

Architektur-Prüfbogen für RAG-Systeme

Ein Angebot oder ein laufendes System in einer Stunde bewerten: IT-Leitung, Datenschutz und Fachbereich gemeinsam.

SYSTEM / ANBIETER	DATUM	GEPRÜFT VON
-------------------	-------	-------------

01 BERECHTIGUNGEN ☐ Weg: Rechte im Index / Abfrage im Namen des Nutzers / Dienstkonto ☐ Quellsysteme, deren Rechte übernommen werden ☐ Frist für den Rechteabgleich (Minuten / Stunden) ☐ Test: Nutzer ohne Recht fragt nach gesperrtem Dokument, Ergebnis ☐ Zwischenspeicher prüft Rechte je Nutzer: ja / nein	02 DATENRESIDENZ ☐ Standort Index (Rechenzentrum, Land) ☐ Standort Modellaufruf (Rechenzentrum, Land) ☐ Auftragsverarbeitungsvertrag nach Art. 28 mit Trainingsausschluss: ja / nein ☐ Unterauftragnehmer außerhalb der EU: keine / welche ☐ Löschfrist nach Löschung in der Quelle (Stunden / Tage)
03 QUELLENPFLICHT ☐ Jede Antwort mit Dokument, Seite, Stand: ja / nein ☐ Verhalten ohne Treffer: „nicht gefunden“ / erfindet Antwort ☐ Test: fünf Fragen ohne Antwort im Bestand, Ergebnis ☐ Widersprüchliche Versionen werden als Widerspruch gemeldet: ja / nein	04 AUDIT-TRAIL ☐ Protokoll enthält: Nutzer, Zeit, Frage, gelesene Passagen, Antwort, ☐ Aufbewahrungsfrist (Monate) ☐ Auswertungsverbot für Leistung und Verhalten in der Betriebsvereinbarung: ja / ☐ Zugriff auf das Protokoll nur mit Vier-Augen-Prinzip: ja / nein
05 ERGEBNIS ☐ Säulen erfüllt (0 bis 4) ☐ Ausschlusskriterien getroffen (Dienstkonto, Drittland, kein ☐ Entscheidung: freigeben / nachbessern / ablehnen ☐ Nachbesserungen mit Termin und Verantwortlichem	

REIHENFOLGE

1 Berechtigungen	2 Residenz	3 Quellenpflicht	4 Audit-Trail	5 Ergebnis
------------------	------------	------------------	---------------	------------



TIPPS VOM BYTE

- Berechtigungen werden zur Abfragezeit geprüft, nicht beim Import. Alles andere ist ein Datenleck mit Verzögerung.
- Trennen Sie Index, Modell und Anwendung so, dass Sie jedes Teil austauschen können, ohne die anderen anzufassen.
- Lassen Sie sich den Datenfluss aufzeichnen: wo liegt der Index, wohin geht der Modell-Aufruf, was bleibt im Haus.

GEGENZEICHNUNG

IT-Leitung	Datenschutz	Fachbereich
------------	-------------	-------------

Regel: Ein Dienstkonto, das alles lesen darf, ein Modellaufruf ins Drittland oder ein fehlender Trainingsausschluss ist ein Ausschluss, keine Nachbesserung.