

Cautela und Ihre Daten.

Alle Datenflüsse auf einer Seite — für Geschäftsführung, Datenschutz und IT. Cautela ordnet die Pflichten der EU-KI-Verordnung. Dieses Blatt zeigt, wie das Werkzeug selbst mit Ihren Daten umgeht.

Datenminimierung Cautela fragt nicht nach Geschäftszahlen, Kundendaten oder Betriebsgeheimnissen. Es braucht nur eines: die Liste der KI-Tools, die Ihr Betrieb einsetzt.	Personendaten bleiben im Haus Mitarbeiternamen, Testergebnisse, Schulungsregister und Kompetenznachweise verlassen unsere EU-Server nicht — kein externes KI-Modell erhält sie.	Regelwerk statt Blackbox Risiko-Einstufungen und Pflichten-Aussagen berechnet ein versioniertes Prüfschema mit Artikel-Fundstellen — kein freies KI-Urteil.
---	---	---

WAS LIEGT WO

DATEN	VERARBEITUNG
Firmen-Stammdaten, KI-Inventar, Compliance-Status	Nur auf unserem Server in Deutschland (Rechenzentrum Berlin), getrennt je Mandant.
KI-Verzeichnis und KI-Richtlinie (Ihre Dokumente)	Nur auf unseren EU-Servern — erzeugt aus Ihrem Inventar, Download durch Sie.
Mitarbeiternamen, Schulungsregister, Testergebnisse, Kompetenznachweise	Nur auf unseren EU-Servern — diese Daten gehen n ie an ein Sprachmodell.
Risiko-Einstufung nach EU-KI-Verordnung	Auf unseren EU-Servern berechnet — deterministisch aus dem versionierten Regelwerk, ganz ohne KI.
Schulungs-Lektionen und Wissenstest	Statische Inhalte auf unseren EU-Servern — ohne KI, ohne externe Dienste.
Das Erfassungsgespräch (Ihre Beschreibung der eingesetzten Tools)	Vorübergehend an das Sprachmodell (Anthropic Claude, per API): ohne Mitarbeiternamen; der Anbieter darf Eingaben vertraglich nicht zum Training verwenden. Das strukturierte Ergebnis kommt zurück auf unseren EU-Server — und bleibt dort.

TECHNISCHE SCHUTZMASSNAHMEN

- **EU-Hosting:** eigene Server in europäischen Rechenzentren (IONOS), DSGVO-konform.
- **Mandantentrennung auf Datenbankebene:** Row-Level Security — jede Abfrage ist technisch auf Ihren Mandanten begrenzt.
- **Transportverschlüsselung (TLS)** für jede Verbindung.
- **Login ohne Passwort:** Einmal-Links mit kurzer Gültigkeit; Zugangs-Token speichern wir nur als Hash.
- **Schulung ohne Mitarbeiter-Konten:** ein Einladungslink genügt — Ihre Mitarbeiter geben nicht einmal eine E-Mail-Adresse an.
- **Tägliche Datensicherung** mit begrenzter Aufbewahrung (30 Tage).

VERTRÄGE, DIENSTLEISTER, IHRE RECHTE

- **Auftragsverarbeitungsvertrag** (Art. 28 DSGVO) — Bestandteil jedes Vertrags.
- **Dienstleister offen gelegt:** IONOS (Hosting, Berlin) · Anthropic (Sprachmodell — nur das Erfassungsgespräch, kein Training) · Brevo (E-Mail-Versand, EU).
- **Export & Löschung:** vollständiger Datenexport und endgültige Löschung jederzeit auf Anfrage (Art. 15–20 DSGVO).
- **Kein Verkauf von Daten,** keine Werbenutzung, kein Training von KI-Modellen mit Kundendaten — durch uns nicht und durch Dienstleister nicht.
- **Transparenz:** Cautela sagt Ihnen immer, dass sie KI ist. Das Produkt lebt vor, was es lehrt.