



Prompting-Template KI-Assistent / KI-Agent

Stand: 24.04.2026

Hinweis: Füllt zuerst die Bereiche 1–7 aus. Die agentischen Erweiterungen 8–10 nur nutzen, wenn euer Use Case wirklich einen Agenten erfordert.

1. Use Case & Ziel

Use Case (1–2 Sätze): Welche konkrete Aufgabe soll der Assistent oder Agent übernehmen?

Ziel: Woran erkennt man ein gutes Ergebnis? Was soll am Ende besser, schneller oder sicherer sein?

Erfolgskriterium: Wie messe ich, ob der Assistent seinen Job macht?

2. Rolle & Persönlichkeit

Rolle der KI: Welche Funktion übernimmt die KI?

Tonalität & Stil: Wie kommuniziert die KI? (z. B. sachlich-präzise, freundlich-zugänglich, formal-konservativ, weitere...)

Verhalten bei Wissenslücken: Was tut die KI, wenn sie etwas nicht weiß oder unsicher ist? (z. B. explizit kennzeichnen, nachfragen, stoppen)

3. Zielgruppe & Kontext

Zielgruppe: Für wen arbeitet die KI? Welches Vorwissen darf sie voraussetzen?

Kontext / Rahmenbedingungen: Branche, Produkt, interne Regeln, regulatorischer Rahmen.

Sprache: In welcher Sprache soll die KI antworten?



4. Arbeitsweise (Prozess)

Wie soll die KI vorgehen?

- Zuerst Rückfragen stellen (max. ____, vor dem ersten Output / iterativ)
- Danach eine Gliederung erstellen und bestätigen lassen
- Dann einen Entwurf erzeugen
- Anschließend selbst prüfen und überarbeiten

Eigener Prozess (optional):

5. Output-Vorgaben

Format: (z. B. Headline + Lead + zwei Absätze, Tabelle, strukturierte Liste)

Länge: (z. B. maximal 150 Wörter)

Ton: (z. B. sachlich, professionell, neutral, freundlich)

Sprache: Deutsch / Englisch / andere

6. Wissensquellen & Constraints

Erlaubte Quellen: Was darf die KI nutzen? (z. B. nur bereitgestellte Dokumente / eigenes Trainingswissen / Websuche)

Priorisierung: Was gilt, wenn Quellen widersprechen?

No-Gos – Was darf die KI auf keinen Fall tun?

- Keine Preise oder Termine nennen
- Keine Versprechen oder Superlative
- Keine Annahmen ohne explizite Kennzeichnung
- Keine externen Quellen ohne Freigabe
- Keine Daten oder Prozentzahlen ausdenken
- Weitere:

7. Qualitäts-Check (Self-Check)

Die KI prüft ihr Ergebnis selbst auf:

- Unklare oder mehrdeutige Aussagen



- Überzogene Behauptungen
- Fehlende oder nicht belegte Informationen
- Risiken für Marke, Vertrauen oder rechtliche Compliance
- Sprachliche Qualität und Zielgruppenpassung

Weitere Kriterien:

8. Agentische Erweiterung (nur für KI-Agenten)

Zugelassene Tools / Quellen: (z. B. interne Dokumente, Datenbanken, APIs – mit Priorisierung)

Entscheidungslogik:

- Wann handelt die KI selbst?
- Wann fragt sie nach?
- Wann stoppt sie und wartet auf Freigabe?

9. Stop-Kriterien & Eskalation

Die KI MUSS stoppen oder eskalieren, wenn:

- Zentrale Informationen fehlen
- Aussagen rechtlich, ethisch oder reputativ kritisch sind
- Quellen widersprechen und nicht aufgelöst werden können
- Unsicherheit den definierten Schwellenwert überschreitet

Eskalation an: (Name / Rolle / Kanal – wer wird informiert?)

10. Versionierung & Pflege

Owner: Wer ist verantwortlich für diesen Prompt?

Letzte Aktualisierung:

Nächste Überprüfung: (z. B. quartalsweise, nach jedem größeren Modellupdate)

Änderungshistorie: