Waiva: IT-Security & Data Privacy Factsheet

Dokumentenstatus: Technisches Datenblatt für Compliance-Prüfungen **Version:** 1.0 (Januar 2026) **Fokus:** Zero-Trust, Datenminimierung, Deutsche Souveränität

---

1. Datenhaltung & Souveränität (Data Residency)

Waiva verfolgt einen radikalen Ansatz der Datenvermeidung.

- **Standort:** Der Betrieb erfolgt ausschließlich auf dedizierter Infrastruktur in **Berlin, Deutschland (IONOS)**.
- **Rechtssicherheit:** Es findet kein Datentransfer in Drittstaaten statt. Der Gerichtsstand und die gesetzliche Grundlage sind rein deutsch/europäisch (DSGVO-konform).
- **Unabhängigkeit:** Keine Abhängigkeit von US-Hyperscalern (AWS, Azure, GCP), was das Risiko durch den US Cloud Act eliminiert.

2. Transiente Analyse (Zero-Logging Policy)

Waiva ist als „Durchlaufsystem“ konzipiert.

- **Keine Speicherung:** Prompts des Nutzers und Antworten der KI werden ausschließlich im Arbeitsspeicher (RAM) zur Drift-Analyse verarbeitet.
- **Sofortige Löschung:** Nach Abschluss des Analysezyklus werden die Inhalte unwiderruflich aus dem transienten Speicher gelöscht. Es verbleiben lediglich anonymisierte Metadaten für das Monitoring des Stabilitätsscores.
- **Kein Training:** Kundendaten werden zu keinem Zeitpunkt für das Training von Modellen verwendet.

3. Der „Doppelte Scrubber“ (Privacy Layer)

Bevor Daten die Analyse-Engine erreichen, durchlaufen sie ein mehrstufiges Reinigungsverfahren:

- **PII-Filter:** Automatisierte Erkennung und Maskierung von personenbezogenen Daten (Namen, E-Mails, Telefonnummern).

- **Kontext-Reinigung:** Der Scrubber stellt sicher, dass nur die für die strukturelle Stabilitätsmessung notwendigen Merkmale an die Engine übertragen werden.

4. Infrastructure Hardening (BaFin/MaRisk orientiert)

Die Serverumgebung wurde nach Best-Practice-Standards für Hochsicherheitsumgebungen gehärtet:

- **Zugriffsschutz:** SSH-Key-only Authentifizierung (keine Passwörter), Deaktivierung des Root-Logins.
- **Aktive Abwehr:** Einsatz von **Fail2ban** zur automatisierten Sperrung von Brute-Force-Angriffen und **UFW-Shielding** für restriktive Port-Kontrolle.
- **Zahlungssicherheit:** Vollständige Trennung von Business-Logik und Finanzdaten durch **Stripe-Integration**. Waiva verarbeitet oder speichert selbst keine Kreditkarten- oder Bankdaten.

5. Compliance & Human Oversight (EU AI Act)

- **Art. 29 AI Act:** Waiva liefert den technischen Nachweis der Überwachungspflicht für Betreiber von KI-Systemen.
- **Human-in-the-loop:** Durch kontextsensitive Tooltips (bei Scores < 80) wird der menschliche Operator gezielt angeleitet, korrigierende Impulse zu setzen, um die Systemstabilität wiederherzustellen.