

Ausgefülltes fiktives Beispiel — CloudKite AI

FIKTIV — kein reales Unternehmen	
Auslöser / nächstes Käufergespräch	Vendor Review mit MedicoWorks, 30.07.2026
Zählfeld B / T / O / N/A	18 / 17 / 13 / 2
Wichtigstes Muster aus dem Scan	Datenflüsse zu LLM-Provider und Supportzugriff sind nicht zusammengeführt.
Größte Unsicherheit	Ob Prompt-/Output-Retention beim aktuellen Providervertrag deaktiviert ist.
Aussage, die wir bis zur Klärung nicht verwenden	„EU-only processing“

Top 3 nächste Schritte

NÄCHSTER SCHRITT 1	
Unsicherheit / Red Flag	AI-Retention im aktuellen Providervertrag unklar
Warum relevant	Eine falsche Aussage zur Nutzung von Prompts kann den Vendor Review stoppen.
Nächste Aktion	DPA und Adminsetting gemeinsam prüfen; freigabefähige Aussage formulieren.
Verantwortliche Rolle	Mira / CTO
Termin	17.07.2026
Abnahmekriterium	Aussage durch CTO geprüft und im Antwortbestand aktualisiert.
Ablage / Nachweis	DPA v3.2 + datierter Screenshot des Adminsettings.

NÄCHSTER SCHRITT 2	
Unsicherheit / Red Flag	Supportzugriff nicht durchgängig protokolliert
Warum relevant	Unbelegter privilegierter Zugriff ist ein konkreter Käufer- und Incident-Risikopunkt.
Nächste Aktion	JIT-Zugriff mit Ticket-ID in Staging testen und Arbeitsanweisung ergänzen.
Verantwortliche Rolle	Jonas / Engineering
Termin	22.07.2026
Abnahmekriterium	Test erfolgreich; Ticket-, Freigabe- und Logkette nachvollziehbar.
Ablage / Nachweis	TEST-LOG-014 + Arbeitsanweisung SUP-02 v0.3.

NÄCHSTER SCHRITT 3		
Unsicherheit / Red Flag		Löschung in Backups nicht erklärt
Warum relevant		Ein pauschales Löschversprechen wäre ohne Backup-Ausnahme nicht belastbar.
Nächste Aktion		Backupzyklen und Ausnahmen dokumentieren; Käuferantwort begrenzen.
Verantwortliche Rolle		Mira / CTO
Termin		24.07.2026
Abnahmekriterium		Retention-Antwort freigegeben und in DPA-FAQ übernommen.
Ablage / Nachweis		Retention-Tabelle v0.1 + Reviewnotiz 2026-07-24.

Entscheidungsregel

STOP: Externe Aussage aussetzen, wenn Datenweg, Providerbedingung oder Kontrollnachweis unbekannt ist. CAUTION: offen kennzeichnen und Termin/Owner setzen. GO: nur konkret, aktuell und belegbar antworten.

Ergebnis nach 30 Tagen: AI-Disclosure v0.1, protokollierter Supportzugriff und belastbare Retention-Antwort; kein Compliance-Claim.