



KUNDENINFORMATION

Precoria.

So verarbeiten wir
Ihre Daten

ENTWURF

Stand 28.08.2026 · Ergänzung zum Auftragsverarbeitungsvertrag

1. Wer ist wofür verantwortlich

Sie als Betrieb sind **Verantwortlicher** für die Daten Ihrer Beschäftigten. Precoria verarbeitet diese Daten **in Ihrem Auftrag** und nach Ihrer Weisung (Art. 28 DSGVO). Wir entscheiden nicht, welche Daten Sie erfassen — wir stellen das Werkzeug und sichern es.

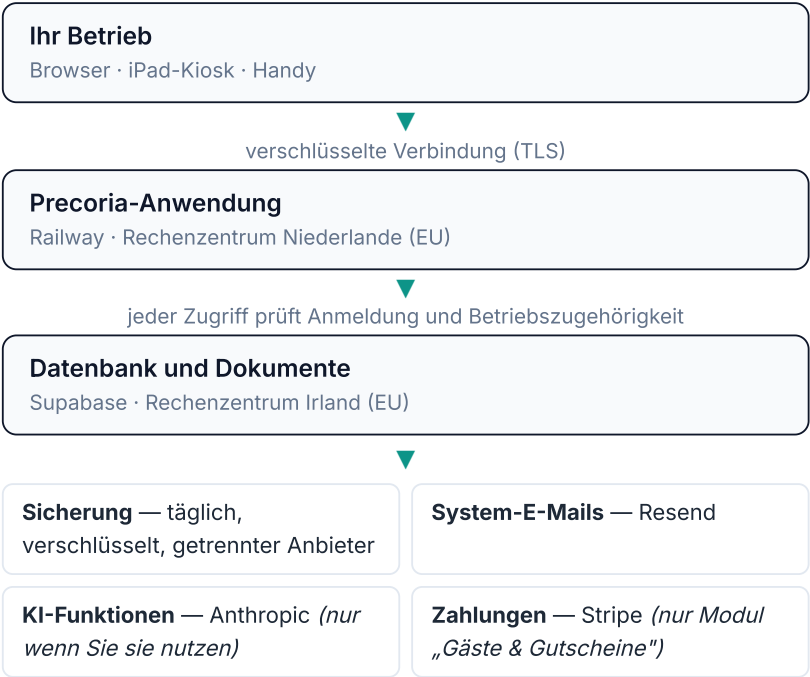
Für die Nutzung unserer Website und für Ihren Vertrag mit uns sind wir selbst Verantwortlicher. Beides ist in der Datenschutzerklärung getrennt beschrieben.

2. Welche Daten Precoria für Sie verarbeitet

Bereich	Daten (Beispiele)	Wofür
Stammdaten	Name, Adresse, Geburtsdatum, Steuer-ID, SV-Nummer, Bankverbindung	Personalakte, Lohnvorbereitung
Arbeitszeit	Stempelungen, Pausen, Dienstpläne, Zeitkonten	Zeiterfassung, ArbZG-Prüfung, § 17 MiLoG
Abwesenheiten	Urlaub, Krankheit, Kind krank	Abwesenheitsverwaltung, Lohnfortzahlung
Dokumente	Verträge, Unterweisungen, Signaturen, Belege	Nachweise, digitale Personalakte
Gäste (nur mit Modul „Gäste & Gutscheine“)	Name, Kontakt, Reservierung, Gutscheinkauf	Reservierungen, Gutscheine

Steuer-ID, SV-Nummer und Bankverbindung sowie hochgeladene Dokumente werden **zusätzlich feldweise verschlüsselt** gespeichert (AES-256). Krankheitsdaten sind besondere Kategorien nach Art. 9 DSGVO und unterliegen gesonderten Zugriffsregeln (Abschnitt 5).

3. Wo Ihre Daten liegen — die Verarbeitungskette



Ihre Daten liegen in der EU. Datenbank, Dokumente und Anwendung werden ausschließlich in Irland und den Niederlanden betrieben; die Website in Frankfurt.

4. Unsere Dienstleister — vollständige Liste

Jeder Dienstleister ist vertraglich zu denselben Pflichten verpflichtet, die wir Ihnen zusagen (Art. 28 Abs. 4 DSGVO). Alle Verträge liegen vor und können auf Anfrage nachgewiesen werden.

Dienstleister	Aufgabe	Standort der Verarbeitung	Vertrag
Supabase	Datenbank, Dokumentenspeicher	Irland (EU)	AVV mit EU-Standardvertragsklauseln
Railway	Betrieb der Anwendung, Sicherungen	Niederlande (EU)	AVV, unterzeichnet 28.08.2026
Vercel	Website und Oberfläche	Frankfurt (EU)	AVV mit EU-Standardvertragsklauseln
Resend	Versand von System-E-Mails	USA	AVV mit EU-Standardvertragsklauseln
Anthropic	KI-Funktionen (Arbeitsrecht-Assistent, Belegerkennung, Gefährdungsbeurteilung)	USA	AVV mit EU-Standardvertragsklauseln
PostHog	Nutzungsanalyse — nur nach Einwilligung, keine Aufzeichnung von Eingaben	EU-Cloud, anteilig USA	AVV, unterzeichnet 28.08.2026
Stripe	Zahlungsabwicklung — nur Modul „Gäste & Gutscheine“	Irland / USA	AVV mit EU-Standardvertragsklauseln

Was in die USA geht — und was nicht: Ihre Stammdaten, Arbeitszeiten und Dokumente verlassen die EU nicht. In die USA gehen nur: der Inhalt von System-E-Mails an den jeweiligen Empfänger (Resend), Eingaben in KI-Funktionen, wenn Sie diese aktiv nutzen (Anthropic), Zahlungsdaten bei Gutscheinkäufen (Stripe) sowie anonymisierte Nutzungsstatistik nach Einwilligung (PostHog). Für jeden dieser Fälle gelten EU-Standardvertragsklauseln.

5. Wie Ihre Daten geschützt sind

Maßnahme	Konkret
Mandantentrennung	Jeder Betrieb sieht ausschließlich seine eigenen Daten. Die Zugehörigkeit wird bei jedem einzelnen Zugriff serverseitig geprüft — nicht nur beim Anmelden.
Kein Direktzugriff	Weder Browser noch Kiosk sprechen direkt mit der Datenbank. Jeder Zugriff läuft über die Anwendung mit Anmeldeprüfung. Auf Datenbankebene ist zusätzlich Zeilenschutz (Row Level Security) aktiv.
Anmeldung	Betriebsnummer + Benutzername + Passwort. Passwörter werden nur als bcrypt-Hash gespeichert, müssen mindestens 12 Zeichen haben und werden gegen bekannt gewordene Datenlecks geprüft. Zwei-Faktor-Anmeldung (TOTP) verfügbar.
Verschlüsselung	Übertragung durchgehend TLS. Sensible Felder und Dokumente zusätzlich AES-256 im Speicher.
Rollen	Mitarbeiter sehen nur eigene Daten; Administratoren die des Betriebs.
Protokollierung	Sicherheitsrelevante und ändernde Aktionen werden im Audit-Log festgehalten.
Wartungszugriff	Zugriffe unserer Mitarbeiter auf Produktivdaten sind auf konkrete Anlässe beschränkt (Störung, Ihre Weisung, gesetzliche Pflicht), folgen dem Grundsatz „Struktur vor Inhalt“ und werden gesondert protokolliert. Gesundheitsdaten werden bei Wartungsarbeiten nicht abgerufen. Bei KI-gestützten Wartungswerkzeugen werden keine Klartext-Personendaten Ihrer Beschäftigten verarbeitet.

6. Sicherung und Wiederherstellung

- **Täglich** vollständige Sicherung von Datenbank und Dokumenten
- **Verschlüsselt** (AES-256) und **bei einem anderen Anbieter** als der Datenbank abgelegt — ein Ausfall bei einem Anbieter trifft nie Daten und Sicherung zugleich
- **Aufbewahrung:** 14 Tagesstände und 12 Monatsstände
- **Jede Sicherung prüft sich selbst** auf Lesbarkeit und Vollständigkeit; bleibt sie aus, schlägt eine Überwachung Alarm
- **Wiederherstellung wird real geprobt** — mindestens vierteljährlich, zuletzt am 28.08.2026 erfolgreich

7. Ihre Rechte als Auftraggeber

Recht	So üben Sie es aus
Export	Vollständiger Export aller Betriebsdaten jederzeit in der Anwendung (Einstellungen → Datenexport), als ZIP
Löschung	Nach Vertragsende bleibt der Export 30 Tage möglich, danach werden die Daten gelöscht. Beschäftigtendaten werden nach Ablauf gesetzlicher Aufbewahrungsfristen automatisch pseudonymisiert.
Nachweis	Verträge mit allen Dienstleistern, Sicherungsprotokoll, Audit-Log — auf Anfrage
Kontrolle	Prüfrecht nach Art. 28 Abs. 3 lit. h DSGVO, per Selbstauskunft oder Bericht
Vorfall	Bei einer Datenschutzverletzung informieren wir Sie unverzüglich mit allen Angaben, die Sie für Ihre eigene Bewertung und ggf. Meldung benötigen

8. Was wir bewusst nicht tun

- keine Nutzung Ihrer Daten für eigene Zwecke, kein Verkauf, keine Werbung
 - keine Weitergabe an Dritte außerhalb der Liste in Abschnitt 4
 - keine automatisierte Entscheidung mit rechtlicher Wirkung — KI-Ausgaben sind Vorschläge
 - keine Aufzeichnung von Bildschirmsitzungen oder Eingaben durch Analyse-Dienste
-

Fragen? hallo@precoria.de · Precoria UG (haftungsbeschränkt), Auenweg 5, 06237 Leuna OT Günthersdorf ·
Amtsgericht Stendal HRB 37991