

8 Schritte zur **sicheren** KI-Beschaffung

Von der Bedarfsklärung bis zum laufenden Betrieb
Für Einkauf · Compliance · IT-Leitung · Entscheider

1

SCHRITT 1

Bedarfsklärung

Problem in einem Satz definieren. Datenarten, Nutzerzahl und Frequenz klären. **Budget** in Einmal- und laufende Kosten aufteilen.

2

SCHRITT 2

Eignungsprüfung

Ist KI wirklich nötig oder reicht Automatisierung? **Shadow-AI-Check: 4 von 10 Unternehmen** bereits betroffen.

3

SCHRITT 3

Rechtliche Prüfung

EU AI Act Risikoklasse bestimmen. DSGVO, **Berufsgeheimnisschutz** (§43e BRAO, §57 StBerG) und AI Literacy sicherstellen.

4

SCHRITT 4

Betriebsmodell wählen

Cloud, **EU-Plattform** (z.B. Langdock) oder Self-Hosted. Bei sensiblen Daten EU-Standort für Datensouveränität.

5

SCHRITT 5

Kostencheck (TCO)

TCO über 3 Jahre berechnen. Produktion kostet **10-50x mehr** als der Pilot. ROI entfaltet sich erst in Jahr 2-3.

6

SCHRITT 6

Anbieter Due Diligence

AVV und Zertifizierungen (**ISO 42001**, SOC 2, BSI C5) prüfen. Trainingsnutzung eigener Daten **vertraglich ausschließen**.

7

SCHRITT 7

Vertragliche Absicherung

IP-Rechte, Exit-Klauseln (max. 3 Monate Kündigung) und **MCC-AI** Mustervertragsklauseln als Ausgangspunkt nutzen.

8

SCHRITT 8

Laufender Betrieb

Kosten- und Qualitätsmonitoring einrichten. **Erlaubte-KI-Liste** kommunizieren. Anbieter alle 6-12 Monate neu evaluieren.