

Sicherheit & Datenschutz bei Portario

Hosting, Verschlüsselung, Zugriff, Sicherung und Datenflüsse – kompakt für IT-Leitung und Datenschutzbeauftragte. Inklusive der Punkte, die Portario nicht hat.

Für wen: IT-Leitung, Datenschutzbeauftragte und Geschäftsführung, die vor einer Entscheidung wissen wollen, wo die Daten liegen, wer darauf zugreifen kann und was im Ernstfall passiert. Dieses Dokument ist die Kurzfassung; die vertraglich verbindliche Beschreibung steht im Auftragsverarbeitungsvertrag (AVV), der auf Anfrage vorab bereitgestellt wird.

Dieses Dokument wird bei jeder neuen Version von Portario automatisch neu erzeugt und trägt Stand und Versionsnummer der laufenden Anwendung. Es ist damit nie älter als die Software, die es beschreibt.

Auf einen Blick

FRAGE	ANTWORT
Wo liegen die Daten?	In Deutschland: Hetzner Online GmbH, Rechenzentrum Falkenstein (Sachsen), ISO-27001-zertifiziert. Nur das optionale KI-Modul verarbeitet die jeweilige Anfrage in EU-Rechenzentren (AWS Bedrock, primär Frankfurt)
Wer betreibt Portario?	Ein deutscher Anbieter (Impressum auf portario.de), kein Wiederverkäufer, keine Zwischenschicht
Übertragung in Drittländer?	Nein. Auch das optionale KI-Modul läuft ausschließlich in EU-Rechenzentren
Verschlüsselung?	Durchgängig TLS/HTTPS mit HSTS; Passwörter nur als bcrypt-Hash; Datenbank von außen nicht erreichbar
Zwei-Faktor-Anmeldung?	Ja, je Benutzerkonto aktivierbar (TOTP, z. B. mit einer Authenticator-App); mit Schutzstufe für alle Konten Pflicht
Gesundheitsdaten (Art. 9 DSGVO)?	Schutzstufe „Besondere Kategorien“ je Organisation: 2FA-Pflicht, Support-Zugriff nur nach Ihrer Freigabe, KI nur nach ausdrücklicher Bestätigung, Löschfrist für Anhänge, Hinweis im Kundenportal – alles serverseitig erzwungen
Sicherung?	Täglich automatisch, 14 Tage Aufbewahrung, jede Sicherung wird auf Plausibilität geprüft; Wiederherstellung erprobt

FRAGE	ANTWORT
Verfügbarkeit?	Interne Überwachung alle 5 Minuten plus externe, vom Server unabhängige Messung; öffentliche Statusseite unter portario.de/status
Wer sieht meine Daten beim Anbieter?	Nur anlassbezogen über die Support-Konsole; jeder Zugriff wird protokolliert und ist zeitlich begrenzt; Änderungen tragen in Ihrem Verlauf das Etikett „via Support“, das Zugriffsprotokoll erhalten Sie auf Anfrage
Daten auf Handys und Laptops?	Standardmäßig nein. Optional „Offline für unterwegs“ (vom Administrator freizuschalten): dann AES-256-verschlüsselt auf dem Gerät, Schlüssel nur mit Anmeldung oder Offline-Kennwort, Löschung beim Abmelden und nach 14 Tagen ohne Verbindung
Tracking, Cookies, Werbenetzwerke?	Nein. Keine Analyse-Dienste Dritter, keine externen Schriften, kein Einwilligungsbanner nötig
AVV?	Liegt fertig vor und wird zum Start geschlossen, nicht nachgereicht
Was fehlt?	Kein ISO-27001-Zertifikat für Portario selbst, keine räumlich getrennte Zweitkopie der Sicherungen, keine Verschlüsselung der Datenträger. Steht im Abschnitt „Offen gesagt“

1. Hosting und Standort

Portario läuft auf einem eigenen Server bei der **Hetzner Online GmbH** (Gunzenhausen) im Rechenzentrum **Falkenstein, Sachsen**. Hetzner betreibt die Rechenzentren nach **ISO 27001**; Zutritt, Stromversorgung, Brandschutz und physische Sicherheit liegen beim Hoster.

Anwendung, Datenbank und Datei-Anhänge liegen auf diesem einen Server. Es gibt keine Verteilung auf mehrere Länder, keine Zwischenspeicher bei Dritten und keine Inhalte-Netzwerke (CDN). Wer portario.de aufruft, spricht direkt mit dem Server in Falkenstein.

2. Verschlüsselung und Netz

- **Transport:** Alle Verbindungen laufen über **TLS/HTTPS**. **Strict-Transport-Security** (HSTS) sorgt dafür, dass ein Browser Portario nach dem ersten Besuch nie mehr unverschlüsselt anspricht. Weitere Sicherheits-Kopfzeilen sind gesetzt: eine strikte **Content-Security-Policy**, **X-Content-Type-Options**, **Referrer-Policy**, **Permissions-Policy** und **X-Frame-Options**.
- **Netzabschottung:** Die Datenbank hat **keinen Netzwerk-Port nach außen**. Cloud-Firewall und Server-Firewall lassen ausschließlich SSH, HTTP und HTTPS zu. SSH ist nur mit Schlüssel möglich; die Passwort-Anmeldung ist abgeschaltet.
- **Geheimnisse:** Passwörter werden nie im Klartext gespeichert, sondern als **bcrypt-Hash**. Einmal-Token (Passwort zurücksetzen, E-Mail-Bestätigung) liegen nur als SHA-256-Hash vor. Konfigurationsdateien mit Zugangsdaten und die Sicherungen sind nur für den Dienstbenutzer lesbar (Dateirechte 0600).
- **Ruhezustand – offen gesagt:** Die Datenträger selbst sind **nicht verschlüsselt** (kein LUKS). Der Schutz beruht auf der Netz- und Zugriffsabschottung sowie der physischen Sicherung des Rechenzentrums.

- **Outlook-Add-In (seit 2.92.0):** Verbindet sich mit einem persönlichen Schlüssel, der nur für die Add-In-Schnittstelle gilt, nur als SHA-256-Hash gespeichert wird und einzeln widerrufbar ist; Passwortänderung, Deaktivierung und fehlende Pflicht-Zwei-Faktor-Anmeldung sperren ihn. Übertragen werden nur Mails, die eine Person aktiv ablegt – kein Mitlesen des Postfachs. Das Seitenfenster lädt Microsofts Office.js (Vorgabe für Outlook-Add-Ins); Daten fließen dabei nur zwischen Outlook und Portario.
- **Endgeräte (Offline für unterwegs, seit 2.91.0):** Standardmäßig speichert Portario keine Kundendaten auf Geräten. Schaltet ein Administrator den Offline-Betrieb frei, können Mitarbeitende ihr Gerät einrichten: Die Daten liegen dann **AES-256-verschlüsselt** im Browser-Speicher. Der Schlüssel ist nie im Klartext auf dem Gerät, sondern doppelt verpackt – mit einer Server-Hälfte, die es nur mit gültiger Anmeldung gibt, und mit einem Offline-Kennwort des Nutzers. Ein verlorenes Gerät gibt ohne Kennwort oder gültige Anmeldung nichts preis. Gelöscht wird beim Abmelden, nach 14 Tagen ohne Verbindung, nach 5 falschen Kennwort-Versuchen und beim Abschalten durch den Administrator. Geräteverschlüsselung und Bildschirmsperre des Geräts bleiben trotzdem Pflicht Ihrer Geräteverwaltung.

3. Zugang und Berechtigungen

- **Individuelle Konten:** Jede Person meldet sich mit eigenem Konto an. Sammelkonten sind nicht vorgesehen.
- **Zwei-Faktor-Anmeldung (TOTP):** Je Benutzerkonto aktivierbar, funktioniert mit jeder gängigen Authenticator-App.
- **Sitzungen:** Anmelde-Token sind auf **12 Stunden** begrenzt, danach ist eine neue Anmeldung nötig. Links zum Zurücksetzen des Passworts verfallen nach 30 Minuten.
- **Schutzstufe „Besondere Kategorien“ (Art. 9 DSGVO):** Für Organisationen, bei denen Gesundheitsdaten in Tickets landen können (z. B. Softwarehäuser mit Pflegeeinrichtungen als Kunden). Ein Administrator schaltet sie unter Administration → Datenschutz ein. Dann gilt: Zwei-Faktor-Anmeldung für jedes Konto, Support-Zugriff des Anbieters nur nach Freigabe (höchstens 24 Stunden), KI erst nach ausdrücklicher Bestätigung, Hinweis im Kundenportal, keine Gesundheitsdaten zu schicken. Unabhängig davon lässt sich eine Frist setzen, nach der Anhänge erledigter Tickets gelöscht werden. Alle Schalter stehen im Verlauf. Vertraglich regelt das eine eigene, anwaltlich geprüfte Anlage zum AVV (Anlage 4).
- **Drosselung:** Anmeldung, Kontaktformulare und andere missbrauchsanfällige Endpunkte sind je IP-Adresse bzw. Konto gedrosselt (Rate-Limiting), damit Passwort-Raten ins Leere läuft.
- **Rollen und Rechte:** Administrator, Teamleiter, Mitglied, Nur-Lesen. Dazu Bereiche und Sichtbarkeiten – auf Wunsch sieht ein Mitarbeiter nur seine eigenen Datensätze. **Alle Rechte werden serverseitig erzwungen**, nicht nur in der Oberfläche ausgeblendet.
- **Mandantentrennung:** Jede Organisation ist logisch strikt getrennt. Jede Datenbankabfrage ist an die Organisation des angemeldeten Benutzers gebunden – in zwei unabhängigen Schichten, und diese Trennung wird bei jeder Code-Änderung automatisch getestet (siehe Abschnitt 6).

4. Nachvollziehbarkeit

- **Änderungsverlauf:** Jede Änderung an einem Datensatz wird mit Zeitpunkt, Person, altem und neuem Wert festgehalten – lückenlos und für berechtigte Nutzer in der Anwendung einsehbar.
- **Änderungen an der Einrichtung:** Ändert jemand die Einrichtung Ihrer Organisation (Begriffe, Status, eigene Felder und Feldregeln, Module, Rollen, Benutzer, Anbindungen ...), hält Portario fest, wer das

wann getan hat und wie der Stand vorher und nachher war. Passwörter, Schlüssel und Zugangsdaten werden dabei nie gespeichert. Dieses Protokoll sieht unser Support, damit er bei einer Störung schnell findet, was sich geändert hat; auf Wunsch erhalten Sie die Einträge Ihrer Organisation. Es wird mit Ihrer Organisation gelöscht.

- **Papierkorb:** Gelöschtes wandert zuerst in den Papierkorb und lässt sich wiederherstellen. Endgültiges Löschen ist ein bewusster zweiter Schritt.
- **Support-Zugriff des Anbieters:** Portario greift auf Ihre Organisation nur anlassbezogen zu (z. B. auf Ihre Bitte hin bei einer Störung) – über eine eigene Support-Konsole, nicht mit Ihrem Konto. Jeder Zugriff wird **unveränderlich protokolliert** (wer, wann, als wen), die Sitzung endet automatisch nach **2 Stunden**, der Modus ist in der Anwendung sichtbar gekennzeichnet, und Änderungen aus einer solchen Sitzung tragen dauerhaft das Etikett „via Support“. Das Protokoll der Zugriffe auf Ihre Organisation erhalten Sie auf Anfrage. Klartext-Passwörter Ihrer Nutzer kennt der Anbieter zu keinem Zeitpunkt. Innerhalb der Support-Konsole gilt das Prinzip der geringsten Rechte: Support-Mitarbeiter dürfen nur Organisationen ansehen und im Kundenauftrag arbeiten; Organisationen anlegen, sperren oder löschen sowie Tarife und Zugänge verwalten kann allein der Betreiber. Die Einzelheiten stehen in § 5 des AVV.

5. Verfügbarkeit und Sicherung

- **Tägliche Sicherung:** Jede Nacht um 03:30 Uhr wird die Datenbank komplett gesichert (`pg_dump` , komprimiert) und jede Sicherung automatisch auf Plausibilität geprüft. Datei-Anhänge werden mitgesichert. Aufbewahrung: **14 Tage** rollierend.
- **Wiederherstellung erprobt:** Das Verfahren ist dokumentiert und wurde zuletzt am **13.08.2026** vollständig durchgespielt (Sicherung in eine separate Datenbank eingespielt und verifiziert). Es wird mindestens jährlich und nach wesentlichen Änderungen an der Datenhaltung wiederholt.
- **Überwachung:** Ein interner Erreichbarkeits-Check läuft alle **5 Minuten** und alarmiert per E-Mail bei jedem Zustandswechsel; er überwacht zusätzlich Plattenplatz und Arbeitsspeicher. Ergänzend misst ein **externer, vom Server unabhängiger Dienst** (UptimeRobot) die Erreichbarkeit von außen – der einzige Weg, einen Totalausfall der Maschine selbst zu erkennen.
- **Statusseite:** Unter portario.de/status steht jederzeit die gemessene Verfügbarkeit, laufende Störungen und angekündigte Wartungen. Bei einer Störung erscheint zusätzlich ein Hinweiskasten in der Anwendung selbst.
- **Ausrollen ohne Risiko:** Vor jeder neuen Version wird der laufende Stand gesichert; ein Rollback ist jederzeit möglich. Das Einspielen selbst unterbricht den Dienst nur für wenige Sekunden (Neustart des Anwendungsdienstes) und findet außerhalb der Geschäftszeiten statt.
- **Kapazität:** Der Server ist auf mehrere hundert gleichzeitige Nutzer ausgelegt und wird bei Bedarf innerhalb weniger Minuten vergrößert, ohne Umzug und ohne Code-Eingriff.

6. Entwicklung und Änderungen

- **Prüfkette bei jeder Änderung:** Kein Code geht live, ohne dass automatisch die Typprüfung, der komplette Testlauf – **einschließlich der Tests zur Mandantentrennung** –, eine Schwachstellenprüfung aller Abhängigkeiten (Abbruch bei hohem Schweregrad) und der vollständige Bau beider Anwendungen bestanden sind.
- **Transparenz:** Jede ausgelieferte Version hat eine Versionsnummer, und die Neuerungen sind für Ihre Nutzer direkt in der Anwendung nachzulesen.

- **Keine Fremdinhalte zur Laufzeit:** Die Anwendung lädt ausschließlich eigene Inhalte – keine externen Schriften, Skripte oder Bilder-Netzwerke. Das ist auch der Grund, warum die Content-Security-Policy so streng sein kann.

7. Datenflüsse und Unterauftragnehmer

EMPFÄNGER	ZWECK	STANDORT	DRITTLANDTRANSFER
Hetzner Online GmbH, Gunzenhausen	Server-Hosting, E-Mail-Versand (SMTP)	Deutschland (Falkenstein)	Nein
Nur bei aktiviertem KI-Modul: Amazon Web Services EMEA SARL, Luxemburg	KI-Assistent über Amazon Bedrock (Antwort-Entwürfe, Zusammenfassungen)	EU – ausschließlich EU-Regionen, primär Frankfurt	Nein

Weitere Unterauftragnehmer gibt es nicht – insbesondere keinen Zahlungsdienstleister, keine Cloud-Analyse und keine externen Schriftarten.

Zum KI-Modul: Es ist **optional** und nur aktiv, wenn Sie es in Ihrer Organisation einschalten. Ohne Aktivierung verlassen Ihre Daten das Rechenzentrum nicht. Ist es aktiv, werden nur die für die jeweilige Aktion nötigen Vorgangsinhalte übermittelt, nie Zugangsdaten. AWS sagt für Bedrock zu, Ein- und Ausgaben nicht zu speichern, nicht zum Training zu verwenden und nicht an den Modellanbieter weiterzugeben. Grundlage ist das AWS-GDPR- Datenverarbeitungsaddendum mit EU-Standardvertragsklauseln.

Von Ihnen eingerichtete Anbindungen: Webhooks, Zapier/Make, die Jira-Anbindung und die DMS-Anbindung (SharePoint, DocuWare) übermitteln Daten nur, wenn Sie sie selbst einrichten, und nur an das Ziel, das Sie eintragen (z. B. Ihr eigenes Jira oder Ihr eigenes DMS). Zugangsdaten dafür liegen verschlüsselt (AES-256-GCM). Diese Empfänger sind Ihre Dienstleister, nicht Unterauftragnehmer von Portario. Mit Schutzstufe „Besondere Kategorien“ überträgt die Jira-Anbindung keine Ticket-Beschreibung.

Auf der Website: Besuche werden cookieless und ohne Wiedererkennung gezählt (Tages-Hash, keine IP-Speicherung); die „Do Not Track“-Einstellung des Browsers wird respektiert. Deshalb gibt es kein Einwilligungsbanner.

8. Betroffenenrechte und Löschung

- **Auskunft (Art. 15 DSGVO):** Portario stellt die Auskunft zu einer Person als Datei zusammen – ein Knopf, kein Projekt.
- **Löschung (Art. 17):** Endgültiges Löschen bzw. Anonymisieren einer Person aus der Anwendung heraus; nicht nur ausblenden.
- **Aufbewahrungsregeln:** Fristen je Datenart lassen sich hinterlegen, damit Daten nicht länger liegen als nötig.
- **Datenübertragbarkeit:** Ihren gesamten Bestand exportieren Sie jederzeit selbst als CSV.
- **Vertragsende:** Auf Wunsch stellt der Anbieter den vollständigen Export bereit und löscht danach die Organisation samt aller Daten, Anhänge und Sicherungen nach Ablauf der Rotationsfrist. Das Verfahren ist in § 8 des AVV geregelt.

9. Offen gesagt: was Portario nicht hat

Ein Datenschutzbeauftragter findet diese Punkte ohnehin. Sie stehen deshalb hier, nicht im Kleingedruckten:

- **Kein ISO-27001-Zertifikat für Portario selbst.** Zertifiziert ist das Rechenzentrum des Hosters. Portario wird von einem kleinen Anbieter betrieben, nicht von einem Konzern mit Auditbudget.
- **Keine räumlich getrennte Zweitkopie der Sicherungen.** Die Sicherungen liegen auf demselben Server wie der Dienst. Das ist bewusst so entschieden und im AVV offengelegt; mit wachsender Kundenzahl wird das neu bewertet.
- **Keine Verschlüsselung der Datenträger** (siehe Abschnitt 2).
- **Kein externer Penetrationstest.** Die Sicherheit wird laufend intern geprüft (zuletzt umfassend im August/September 2026 mit anschließender Härtung); ein Test durch einen unabhängigen Dritten hat bisher nicht stattgefunden.

10. Dokumente, die Sie zusätzlich erhalten

Auf Anfrage vorab, spätestens zum Vertragsstart:

- **Auftragsverarbeitungsvertrag (AVV)** nach Art. 28 DSGVO mit Verarbeitungsübersicht, technisch-organisatorischen Maßnahmen und der Liste der Unterauftragnehmer – anwaltlich geprüft (Fassung August 2026; spätere Ergänzungen werden nachgeprüft).
- **Datenschutzkonzept** und **Verzeichnis von Verarbeitungstätigkeiten** des Anbieters (Art. 30 DSGVO).
- **Pilotvereinbarung** für eine unentgeltliche Testphase.

Fragen dazu beantwortet der Anbieter persönlich – Kontaktweg auf portario.de.