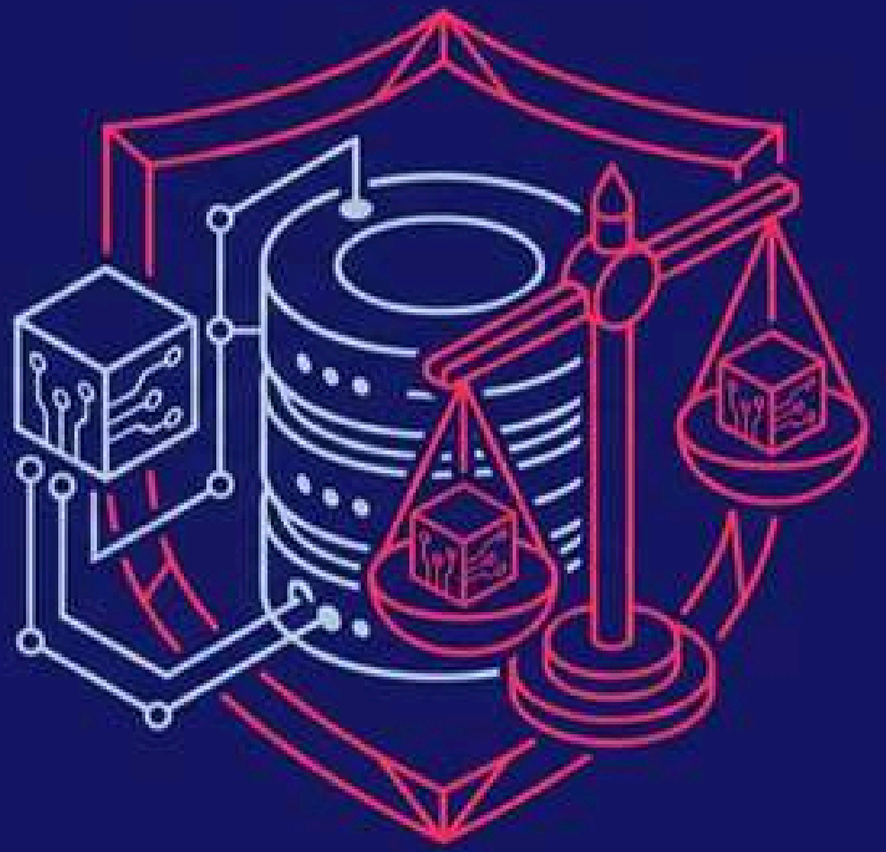
Assistini



KI-Wissensdatenbanken & DSGVO

Wie Unternehmen Künstliche Intelligenz rechtssicher und effizient einsetzen.

Das Spannungsfeld: Effizienz vs. Verantwortung

Effizienz

- Kontext
- Schnelligkeit
- Innovation

Verantwortung

- Datenschutz
- Governance
- Sicherheit

Unternehmen müssen enorme Wissensbestände (Verträge, HR, ERP) nutzbar machen. Doch unkontrollierte KI-Nutzung riskiert rechtliche und wirtschaftliche Folgen. Innovation erfordert Struktur.

Vom Suchen zum Finden

Klassische Suche

Trefferlisten

KI-Wissensdatenbank

Konkrete Antworten

Basiert auf Vektordatenbanken, NLP und RAG. Ziel: Entlastung von Support-Teams und schnellere Entscheidungen.

Warum ChatGPT keine Unternehmens-Datenbank ist

Der direkte Upload sensibler Daten ist technisch einfach, aber regulatorisch gefährlich ("Shadow AI").

Viele Unternehmen unterschätzen die Risiken von Direkt-Uploads in Tools wie ChatGPT oder Gemini.

Die 4 Gefahren direkter Uploads

Drittlandtransfers

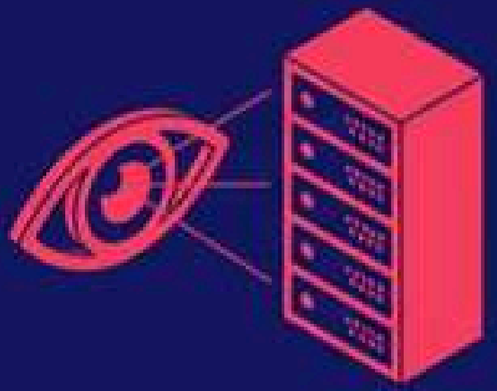
Daten verlassen die EU (Art. 44–50 DSGVO).

Training

Daten verbessern das Modell und sind nicht mehr kontrollierbar.

Löschbarkeit

‘Gelerntes’ Wissen kann nicht gezielt gelöscht werden (Art. 17).



Zugriff

Zugriffsmöglichkeiten ausländischer Behörden.

Compliance als Fundament

Rechtsgrundlage & Zweck

Wofür werden die Daten verarbeitet?

Datenminimierung

Nur das Notwendige speichern.

TOMs

Technische & organisatorische Maßnahmen.

Folgenabschätzung

Pflicht bei sensibler Datenverarbeitung.

Daten & Zweck: Klasse statt Masse

- **Zweckbindung:** Klare Definition, wofür Modelle auf Daten zugreifen.
- **Minimierung:** Beschränkung auf notwendige Daten.
- **Löschkonzepte:** Technische Wege zur Entfernung von Embeddings.

Technische und organisatorische Maßnahmen (TOMs)

- Verschlüsselung (AES-256 für Data-at-Rest)
- Übertragung (TLS-gesicherte Wege)
- Zugriff (Rollenbasierte Zugriffskontrolle & MFA)
- Netzwerk (Segmentierung & Monitoring)

Ohne diese Maßnahmen nach Art. 32 DSGVO ist eine KI-Infrastruktur nicht belastbar.

Die Lösung: Trennung von Wissen und Modell

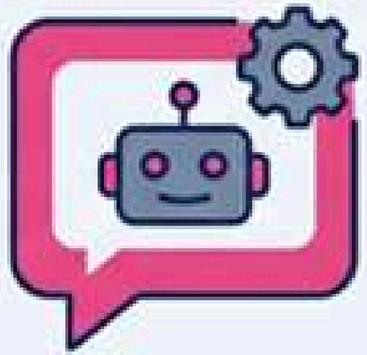
1. Die Datenebene

Wissens-Tresor

2. Kontrollschicht

Gatekeeper

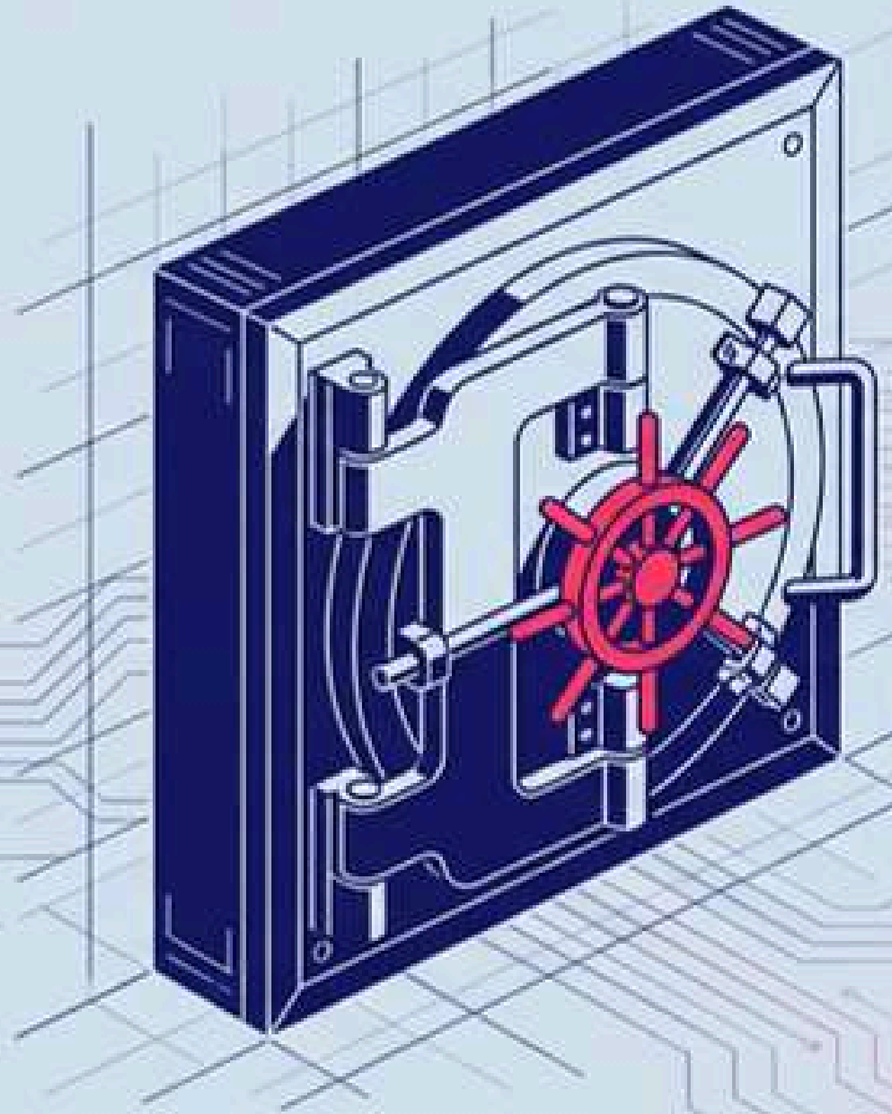
3. Modellebene



Prozessor

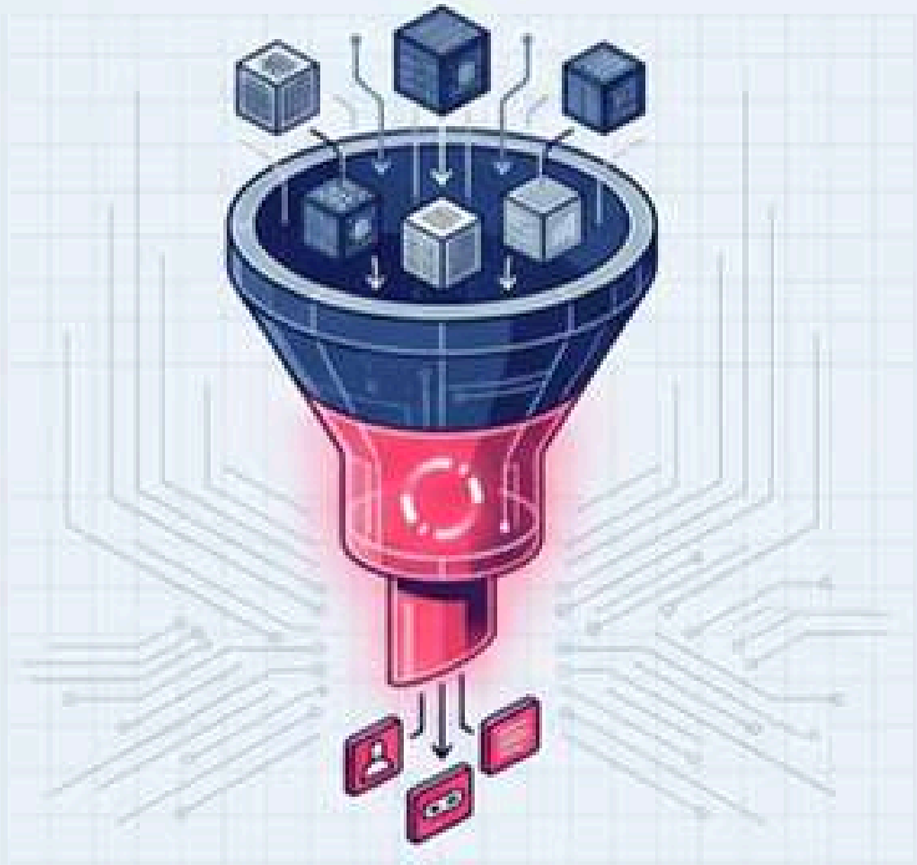
Nutzerfrage → Suche → Filter → Modell

Ebene 1: Der Wissens-Tresor (Datenebene)



- **Inhalt:** Originaldokumente, strukturierte Daten, Embeddings.
- **Hosting:** EU-Hosting oder On-Premise.
- **Sicherheit:** Verschlüsselte Speicherung.
- **Kontrolle:** Sensible Rohdaten verbleiben vollständig beim Unternehmen.

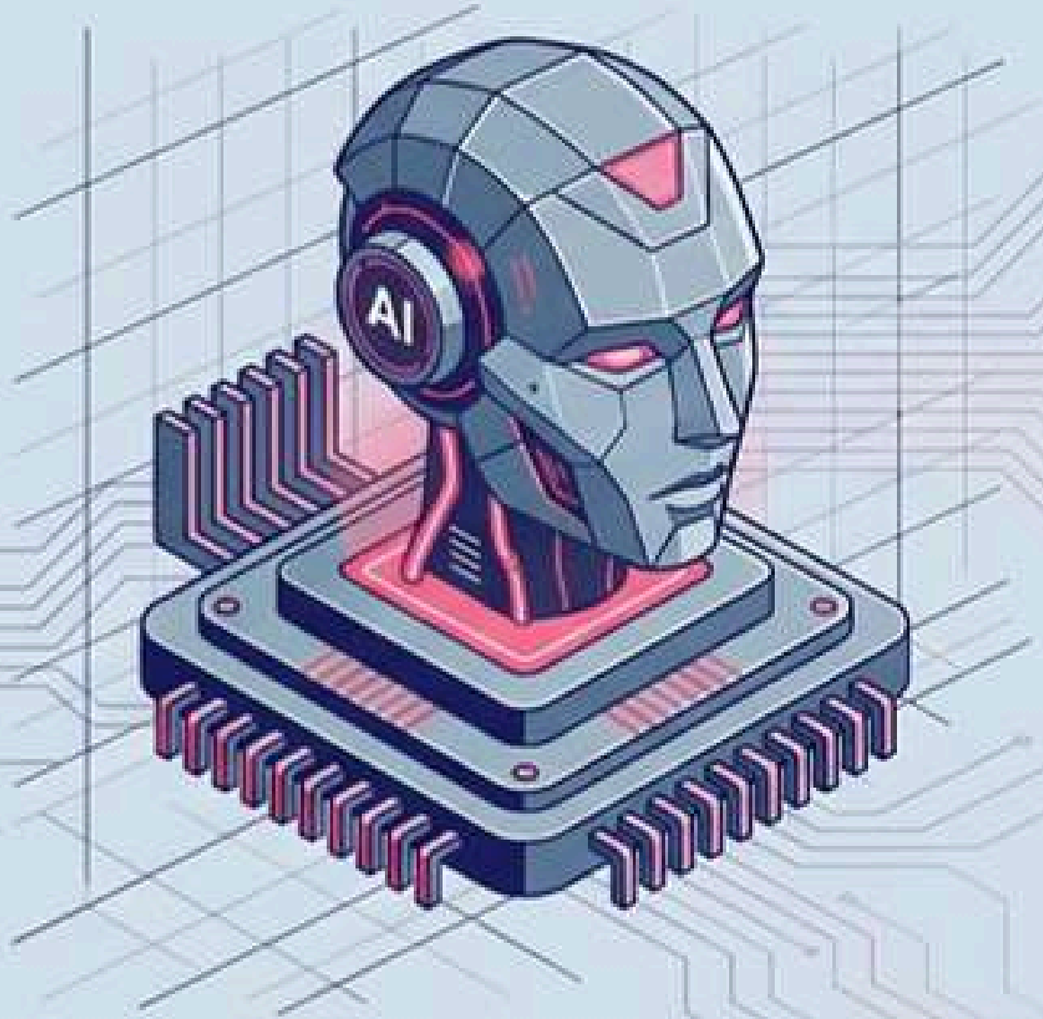
Ebene 2: Der Gatekeeper (Kontrollschicht)



1. PII-Erkennung: Identifikation personenbezogener Daten.
2. Pseudonymisierung: Daten werden maskiert.
3. Reduktion: Nur relevanter Kontext wird weitergeleitet.

Diese Schicht stellt sicher, dass das KI-Modell niemals Rohdaten sieht.

Ebene 3: Der Prozessor (Modellebene)



- **Input:** Erhält nur die Nutzerfrage + bereinigte Snippets.
- **Kein Training:** Vertraglicher Ausschluss der Trainingsnutzung.
- **Kein Gedächtnis:** Keine dauerhafte Speicherung produktiver Daten.

Das Modell generiert die Antwort und ‘vergisst’ die Daten sofort wieder.

The Strategic Blueprint

Vertrauen durch Transparenz (Auditierbarkeit)

Protokollierung der Anfrage

Eindeutige Speicherung der eingehenden Benutzeranfragen mit Zeitstempel und Kontext.

Dokumentation der genutzten Datenquellen

Nachvollziehbare Auflistung aller verwendeten internen und externen Datenquellen und Dokumente.

Angabe der Modellversion

Klare Kennzeichnung der spezifischen Version des verwendeten KI-Modells und seiner Konfiguration.

Essenziell für interne Revision, Risikomanagement und Aufsichtsbehörden.

Der Blick nach vorn: Hosting & Regulierung

Nicht der Betriebsmodus (Cloud vs. On-Prem) ist entscheidend, sondern die Rechtsordnung und vertragliche Garantien.

Der **'EU AI Act'** wird Transparenzpflichten weiter erhöhen. 'Privacy-by-Design' ist strategische Weitsicht.

The Strategic Blueprint

Fazit: Innovation braucht Struktur

- Trennung von Wissensdatenbank und Sprachmodell.
- EU-basierte Infrastruktur.
- Löschbarkeit und Auditierbarkeit.

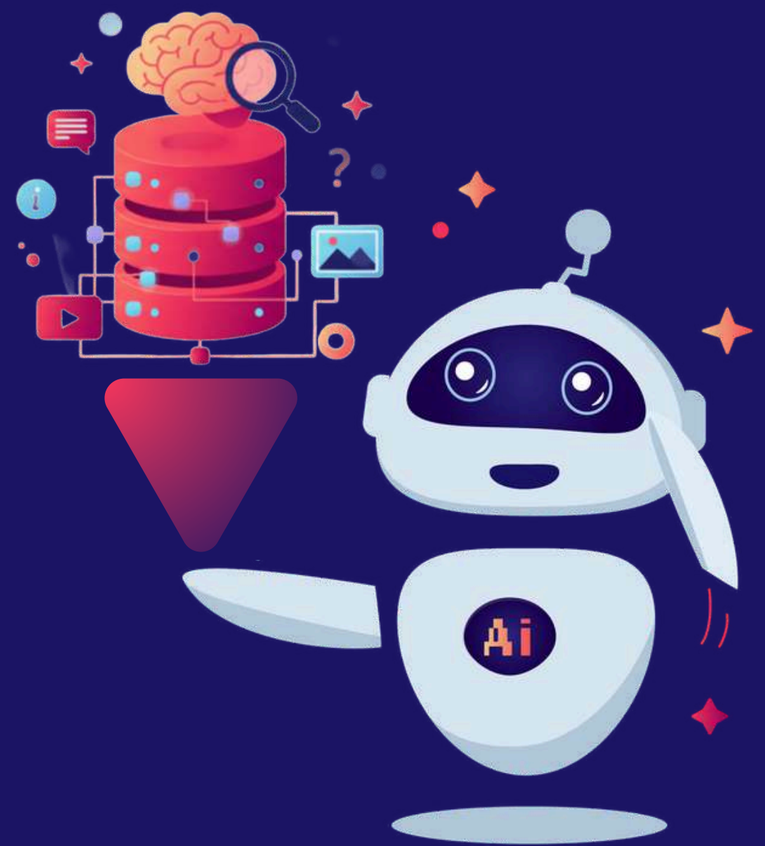
Wer KI auf dieser Grundlage implementiert, schafft **Effizienz** und **stärkt das Vertrauen**. Positionieren Sie sich als verantwortungsbewusster **Innovationsführer**.

Assistini

KI-Wissensdatenbank

Ihre Daten. Ihre Kontrolle. Ihre KI.

- ✓ EU-konforme Architektur
- ✓ Trennung von Daten & LLM
- ✓ Keine Trainingsnutzung
- ✓ Vollständige Auditierbarkeit



Mehr erfahren:

👉 Gesprächstermin vereinbaren: https://assistini.de/kontakt
👉 Eigenen Use Case testen: https://assistini-knowledge.de

Assistini.de

Innovation trifft Verantwortung.