Sicherheit und Datenschutz – Übersicht für IT-Fragebögen

Stand: November 2026. Beschreibt den Stand der Software. Angaben zum Betrieb in der Plica-Cloud gelten erst, wenn der Server in Betrieb ist; beim Betrieb auf dem Firmenserver verantwortet der Kunde Rechenzentrum, Netz und Sicherung.

1. Betriebsarten

	Plica-Cloud	Firmenserver
Standort	Rechenzentrum in Deutschland (geplant: Hetzner, Nürnberg)	beim Kunden
Trennung der Kunden	eigene Instanz (eigener Container, eigene Datenbank, eigenes Volume) je Kunde	nicht relevant
Verantwortung Betrieb	Plica (Auftragsverarbeiter)	Kunde
Datenübermittlung an Plica	nur im Rahmen des AVV	keine

2. Technische und organisatorische Maßnahmen (TOMs, Art. 32 DSGVO)

Zugangskontrolle

- Anmeldung mit Firmenkonto (OpenID Connect, z. B. Microsoft Entra ID) oder Passwort.
- Passwörter: PBKDF2-SHA256, 200.000 Iterationen, individueller Salt; Mindestlänge 12; Sperre nach 5 Fehlversuchen für 15 Minuten.
- Zwei-Faktor-Anmeldung mit Authenticator-App (TOTP nach RFC 6238), auf Wunsch für die ganze Organisation verpflichtend; acht Einmal-Wiederherstellungscodes, nur als Prüfsumme gespeichert.
- Sitzungen enden nach 12 Stunden Inaktivität; Cookie nur per HTTPS, nicht per Skript lesbar, nur für die eigene Firmenadresse gültig. Sitzungen werden in der Datenbank nur als Prüfsumme gespeichert – ein Datenbankabzug enthält keine nutzbaren Sitzungen.
- Begrenzung der Anfragen je Absender für Anmeldung, Passwort-Links, Registrierung und Formulare (Schutz gegen Durchprobieren von Passwörtern).
- Optional: Passwort-Anmeldung abschalten (nur Firmenkonto), Notzugang für Admins.

Schutz der Anwendung

- Strenge Content-Security-Policy: Der Browser führt nur Skripte von der Plica-Adresse selbst aus, keine fremden Quellen, keine eingeschleusten Skripte; Einbetten in fremde Seiten ist gesperrt.
- Weitere Sicherheits-Header (kein MIME-Sniffing, Referrer-Begrenzung, Berechtigungen für Standort und Mikrofon gesperrt, HSTS).
- Größenbegrenzung für Uploads; Dateien werden als Daten gespeichert, nie ausgeführt.
- Zahlungsdaten (Karte, Konto) gehen ausschließlich an den Zahlungsdienstleister Stripe (PCI DSS Level 1); Zahlungsmeldungen werden per Signatur geprüft.

Zugriffskontrolle

- Rollen: Admin, Bearbeiter, Prüfer, Freigeber, Leser; Gäste nur über persönliche Links, die an eine Freigabe bzw. einen Versand gebunden sind.
- Rechte werden serverseitig bei jeder Anfrage geprüft.

Weitergabekontrolle

- Transport ausschließlich verschlüsselt (HTTPS/TLS, HSTS).
- Versand von Plänen nur über persönliche Links mit Empfangsbestätigung und Protokoll.

Eingabekontrolle

- Jede Aktion wird mit Zeit, Person und Details protokolliert; das Protokoll ist verkettet (jede Zeile enthält die Prüfsumme der vorherigen), nachträgliche Änderungen sind erkennbar.
- Metadaten-Änderungen mit altem und neuem Wert.

Integrität

- Jeder Planstand wird unveränderlich mit SHA-256-Prüfsumme gespeichert; nichts wird überschrieben.
- Freigabeprotokolle enthalten Prüfsummen von Datei und freigegebenem PDF.

Verfügbarkeit

- Tägliche Sicherung von Datenbank und Dateien (Skript mitgeliefert), Aufbewahrung 30 Tage; Wiederherstellung dokumentiert.

Trennungsgebot

- In der Plica-Cloud eine eigene Datenbank und ein eigener Dateibereich je Kunde, erreichbar nur unter der eigenen Adresse (z. B. `ihr-buero.getplica.de`). Es gibt keine gemeinsame Kundendatenbank; Zwischenspeicher sind je Kunde getrennt.
- Auf Wunsch: eigener Server im Firmennetz (Firmenserver-Paket).

KI

- KI-Funktionen sind standardmäßig ausgeschaltet. Es werden keine Plandaten an KI-Dienste übermittelt. Eine spätere Nutzung erfolgt nur nach ausdrücklicher Freischaltung durch den Kunden und über einen Anbieter mit Rechenzentrum in der EU.

3. Elektronische Signatur

Freigaben erfolgen als einfache elektronische Signatur nach eIDAS-Verordnung (EU) Nr. 910/2014: Identifikation über den persönlichen E-Mail-Link, Protokoll mit Zeit, IP-Adresse, Browser und Prüfsummen. Für fortgeschrittene oder qualifizierte Signaturen ist die Anbindung eines zertifizierten Vertrauensdienstes vorgesehen.

4. GMP

Plica bietet Grundlagen, die für den Einsatz in GMP-Umgebungen nötig sind (Audit-Trail, unveränderliche Stände, Rollen, elektronische Freigabe). Eine Validierung nach EU-GMP Annex 11 bzw. 21 CFR Part 11 ist nicht Bestandteil des Standardumfangs und wird mit dem Kunden projektbezogen vereinbart.

5. Noch offen (ehrliche Liste)

- Externer Penetrationstest – vor dem ersten Produktivbetrieb geplant.
- Verschlüsselung der gespeicherten Daten auf Anwendungsebene – derzeit über die Festplattenverschlüsselung des Servers.
- Formale Zertifizierung (z. B. ISO 27001) – nicht vorhanden.