

E02

KI IST KEIN TOOLPROBLEM

Warum Führbarkeit vor Toolwahl kommt.

Viele Unternehmen beginnen mit Modellen, Lizenzen und Funktionen. Ein leistungsfähiges Tool wird jedoch erst dann zu einem verlässlichen Arbeitsinstrument, wenn Rolle, Kontext, Grenzen, Qualitätsmaßstäbe und Freigaben geklärt sind.

MERKSATZ

Nicht das Tool führt. Die Architektur.

1

Toolwahl ist nur ein Teil

Das stärkste Modell löst keine unklaren Rollen oder fehlenden Prüfwege.

2

Architektur schafft Führung

Sie verbindet Unternehmensziel, Kontext, Arbeitsablauf und Verantwortung.

3

Geschäftslogik bleibt bestehen

Tools können wechseln; die übergeordnete Arbeitslogik bleibt nutzbar.

TOOL-FIRST ODER ARCHITEKTUR-FIRST?

Frage	Tool-first	Architektur-first
Start	Welches Modell kaufen wir?	Welche Aufgabe soll besser werden?
Nutzung	Jeder probiert individuell.	Rollen und Kriterien sind wiederverwendbar.
Risiko	Grenzen bleiben implizit.	Datenregeln und Freigaben sind definiert.
Messung	Aha-Effekt und Gefühl.	Zeit, Nacharbeit und Qualität werden geprüft.

PRAXISBEISPIEL: PREISNACHLASS-ANFRAGE

Ohne Architektur entstehen schnell drei völlig verschiedene Antworten: zu weich, zu hart oder mit ungeprüfter Zusage. Mit klarer Rolle, Preislinie, Tonalität und Freigabe formuliert das Modell - die Architektur führt.

KURZCHECK

- ☐ Ein klarer Anwendungsfall ist in einem Satz beschreibbar.
- ☐ Erlaubte und sensible Daten sind getrennt.
- ☐ Wichtige Ergebnisse haben einen Freigabepunkt.
- ☐ Nutzen wird über mehrere Fälle gemessen.

DIE FÜNF EBENEN EINER FÜHRBAREN NUTZUNG

- 1 Ziel und Nutzen: Welche konkrete Verbesserung soll entstehen?
- 2 Rolle und Verantwortung: Wer nutzt, prüft und entscheidet?
- 3 Kontext und Wissen: Welche Informationen sind wirklich notwendig?
- 4 Qualität und Prüfung: Woran erkennt man ein gutes Ergebnis?
- 5 Arbeitsablauf: Wie wird aus der Antwort ein sicherer nächster Schritt?

PRAXIS-TRANSFER: IN DREI SCHRITTEN STARTEN

1

Anwendungsfall wählen

Eine konkrete, häufige Aufgabe auswählen - z. B. Angebot, Kundenantwort oder Meeting-Briefing.

2

Führungsschicht definieren

Rolle, Kontext, Datenregeln, Qualitätskriterien und Freigabe festhalten.

3

Werkzeuge vergleichen

Erst jetzt Modelle mit denselben typischen und schwierigen Fällen testen.

TRANSFERFRAGE FÜR IHREN BETRIEB

Welche wiederkehrende Aufgabe würde bei klarer Führung sofort messbar besser?

ISO/IEC 42001 - AI management systems
International Organization for Standardization

Quelle

AI Risk Management Framework
National Institute of Standards and Technology

Quelle

E03

VOM SPIELZEUG ZUM WERKZEUG

Wann aus Faszination ein verlässlicher Arbeitsnutzen wird.

Ein überraschend guter Text oder eine schnelle Analyse erzeugt Aufmerksamkeit. Geschäftlicher Nutzen entsteht erst, wenn Ergebnisse wiederholbar, bewertbar und in einen realen Arbeitsablauf eingebettet sind.

MERKSATZ

Aus Faszination wird ein Werkzeug.

1

Aha-Effekt ist kein Betriebsnutzen

Ein beeindruckender Einzelversuch beweist noch keinen verlässlichen Prozess.

2

Ein Werkzeug hat einen Zweck

Aufgabe, Nutzer, Qualitätsmaßstab und Übergabe sind klar definiert.

3

Wiederholbarkeit entscheidet

Gute Ergebnisse müssen auch beim nächsten Fall und bei anderen Nutzern tragen.

VIER REIFESTUFEN DER KI-NUTZUNG

Stufe	Typisches Bild	Nächster Schritt
1 Experiment	Einzelne Tests und Aha-Momente.	Zweck und Kriterien festlegen.
2 Hilfsmittel	Eine Aufgabe wird schneller vorbereitet.	Kontext und Ablauf stabilisieren.
3 Werkzeug	Mehrere Nutzer erzielen vergleichbare Qualität.	Messung und Zuständigkeit klären.
4 Arbeitsmodell	KI ist kontrolliert im Prozess verankert.	Laufend evaluieren und verbessern.

PRAXISBEISPIEL: TECHNISCHE ANGEBOTSERSTELLUNG

Als Versuch schreibt KI einen schönen Absatz. Als Werkzeug kennt sie Zielkunde, Leistungsumfang, Sprache, Ausschlüsse und Qualitätskriterien. Der Mensch prüft Fachangaben und trägt die Verantwortung.

KURZCHECK

- ☐ Der Fall tritt regelmäßig auf.
- ☐ Das Ergebnis lässt sich klar bewerten.
- ☐ Eine fachkundige Person kann prüfen.
- ☐ Der Prozess besitzt Start- und Endpunkt.

SECHS MERKMALE EINES ECHTEN WERKZEUGS

- 1
- Zweck: Erfolg und Misserfolg sind unterscheidbar.
- 2
- Eingaben: Relevante Informationen sind strukturiert; sensible Daten bleiben außen vor.
- 3
- Qualität: Inhalt, Ton und Vollständigkeit sind prüfbar.
- 4
- Menschliche Prüfung: Folgen, Haftung und Reputation bleiben kontrolliert.
- 5
- Übergabe: Nach dem Entwurf ist klar: prüfen, ergänzen, freigeben oder versenden.
- 6
- Messung: Zeitgewinn, Nacharbeit und Nutzung werden beobachtet.

PRAXIS-TRANSFER: IN DREI SCHRITTEN STARTEN

1

Aufgabe festlegen

Einen wiederkehrenden Engpass, verantwortliche Nutzer und ein klares Ergebnisbild bestimmen.

2

Arbeitslogik bauen

Kontext, Beispiele, Grenzen, Ausgabeformat und Prüfung in einer ersten Version bündeln.

3

30 Tage messen

Zeit, Korrekturschleifen, Konsistenz und tatsächliche Nutzung dokumentieren.

TRANSFERFRAGE FÜR IHREN BETRIEB

Welcher heutige KI-Versuch könnte innerhalb von 30 Tagen zu einem echten Werkzeug werden?

OpenAI Business - Learning Hub

OpenAI

Quelle

AI Risk Management Framework

National Institute of Standards and Technology

Quelle

E04

EIN PROMPT IST KEIN SYSTEM

Warum gute Formulierungen wichtig sind - aber allein nicht tragen.

Ein guter Prompt verbessert einzelne Ergebnisse. Sobald mehrere Nutzer, wechselnde Fälle, sensible Informationen oder feste Qualitätsanforderungen hinzukommen, braucht es jedoch eine wiederverwendbare Struktur statt isolierter Textbefehle.

MERKSATZ

Prompts starten. Architektur trägt.

1 Prompts bleiben wichtig

Sie formulieren Aufgaben klar und geben dem Modell Orientierung.

2 Ein System ergänzt den Prompt

Kontext, Beispiele, Regeln, Prüfung und Versionierung machen Ergebnisse belastbarer.

3 Qualität muss testbar sein

Nicht der längste Prompt gewinnt, sondern eine zuverlässig funktionierende Arbeitslogik.

PROMPT UND ARBEITSARCHITEKTUR

Baustein	Einzelner Prompt	Arbeitsarchitektur
Aufgabe	Was soll jetzt entstehen?	Einordnung in Rolle, Ziel und Prozess.
Kontext	Wird oft neu eingetippt.	Stabile und variable Inhalte sind getrennt.
Qualität	Oft nur „gut“ oder „professionell“.	Kriterien, Beispiele und Ausschlüsse sind konkret.
Risiko	Hängt von der Einzelanfrage ab.	Daten- und Freigaberegeln sind verankert.

PRAXISBEISPIEL: „ERSTELLE EIN ANGEBOT“

Der Prompt kennt weder Zielkunde noch Leistungsgrenze, Tonalität, Preislogik oder Ausschlüsse. In einer Architektur wird er Teil eines Pakets aus Rolle, Unternehmenskontext, Beispielen, Qualitätskriterien und Prüfung.

KURZCHECK

- ☐ Stabile Informationen müssen nicht immer neu eingegeben werden.
- ☐ Variable Kundendaten sind vom Grundsystem getrennt.
- ☐ Es gibt Beispiele für akzeptable Ergebnisse.
- ☐ Das System weiß, wann es stoppen oder nachfragen muss.

SECHS BAUSTEINE ÜBER DEM PROMPT

- 1 Rolle: Aus welcher Verantwortung arbeitet die KI?
- 2 Kontext: Welche stabilen und fallbezogenen Angaben sind notwendig?
- 3 Aufgabenlogik: Welche Schritte, Rückfragen und Stopps gelten?
- 4 Beispiele: Gute und schlechte Muster konkretisieren die Erwartung.
- 5 Qualitätskriterien: Inhalt, Ton, Vollständigkeit, Risiko und Format werden prüfbar.
- 6 Freigabe und Versionierung: Änderungen werden mit denselben Fällen getestet.

PRAXIS-TRANSFER: IN DREI SCHRITTEN STARTEN

1 Prompts ordnen

Bestehende Formulierungen nach Aufgabe, Zielgruppe und Risiko gruppieren.

2 Konstanten auslagern

Rolle, Ton, Wissen, Grenzen und Qualitätskriterien zentral definieren.

3 Versionen testen

Jede Änderung mit denselben normalen, schwierigen und unvollständigen Fällen vergleichen.

TRANSFERFRAGE FÜR IHREN BETRIEB

Welche wiederkehrenden Bestandteile Ihrer besten Prompts gehören in ein dauerhaftes System?

Prompt Engineering - Überblick

Anthropic Claude API Docs

Quelle

A practical guide to building agents

OpenAI for Business

Quelle

E05

KONTEXT MACHT KI BRAUCHBAR

Warum Qualität häufig vor der eigentlichen Antwort entsteht.

Eine KI kann sprachlich überzeugen und trotzdem am Unternehmen vorbeiarbeiten. Ursache ist häufig nicht das Modell, sondern fehlender, veralteter oder ungeordneter Kontext. Professionelle Architektur liefert die richtigen Informationen - nicht möglichst viele.

MERKSATZ

Qualität beginnt vor der Antwort.

1

Kontext ist Arbeitsgedächtnis

Das Modell nutzt nur, was im aktuellen Rahmen verfügbar und verständlich ist.

2

Mehr Daten sind nicht automatisch besser

Relevanz, Aktualität und klare Grenzen sind wichtiger als Masse.

3

Stabil und variabel trennen

Grundlagen bleiben wiederverwendbar; Falldaten werden gezielt ergänzt.

FÜNF ARTEN VON KONTEXT

Art	Beispiele	Nutzen
Unternehmen	Leistung, Positionierung, Ton.	Verhindert generische Antworten.
Rolle	Geschäftsführung, Vertrieb, Projektleitung.	Bestimmt Verantwortung und Perspektive.
Aufgabe	Ziel, Empfänger, Format, Frist.	Macht die Anfrage konkret.
Wissen	Freigegebene Fakten, Dokumente, Beispiele.	Erhöht fachliche Passung.
Grenzen	Sensible Daten, Zusagen, Freigaben.	Schützt Unternehmen und Kunden.

PRAXISBEISPIEL: KUNDENBESCHWERDE

Ohne Kontext entsteht eine allgemeine Entschuldigung. Mit Leistungsumfang, bisheriger Kommunikation, Tonalität und der Regel, keine Schuld oder Kulanz vor Prüfung zuzusagen, wird die Antwort geschäftlich passend.

KURZCHECK

- ☐ Rolle, Ziel und Empfänger sind klar.
- ☐ Nur notwendige Kundendaten werden verwendet.
- ☐ Fakten und Annahmen sind getrennt.
- ☐ Quelle und Aktualität des Wissens sind erkennbar.

CONTEXT ENGINEERING IN FÜNF SCHICHTEN

- 1
- Stabiler Grundkontext: Rolle, Unternehmenssprache, Leistungsrahmen und Qualitätsregeln.
- 2
- Situativer Kontext: Kunde, Ziel, Verlauf, gewünschtes Ergebnis und Einschränkungen.
- 3
- Abrufbares Wissen: Nur relevante Ausschnitte aus freigegebenen Quellen.
- 4
- Sensible Informationen: Daten minimieren, anonymisieren und unnötige Details weglassen.
- 5
- Aktualität: Preise, Richtlinien und Zuständigkeiten regelmäßig pflegen.

PRAXIS-TRANSFER: IN DREI SCHRITTEN STARTEN

1

Rolle und Ziel klären

Wer spricht, für wen, mit welchem Ergebnis und in welchem Format?

2

Verlässliche Fakten wählen

Nur relevante, freigegebene und aktuelle Informationen bereitstellen.

3

Grenzen setzen

Sensible Daten minimieren, Annahmen markieren und Aktualität regelmäßig prüfen.

TRANSFERFRAGE FÜR IHREN BETRIEB

Welche drei Informationen fehlen der KI heute am häufigsten, damit Antworten wirklich zu Ihrem Unternehmen passen?

Effective context engineering for AI agents
Anthropic Engineering

Quelle

Context windows
Anthropic Claude API Docs

Quelle

E06

AGENTEN BRAUCHEN ARCHITEKTUR

Warum Handlungsfähigkeit eine stärkere Steuerungsebene verlangt.

Ein KI-Agent kann Informationen abrufen, Schritte planen und über Werkzeuge Aktionen auslösen. Je mehr ein System selbstständig handeln darf, desto klarer müssen Auftrag, Berechtigungen, Zustand, Kontrolle und Rückfallwege geregelt sein.

MERKSATZ

Agenten handeln. Architektur führt.

1 Agent ist mehr als Chat

Er steuert Abläufe und kann externe Systeme oder Werkzeuge nutzen.

2 Autonomie braucht Grenzen

Berechtigungen, Freigaben und reversible Schritte müssen zum Risiko passen.

3 Klein starten ist professionell

Ein enger Agent mit wenigen Tools ist oft belastbarer als ein zu komplexes Netzwerk.

VON DER ANTWORT ZUR HANDLUNG

Stufe	Agent darf	Kontrolle
0 Auskunft	Strukturieren und vorschlagen.	Mensch handelt vollständig selbst.
1 Entwurf	E-Mail oder Bericht vorbereiten.	Prüfung vor externer Wirkung.
2 Vorbereitung	Daten abrufen, reversible Schritte vorbereiten.	Freigabe vor Versand oder Änderung.
3 Begrenzte Aktion	Niedrigrisiko-Aktionen in klaren Regeln.	Monitoring und definierte Stopps.
4 Hochrisiko	Finanzielle, rechtliche, irreversible Aktionen.	Keine autonome Entscheidung.

PRAXISBEISPIEL: AGENT FÜR NACHFASSUNGEN

Sicherer Start: freigegebene CRM-Daten lesen, offene Vorgänge erkennen und einen Entwurf erstellen. Keine Preisänderung, Vertragszusage oder Aussendung ohne Freigabe.

KURZCHECK

- ☐ Der Auftrag ist eng und eindeutig.
- ☐ Jedes Tool besitzt nur minimale Rechte.
- ☐ Irreversible Aktionen brauchen Freigabe.
- ☐ Stopps, Fehlergrenzen und Fallbacks sind definiert.

SIEBEN ARCHITEKTURBAUSTEINE

- 1 Rolle: Auftrag, Ziel, Zuständigkeit und ausgeschlossene Handlungen.
- 2 State: Was ist erledigt, offen und wann endet der Auftrag?
- 3 Memory: Was darf gespeichert, wiederverwendet oder gelöscht werden?
- 4 Tool-Rechte: Lesen, Schreiben, Senden und Bezahlen getrennt behandeln.
- 5 Guardrails: Eingaben, Ausgaben und Aktionen auf Grenzen prüfen.
- 6 Evaluation: Erfolg, Fehler und Abbrüche über reale Fälle messen.
- 7 Fallback: Bei Unsicherheit stoppen und nachvollziehbar an Menschen übergeben.

PRAXIS-TRANSFER: IN DREI SCHRITTEN STARTEN

1 Workflow begrenzen

Mit einer Aufgabe, wenigen Tools und einem klaren Endzustand beginnen.

2 Entwurf vor Aktion

Der Agent bereitet vor; externe oder irreversible Wirkung bleibt freigabepflichtig.

3 Kontrolliert erweitern

Fehler dokumentieren, Rechte staffeln und Autonomie nur bei belegter Zuverlässigkeit erhöhen.

TRANSFERFRAGE FÜR IHREN BETRIEB

Welche Agenten-Aktion wäre nützlich, aber noch sicher genug, um zunächst nur als Entwurf zu starten?

A practical guide to building agents
OpenAI for Business

Quelle

Building Effective AI Agents
Anthropic Research

Quelle

E07

GOVERNANCE BREMST NICHT

Wie klare Grenzen sichere Geschwindigkeit ermöglichen.

Governance wird oft mit Bürokratie verwechselt. Gute Governance beantwortet praktische Fragen: Wer darf was? Welche Daten sind erlaubt? Wann braucht es Prüfung? Wer trägt Verantwortung? Klarheit reduziert Rückfragen und Schattennutzung.

MERKSATZ

Klare Grenzen schaffen Tempo.

1

Regeln reduzieren Reibung

Teams wissen, welche Nutzung erlaubt ist und wo sie stoppen müssen.

2

Governance ist Arbeitslogik

Rollen, Datenklassen und Freigaben werden in den Alltag übersetzt.

3

Kontrolle ermöglicht Skalierung

Was verständlich dokumentiert ist, kann sicherer erweitert werden.

WO UNKLARE KI-NUTZUNG ZEIT VERLIERT

Unklarheit	Typische Folge	Klare Regel
Daten	Unsicherheit bei Eingaben.	Datenklassen und Beispiele.
Rollen	Niemand verantwortet Ergebnis oder Risiko.	Owner, Nutzer, Prüfer, Eskalation.
Qualität	Antworten ohne gemeinsame Maßstäbe.	Kriterien, Stichproben, Freigaben.
Tools	Schattennutzung und Lizenzchaos.	Freigegebene Werkzeuge und Antragsweg.
Fehler	Probleme werden versteckt oder wiederholt.	Meldung, Korrektur und Verbesserung.

PRAXISBEISPIEL: DATENAMPEL

Grün: öffentliche Informationen. Gelb: interne Inhalte nur anonymisiert oder in freigegebenen Systemen. Rot: Passwörter, Bank-, Gesundheits- oder andere hochsensible Daten. Die konkrete Einteilung muss zum Unternehmen passen.

KURZCHECK

- ☐ Genutzte KI-Tools sind bekannt.
- ☐ Mitarbeitende kennen erlaubte und unerlaubte Daten.
- ☐ Wichtige Fälle haben Verantwortliche und Freigaben.
- ☐ Fehler und Grenzfälle werden dokumentiert und ausgewertet.

PRAXIS-TRANSFER: IN DREI SCHRITTEN STARTEN

1

Inventar schaffen

Genutzte Tools, Nutzergruppen und reale Anwendungsfälle sichtbar machen.

2

Regeln vereinfachen

Datenampel, Rollen, Freigaben und wenige klare No-Gos festlegen.

3

Pilot und Review

Einen risikoarmen Fall testen, Erfahrungen auswerten und Regeln nachschärfen.

TRANSFERFRAGE FÜR IHREN BETRIEB

Welche eine klare Regel würde in Ihrem Team sofort Unsicherheit oder Schattennutzung reduzieren?

ISO/IEC 42001 - AI management systems
International Organization for Standardization

Quelle

AI Risk Management Framework
National Institute of Standards and Technology

Quelle

Allgemeine Orientierung - keine Rechts-, Datenschutz-, Audit- oder Zertifizierungsberatung.