

KI-Einkauf ohne Risiko

8 Schritte zur sicheren KI-Beschaffung
Für Einkauf, IT-Leitung, Compliance und Entscheider

1

BEDARF

2

TEAM

3

EIGNUNG

4

RECHT

5

BETRIEB

6

KOSTEN

7

ANBIETER

8

VERTRAG

Diese Checkliste gibt Orientierung für den KI-Einkaufsprozess. Nicht jeder Punkt ist in jedem Projekt relevant – aber jeder sollte bewusst geprüft und eine Entscheidung getroffen werden. **Hintergründe zu jedem Schritt: „AI-SourceKit“ - Einkauf von KI.**

1

WAS WOLLEN WIR EIGENTLICH?

Bedarfsklärung

- ☐ Welches Problem soll die KI lösen? *(In einem Satz!)*
- ☐ Wer nutzt die KI? Welche Abteilung, wie viele Personen?
- ☐ Welche Daten werden verarbeitet? Kunden-, Personal- oder Finanzdaten?
- ☐ Nutzungsfrequenz: 10 Anfragen täglich oder 10.000?
- ☐ Anbindung an bestehende IT-Systeme erforderlich?
- ☐ Budget: Einmal- und laufende Kosten getrennt erfassen

2

WER MUSS EINGEBUNDEN WERDEN?

Wer muss ran?

KI-Beschaffung ist kein Solo-Projekt. Diese Rollen sollten frühzeitig eingebunden werden:

- **Einkauf** – Koordination & Verträge
 - **CISO** – IT-Sicherheit
 - **Legal** – Vertragsrecht, AI Act
 - **Fachbereich** – Anforderungen
- **IT / IT-Admin** – Systemintegration
 - **DISO / Datenschutz** – DSGVO, DSFA
 - **Betriebsrat** – Mitbestimmung
 - **GF / Entscheider** – Freigabe & Budget

Verantwortlichkeiten schriftlich festhalten – wer entscheidet was? Wer fehlt?

3

BRAUCHEN WIR ÜBERHAUPT KI?

Eignungsprüfung

- ☐ Ist KI wirklich die beste Lösung oder reicht eine einfache Automatisierung?
- ☐ Sind genug Daten vorhanden für sinnvollen KI-Einsatz?
- ☐ Ist die Aufgabe klar genug definiert?
- ☐ Mitarbeitende bereit? Schulungsbedarf ermitteln!
- ☐ Shadow-AI-Check: Werden bereits private Tools genutzt?

4 von 10 Unternehmen betroffen

4

WELCHE REGELN GELTEN?

Rechtliche Prüfung

- ☐ EU AI Act anwendbar? Risikoklasse bestimmt?
- ☐ Hochrisiko-KI: Konformitätsbewertung & CE-Kennzeichnung eingeplant?
- ☐ DSGVO: Datenschutz-Folgenabschätzung (DSFA) erforderlich?
- ☐ Branchenregeln geprüft: BaFin, Medizin, Finanzen?
- ☐ Berufsgeheimnisschutz: §43e BRAO, §57 StBerG, §203 StGB
- ☐ Betriebsrat eingebunden? Mitbestimmungspflicht prüfen!

5

WO WERDEN DATEN VERARBEITET?

Betriebsmodell wählen

- ☐ **Cloud** (OpenAI API, Azure): Günstig & schnell, Daten gehen an Anbieter
- ☐ **EU-Plattform** (z.B. Tensorfive, Langdock, Zive): Daten in der EU, DSGVO-konform **Empfohlen**
- ☐ **Self-Hosted**: Volle Datensouveränität, höhere Betriebskosten
- ☐ Entscheidung dokumentiert und mit CISO & Datenschutz abgestimmt?
- ☐ Monitoring & Qualitätssicherung eingeplant: regelmäßige Stichproben

6

WAS KOSTET DAS WIRKLICH?

Kostencheck (TCO)

- ☐ Abrechnungsmodell verstanden: Pro Nutzer, Anfrage oder Token?
- ☐ TCO über 3 Jahre: API, Integration, Schulung, Wartung, Monitoring
- ☐ Proficiency-Kurve: ROI entfaltet sich über Zeit *(J1 Adoption, J2 Optimierung, J3 volle Wirkung)*
- ☐ Skalierungsfalle beachtet: Pilot vs. Produktion **Faktor 10-50x**
- ☐ Automatische Alerts bei Budgetüberschreitung eingeplant?

7

ANBIETER UNTER DIE LUPE

Due Diligence

- ☐ Sitz & Rechenzentrum: EU oder Drittland?
- ☐ AVV (Auftragsverarbeitungsvereinbarung) vorhanden?
- ☐ Werden Eingaben zum Modelltraining genutzt? *(Muss vertraglich ausgeschlossen sein!)*
- ☐ Zertifizierungen vorhanden: ISO 42001, SOC 2, BSI C5?
- ☐ Referenzkunden in der eigenen Branche vorhanden?
- ☐ Schulungen & Prompt Engineering im Lieferumfang?

8

VERTRAG RICHTIG GESTALTEN

Vertragliche Absicherung

- ☐ Nutzungszweck & IP-Rechte klar definiert: Wem gehören die Ergebnisse?
- ☐ Exit-Klausel: max. 3 Monate Kündigungsfrist, mind. 6 Monate Übergangszeitraum
- ☐ Datenexport jederzeit möglich? Format: JSON, CSV
- ☐ MCC-AI: EU-Mustervertragsklauseln als Ausgangspunkt?
- ☐ Meldepflichten bei schwerwiegenden Fehlern (Art. 73 AI Act)
- ☐ Anbieter-Evaluierung alle 6–12 Monate vertraglich verankern