die nur den minimal erforderlichen Datenverkehr zulassen. Die gesamte Kommunikation zwischen dem Webserver und den Clients über das Internet wird je nach Unterstützung der Verschlüsselungssuiten durch den Browser des Endbenutzers mittels TLS verschlüsselt.

Planisware SaaS nutzt:

- Ausschließlich sichere Protokolle (HTTPS, SFTP, IPSec)
- Überwachung von HTTP-Anfragen durch eine Web-Application-Firewall
- Überwachung der Firewall-Protokolle für eingehende und ausgehende Netzwerkdaten
- Ein Intrusion Detection System (IDS) zur Überwachung und Blockierung von böswilligem Datenverkehr und Angriffen auf den Netzwerkverkehr.

3. DATENSICHERUNG

Unser Standard-SaaS-Service von Planisware umfasst Backups ausschließlich für die Produktionsumgebung des Kunden. Die Services zur Daten-Sicherung sind in der folgenden Tabelle beschrieben.

Zu sichernde Daten/Umfang	Häufigkeit	Aufbewahrungsregeln	Sicherungstyp	Schutzmaßnahmen	Standort	Verantwortlicher	Externe Speicherung
Sicherung der Datenbank für Kunden	Täglich	Standardmäßig: • Letzte 10 Tage • Letzte 6 Wochen (jeweils am 1. Tag der Woche) • Letzte 6 Monate (1. Tag jedes Monats) Option(en): je nach Kundenwunsch	Vollständig	Verschlüsselter Dump Verschlüsselte Übertragung	Datenbank-Backup-Plattform der Kundenumgebungen	Planisware	Ja
Vollständige Sicherung der virtuellen Maschine	Tägliche inkrementelle Sicherung	Mindestens 15 Tage (Mindestaufbewahrungsfrist)	Inkrementell	Verschlüsselung	NAS	Planisware	Ja

Standardmäßig wird gemäß dem oben beschriebenen Backup-Prozess täglich eine Sicherung der Kundendaten vor Ort und an einem externen Standort erstellt. Im Falle einer Katastrophe am Hauptstandort wird zunächst die Infrastruktur des Hauptstandorts wiederhergestellt, anschließend die Umgebung. Zusätzlich zur täglichen Sicherung der Produktionsumgebungen können Kunden gegen Aufpreis eine Warm-Backup-Option hinzufügen, bei der eine Kopie der Umgebung und der Datenbank extern in einer passiven Umgebung repliziert und in Bereitschaft gehalten wird. Im Falle einer Katastrophe am Hauptstandort kann der passive Standort mit nur begrenzter Unterbrechung der Services aktiviert werden.

4. BETRIEBSKONTINUITÄTS- UND NOTFALLWIEDERHERSTELLUNGSPLAN

Der Business-Continuity-Plan (BCP) von Planisware befasst sich mit:

- Auswirkungen auf Geschäftsprozesse,
- Aktivierungsschwellen,
- die organisatorischen Rollen und Funktionen der Einsatzkräfte (Mitglieder der Kriseneinheit),
- Interne und externe Kommunikationspläne,
- Betriebsgrundsätze im Notfallmodus,
- Rückkehr zum Normalbetrieb.

Der BCP von Planisware umfasst sowohl die Verfahren des IT-Backup-Plans als auch den Disaster-Recovery-Plan (DRP).

5. SCHWACHSTELLENPRÜFUNG

SCHWACHSTELLEN-SCAN

Schwachstellen-Scans werden regelmäßig durchgeführt. Webseiten werden ausschließlich über das HTTPS-Protokoll bereitgestellt.

PENETRATIONSTESTS

Planisware beauftragt ein unabhängiges Sicherheitsprüfungsunternehmen mit der Durchführung von Penetrationstests einmal jährlich. Zertifikate über die jährlichen Penetrationstests sind auf Anfrage erhältlich.

ANWENDUNGSSICHERHEITSTESTS – GILT AUCH FÜR ON-PREMISE-PRODUKTE

OWASP-Anwendungssicherheitsrisiken werden überprüft, bewertet und in die Testsuiten von Planisware aufgenommen.

BESTIMMUNGEN FÜR ON-PREMISE-PRODUKTE UND SAAS-PRODUKTE

IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG VON ENDBENUTZERN

Endbenutzerkonten werden direkt vom Kunden innerhalb unserer Lösung verwaltet. Innerhalb der Anwendung kann der Administrator des Kunden jedem Endbenutzer ein spezifisches Profil und eine Berechtigungsstufe zuweisen, die den Zugang zu Modulen, Funktionalitäten und Daten definiert. Die Authentifizierung muss vom Kunden über Single Sign-On (SSO) verwaltet werden, wobei der webbasierte Authentifizierungsstandard SAML 2 oder Open ID Connect (OIDC) genutzt wird.
Für Systemkonten, beispielsweise zur Anbindung an externe Systeme, werden Passwörter unter Verwendung eines Verschlüsselungsalgorithmus gespeichert. Bei Verwendung von SSO werden die Passwörter der Endbenutzer weder in der Lösung gespeichert noch verwaltet.

PROFILBASIERTE ZUGRIFFSKONTROLLE

Sobald ein Endbenutzer authentifiziert ist, wird der Zugang zu der Anwendung durch mehrstufige Autorisierungs-Zugriffsebenen weiter eingeschränkt. Der Zugang wird anhand der folgenden Dimensionen definiert:

- Pro Modul, basierend auf dem Profil des Endbenutzers
- Pro Bildschirm innerhalb eines Moduls, basierend auf dem Profil des Endbenutzers
- Für jedes Feature innerhalb des Moduls, basierend auf dem Endbenutzerprofil
- Nach Datenelement, basierend auf dem Endbenutzerprofil UND/ODER spezifischen Benutzerregeln

Benutzerprofile ermöglichen eine Aufgabentrennung auf Anwendungsebene. Sie können in der Anwendung von einem Kunden-Business-Administrator erstellt, aktualisiert und verwaltet werden. Änderungen an einem bestimmten Endbenutzerprofil werden automatisch auf alle Endbenutzer mit diesem Profil übertragen.

Planisware

Stand: 12. Februar 2026

AUDITS

Die Rechenzentren und sonstigen Standorte von Planisware sind nach ISO 27001 oder SOC 2 Typ II zertifiziert. SOC 1/SOC 2-Berichte und das ISO 27001-Konformitätszertifikat sind in der Regel zu Beginn jedes Kalenderjahres verfügbar. Planisware kann solche Zertifikate auf begründete Anfrage des Kunden zur Verfügung stellen.

INTERNE RICHTLINIEN

Planisware hat ein Informationssicherheits-Managementsystem (ISMS) gemäß ISO 27001:2013 implementiert. Dieser Ansatz konzentriert sich auf:

- die Definition und Kommunikation klarer Sicherheitsziele,
- Sensibilisierung der Planisware-Mitarbeiter für Sicherheitsfragen,
- Schaffung eines Rahmens für das Sicherheitsmanagement,
- Anwendung eines Risikomanagement-Rahmens,
- Überwachung der Wirksamkeit von Sicherheitsmaßnahmen durch interne und externe Audits,
- Schaffung eines Rahmens zur Verwaltung von Sicherheitswarnungen und zur Reduzierung von Sicherheitsvorfällen.

EINHALTUNG DER DATENSCHUTZVORSCHRIFTEN

Wenn festgestellt wird, dass der Kunde Endbenutzer innerhalb des Europäischen Wirtschaftsraums hat, verlangt Planisware die Unterzeichnung seines Vertrags zur Datenverarbeitung, der die Verarbeitung der personenbezogenen Daten dieser Endbenutzer regelt, einschließlich der Unterzeichnung der Standardvertragsklauseln der EU-Kommission. Für die Verarbeitung von Daten betroffener Personen in anderen Rechtsordnungen werden bei Bedarf zusätzliche Verträge zur Datenverarbeitung geschlossen (z. B. Kalifornien, Brasilien). Auf Anfrage ist es möglich, für bestimmte Gruppen von Endbenutzern Regeln für Datenschutzzonen einzurichten. Personenbezogene Daten werden für alle Endbenutzer, die nicht derselben Datenschutzzone angehören, in Echtzeit verschlüsselt.

Der Datenschutzbeauftragte (DSB) von Planisware ist unter dpo@planisware.com erreichbar.