

Bevor sich Beschäftigte auf eine KI-Wissensdatenbank verlassen

Erst die Dokumente korrigieren, dann ein Test in sechs Schritten, abgeleitet aus datierten Belegen (Stanford, 30.05.2024; Moffatt v. Air Canada, 14.02.2024; Dokumentation von OpenAI und Microsoft, 2026). Unsere Methode, kein Branchenstandard.

1 Eine aktuelle Fassung pro Thema

Verschieben Sie alte Preislisten, abgelaufene Richtlinien und ersetzte Vorlagen aus den Ordnern, die die Wissensdatenbank liest.

Der Chatbot von Air Canada widersprach Air Canadas eigener Richtlinienseite (2024 BCCRT 149, 14.02.2024).

2 Eine verantwortliche Person und ein Datum je Dokument

Ist eine Antwort falsch, muss jemand wissen, welche Datei zu korrigieren ist und wann sie zuletzt geprüft wurde.

3 Ein schriftlicher Umfang und saubere Freigaben

Legen Sie fest, welche Fragen sie beantworten darf und welche sie ablehnen muss. Entfernen Sie Freigaben für „alle“ auf sensiblen Ordnern, bevor Sie etwas anbinden.

Microsofts Copilot-Plan, aktualisiert am 18.08.2026: erster Schritt „Remediate oversharing“.

4 30 bis 50 echte Fragen sammeln

Nutzen Sie Fragen, die Beschäftigte oder Kunden in den letzten drei Monaten gestellt haben, in deren eigenen Worten.

5 5 bis 10 unbeantwortbare Fragen ergänzen

Richtig ist dann „Das weiß ich nicht“, kein Raten.

Stanford 2024: juristische Programme mit geprüften Quellen erfanden bei 17–33 % von 202 Fragen Inhalte.

6 Quellen einer Stichprobe prüfen

Öffnen Sie bei mindestens zehn Antworten die zitierte Passage und prüfen Sie, ob sie sagt, was die Antwort behauptet.

Stanford zählt Antworten, die eine Quelle fälschlich als Beleg ausgeben, als erfunden.

7 Ein veraltetes Dokument einschleusen

Legen Sie eine alte Fassung neben eine aktuelle und sehen Sie, welche die Wissensdatenbank zitiert.

8 Berechtigungstest mit zwei Personen

Stellen Sie dieselbe Frage als zwei Personen mit unterschiedlichem Zugriff. Wer die Datei nicht öffnen darf, darf ihren Inhalt nicht erhalten.

9 Nach jeder Änderung wiederholen

Lassen Sie denselben Fragenkatalog erneut laufen, wenn sich Dokumente, Modelle oder Einstellungen ändern, und bewahren Sie die Ergebnisse auf.

Grenzen, die Sie kennen sollten

- ChatGPT-Business-Projekte fassen bis zu 40 Dateien, ein eigenes GPT bis zu 10 Wissensdateien für seine Lebensdauer (OpenAI-Hilfe, Oktober 2026).
- Außerhalb von ChatGPT Enterprise liest ChatGPT nur den digitalen Text einer Datei, keine eingebetteten Bilder.
- Antworten an Kunden sind Aussagen Ihres Unternehmens: Halten Sie sie zur Prüfung zurück, wo es darauf ankommt.