Prüfliste: MCP Server anbinden

Zum Ausdrucken und manuellen Ausfüllen, eine Liste je Server. Ausgefülltes Beispiel auf Seite 2, Erklärung im Ratgeber „MCP Server im Unternehmen“ auf inventivo.de.

1 · SERVER UND HERKUNFT

Name des Servers und Anbieter

Anwendungsfall

- ☐ **Hersteller des Systems**
- ☐ **Anbieter mit Vertrag**
- ☐ **Offizielles Verzeichnis** (prüft nur die Herkunft des Namens)
- ☐ **Unbekannter Dritter**

- ☐ **Lokal** auf dem Rechner der Nutzer (stdio)
- ☐ **Entfernt** beim Anbieter (Streamable HTTP)

2 · ANGEBUNDENE SYSTEME UND DATEN

System	Daten, die die KI sehen würde	Personenbezogen?
		☐ ja ☐ nein
		☐ ja ☐ nein
		☐ ja ☐ nein

3 · RECHTE UND FREIGABEN JE WERKZEUG

Werkzeug (Tool)	Lesen	Schreiben	Freigabe vor Ausführung?
	☐	☐	☐ ja ☐ nein ☐ abgeschaltet
	☐	☐	☐ ja ☐ nein ☐ abgeschaltet
	☐	☐	☐ ja ☐ nein ☐ abgeschaltet
	☐	☐	☐ ja ☐ nein ☐ abgeschaltet

- ☐ Eigenes Konto oder eigener Zugangsschlüssel für diesen Server
- ☐ Zugangsdaten nicht in geteilten Dateien oder Chats
- ☐ Nur die verantwortliche Person darf neue Server verbinden

4 · PROTOKOLLIERUNG UND AUFBEWAHRUNG

Was wird protokolliert, und wo?

Wer darf es lesen, wie lange bleibt es?

5 · VERANTWORTUNG, PRÜFTERMIN UND ENTSCHEIDUNG

Verantwortliche Person

Prüftermin und Kriterium für die Entscheidung

- ☐ **Im Pilot anbinden**
- ☐ **Nur lesend anbinden**
- ☐ **Nicht anbinden**

Begründung

Beispiel: Weinhandel mit Gastronomiekunden

Angenommen, ein Weinhandel beliefert Restaurants und verkauft online. Er will Warenwirtschaft und Postfach an seinen KI-Assistenten anbinden. Diese Liste gilt für den Server der Warenwirtschaft. Betrieb und Entscheidungen sind erfunden.

1 · SERVER UND HERKUNFT

Server und Anbieter: Server des Herstellers der Warenwirtschaft

Anwendungsfall: Anfragen der Gastronomie zu Verfügbarkeit und Preisen schneller beantworten

- ☑ **Hersteller des Systems**
- ☐ **Anbieter mit Vertrag**
- ☐ **Offizielles Verzeichnis**
- ☐ **Unbekannter Dritter**

- ☐ **Lokal**
- ☑ **Entfernt** beim Hersteller, Anmeldung über OAuth

2 · ANGEBUNDENE SYSTEME UND DATEN

System	Daten, die die KI sehen würde	Personenbezogen?
Warenwirtschaft	Bestände, Jahrgänge, Preislisten	nein, soweit keine kundenbezogenen Konditionen enthalten sind (prüfen)
Kundenkonten	gesperrt, nicht angebunden	ja, deshalb gesperrt

3 · RECHTE UND FREIGABEN JE WERKZEUG

Werkzeug (Tool)	Lesen	Schreiben	Freigabe vor Ausführung?
Bestand abfragen	☑	☐	nein, wird protokolliert
Preisliste lesen	☑	☐	nein, wird protokolliert
Bestellung anlegen	☐	☐	im Pilot abgeschaltet

- ☑ Eigenes Konto nur für diesen Server, nur lesend
- ☑ Zugangsdaten nur in den Einstellungen der Anwendung

4 · PROTOKOLLIERUNG UND AUFBEWAHRUNG

Was und wo: jeder Werkzeugaufruf mit Person, Zeit, Eingabe und Ergebnis, in der KI-Anwendung

Lesen und Dauer: nur die Verantwortliche; Aufbewahrungsdauer und Löschung mit dem Datenschutzbeauftragten abgestimmt

5 · VERANTWORTUNG, PRÜFTERMIN UND ENTSCHEIDUNG

Verantwortlich: Leiterin des Innendienstes

Prüftermin: nach dem ersten Pilotmonat. **Kriterium:** Antworten zu Bestand und Preis stimmen mit der Warenwirtschaft überein.

- ☑ **Im Pilot anbinden**, zwei Personen aus dem Innendienst
- ☐ **Nur lesend anbinden**
- ☐ **Nicht anbinden**

Begründung: klarer Anwendungsfall, Server vom Hersteller, nur lesende Werkzeuge aktiv, Protokoll vorhanden.

Liste ausgefüllt?
Schick sie an hallo@inventivo.de, gerne ohne Zugangsdaten und ohne personenbezogene Daten. Ich melde mich mit einer Einschätzung zu Rechten und Freigaben für deinen Server.

hallo@inventivo.de

Beispiel erfunden · Orientierung, keine Rechts- oder Sicherheitsberatung · Ratgeber: inventivo.de/blog/ki-automatisierung/mcp-server