

TECHNISCHER STECKBRIEF

Hosting, Anbieter, Datenflüsse, Zugriffe

Für IT-Verantwortliche und Datenschutzbeauftragte. Die Angaben gelten für den Standard. Abweichungen je Lösung stehen im Datenschutz-Steckbrief des Angebots.

Hosting

BAUSTEIN	ANBIETER	STANDORT
Website und Serverfunktionen	Vercel Inc.	Serverfunktionen Frankfurt (fra1)
Datenbank und Wissensbasis	Supabase Inc.	EU-Region Frankfurt, Konto auf Kundennamen
Automatisierung	n8n, selbst betrieben	Server in der EU, Anbieter im AVV benannt
Automatisierung (optional)	Make	EU-Zone des Kundenkontos

Sprachmodelle nach Datenklasse

DATENKLASSE	WEG	VERARBEITUNG
Personenbezogen, intern	Claude über Google Cloud (Endpunkt eu) oder AWS Bedrock (EU-Profil), GPT über Azure Data Zone EU	EU, kein Training auf Kundendaten
Streng vertraulich	Mistral oder offene Modelle in der Umgebung des Kunden	EU oder Rechenzentrum des Kunden
Ohne Personenbezug	Direktzugang beim Anbieter möglich	laut Anbieter, kein Training

Datenfluss je Lösungsklasse

KLASSE	FLUSS
S, M	Auslöser → Automatisierung (EU) → Sprachmodell (EU-Endpunkt) → Entwurf im Kundensystem → Freigabe
L	Eingang → Automatisierung → Wissensbasis Frankfurt → Sprachmodell → Entwurf oder Routing → Freigabe oder Prüfliste
XL	Auftrag → Agent mit begrenzten Rechten → Aktionen über API oder MCP → Audit-Log → Freigabe vor schreibenden Aktionen

Zugriffskonzept und Betrieb

- 01

Geringste Rechte. Lesen statt schreiben, ein Postfach statt aller, ein Ordner statt des Laufwerks.
- 02

Konten beim Kunden. Persönliche, entziehbare Zugänge für das Projektteam.

- 03 **Geheimnisse getrennt.** Schlüssel nur in Geheimnisspeichern der Plattformen, nie im Code oder in Mails.
- 04 **Protokolle.** Läufe, Fehler, Kosten; Audit-Log für Agenten; Kostenlimit je Lösung.
- 05 **Freigabeschritt.** Was nach außen geht oder Daten verändert, gibt ein Mensch frei.
- 06 **Exit.** Übergabe von Zugängen, Konfiguration, Prompts, Runbooks; Löschung der Auftragsdaten mit Bestätigung.

Grenzen: Keine Überwachung oder Leistungskontrolle von Beschäftigten, keine Bewertung von Personen, keine automatisierten Entscheidungen über Menschen.

AVV nach Art. 28 DSGVO mit Liste der Unterauftragnehmer liegt jedem Angebot bei. Ansprechpartner: Jean Hinz, mail@ki-agentur.io.