

Toll E in A gent M acht's

Rainer Tolksdorf

12.03.2026 <https://tolksdorf.digital>
+41 78 405 5095 rainer@tolksdorf.digital





TEAM – Toll Ein Agent Macht's

- **Wir machen gemeinsam Einen Agenten**
 - Ablauf wie bei einem AI- / IT-Projekt
 - Hands-On Beispiel bauen
 - Als Basis für weiteres nutzen
- **Präsentation und Materialien Online**
 - <https://tolksdorf.digital/en/downloads-lectures-and-course-materials>



TEAM – Toll Ein Agent Macht's

1

- KI & AI & LLM & DSGVO

2

- Innovation:
KI im Betrieb

3

- AI Studio Mistral
- n8n Workflow & AI

4

- Playbooks, Role
Description & Setup

5

- Engineering mit AI:
Vibe Mode & CAISE

6

- AI Agent bauen



TEAM – Toll Ein Agent Macht's

1

- KI & AI & LLM & DSGVO



KI & AI & LLM & DSGVO

*KI → Künstliche **Intelligenz***

*LLM → **Large Language Model***

Was sind Intelligenz & Bewusstsein?

Leibniz (17. Jh.) «Mechanische Mühle»



John Searle (1980) «Chinese Room»



LLM-Debatte heute



KI & AI & LLM & DSGVO

*On Demand / On-Premise -
DSGVO «pragmatisch» ausgelegt*

Firmen-
kontext

Fragen

Persönl.
Kontext

Google Index

AI Weltwissen

KI & AI & LLM & DSGVO

*On Demand / On-Premise -
DSGVO «eng» ausgelegt*

Fragen
Firmen-
kontext
Persönl.
Kontext
SearXNG, ...

Bewusst geteiltes und kuratiertes öffentliches Wissen

- Wissenschaft
- Open Source
- Wörterbücher
- Bücher
- Wikipedia
- Fachartikel
- Öffentliche Gespräche
- ...

Problematisch

- *persönliche Profile*
- *private Kommunikation*
- *personenbezogene Dokumente*
- ...

KI & AI & LLM & DSGVO

*On-Premise & abgeschottet
streng DSGVO konform*

Firmen-
kontext

Fragen

Persönl.
Kontext

Bewusst geteiltes Wissen

- Wissenschaft
- Open Source
- Wörterbücher
- Bücher
- Wikipedia
- Fachartikel
- Öffentliche Gespräche
- ...

Problematisch

- *persönliche Profile*
- *private Kommunikation*
- *personenbezogene Dokumente*
- ...



KI & AI & LLM & DSGVO

On-Premise / On-Demand LLM Einsatzszenarien:

Workshop

DSGVO «pragmatisch»

- Weltwissen
- Erfüllt EU AI Act
- In EU / selbst gehostet
- «Server side hosting» mit Anonymisierung ermöglicht alle LLMs

DSGVO «eng» ausgelegt

- Selbst kuratierte und trainierte Inhalte
- Erfüllt EU AI Act
- In EU / selbst gehostet

Streng DSGVO konform

- Selbst kuratierte und trainierte Inhalte
- Abgeschottet
 - Anwälte
 - Finanzen, Steuern
 - Geheimnisse



TEAM – Toll Ein Agent Macht's

2

- Innovation:
KI im Betrieb

Innovation: KI im Betrieb

Gut gemeint, kommt nicht immer gut an.

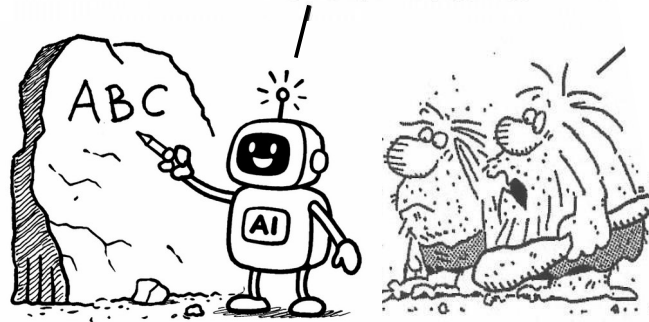
*Die einen wollen aufwerten,
die andern empfinden das als entwertend.*



Quelle unbekannt

Innovation: KI im Betrieb

*KI kann ungewollt
Ängste und Vorbehalte
erzeugen*

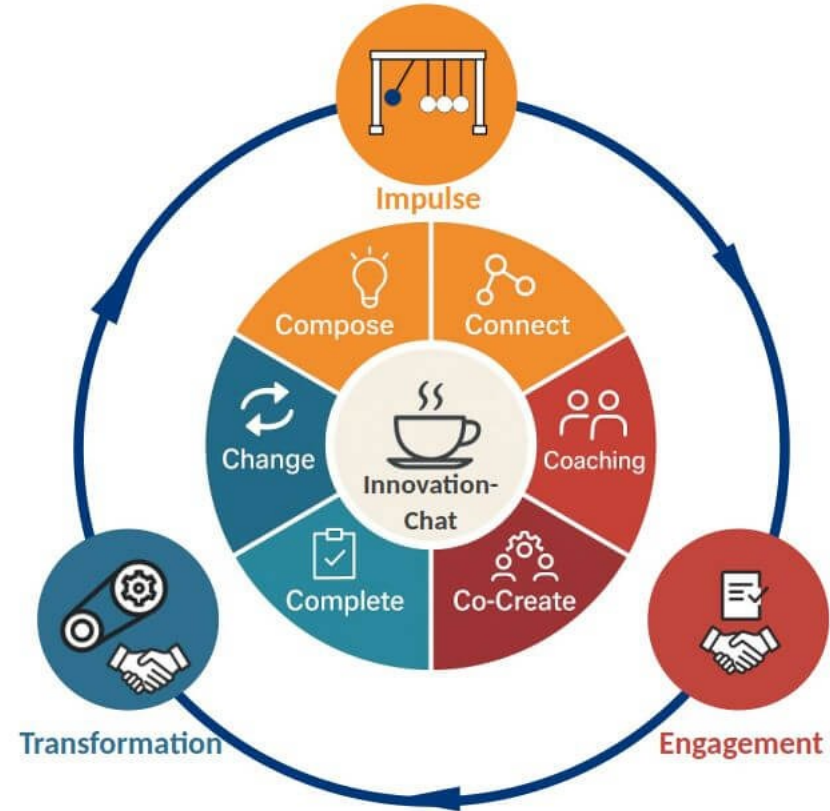


*...und das nachdem wir
damit Erfahrung haben,
sind wir nun überflüssig.
-MUCHT!!*

Quelle unbekannt

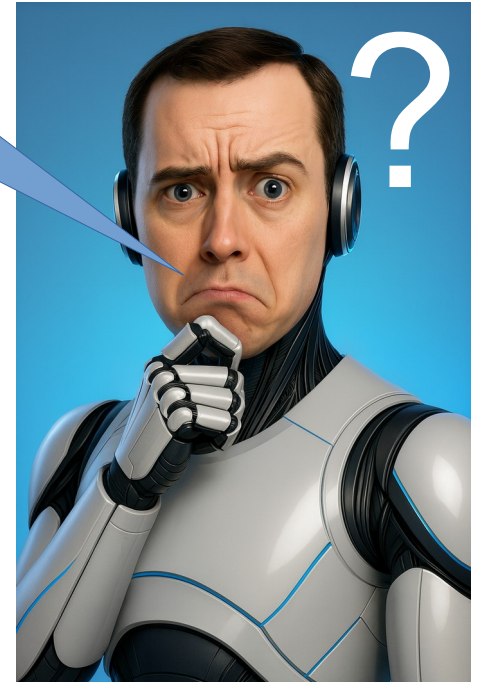
Innovation: KI im Betrieb

Lösung:
Fokus positive Erlebnisse
und Business Effektivität



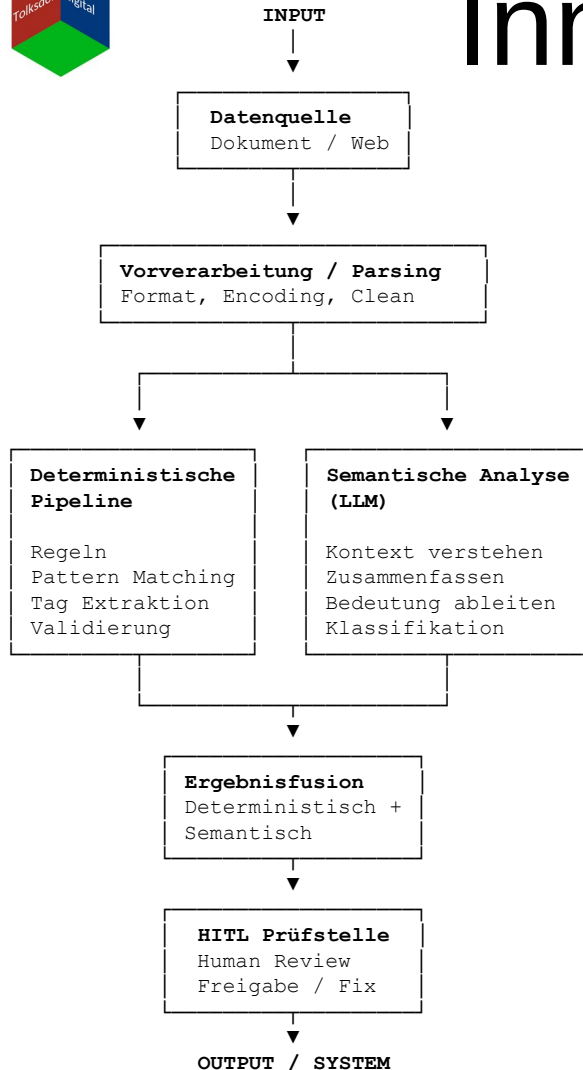
Innovation: KI im Betrieb

AI Agent -
Agentic AI ???

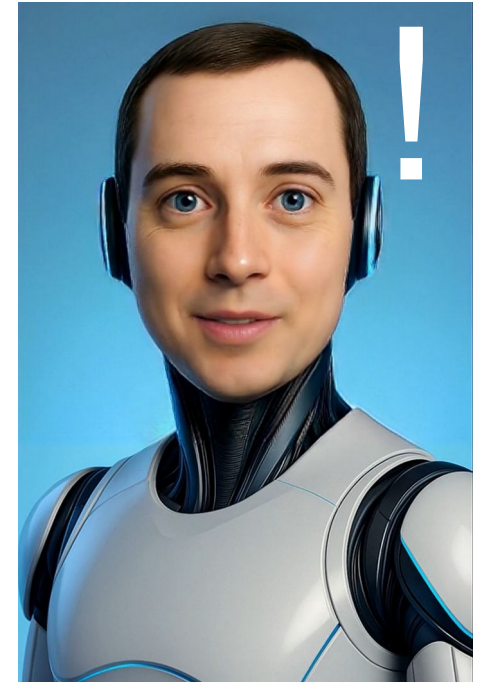


Innovation: KI im Betrieb

Tipps zur Automatisierung



- Fixe Regeln
→ Deterministischer Pipeline
Bsp. Unterschriftenregel
- Semantische Analyse
→ OCR Rechnungsbelege
- Ergebnisse müssen prüfbar und reparierbar sein
- Mensch ist immer verantwortlich «Human in the Loop (=HITL)»



- Beispiel: n8n Workflows



TEAM – Toll Ein Agent Macht's

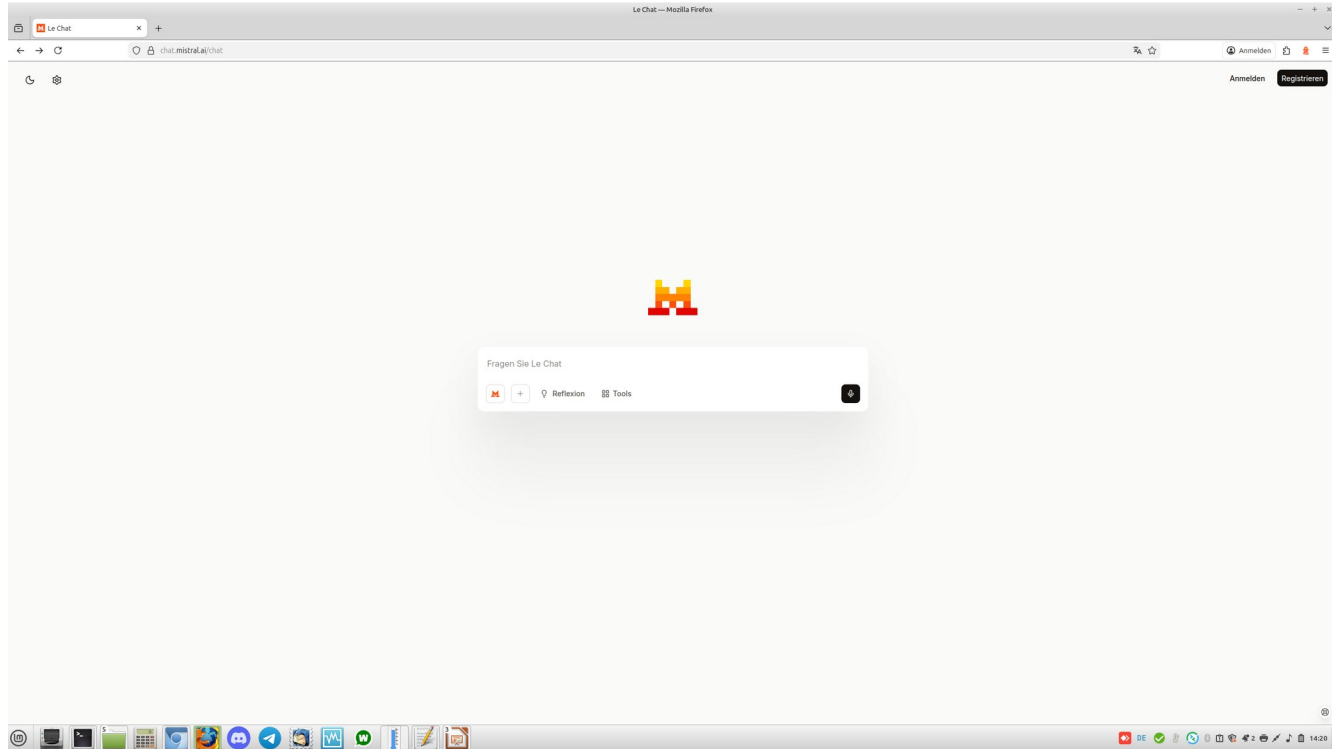
3

- **Mistral Agent**
- **AI Studio Mistral**
- **n8n Workflow & AI**



Mistral Agent / AI Studio & n8n AI Agent

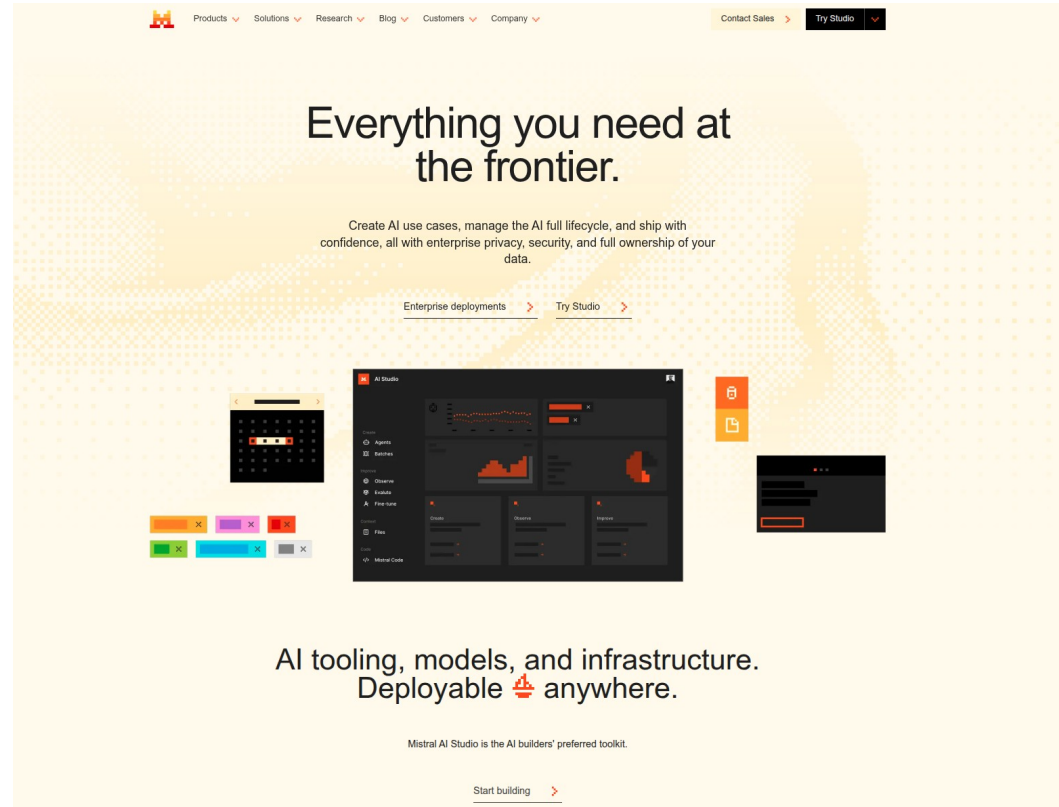
<https://chat.mistral.ai>





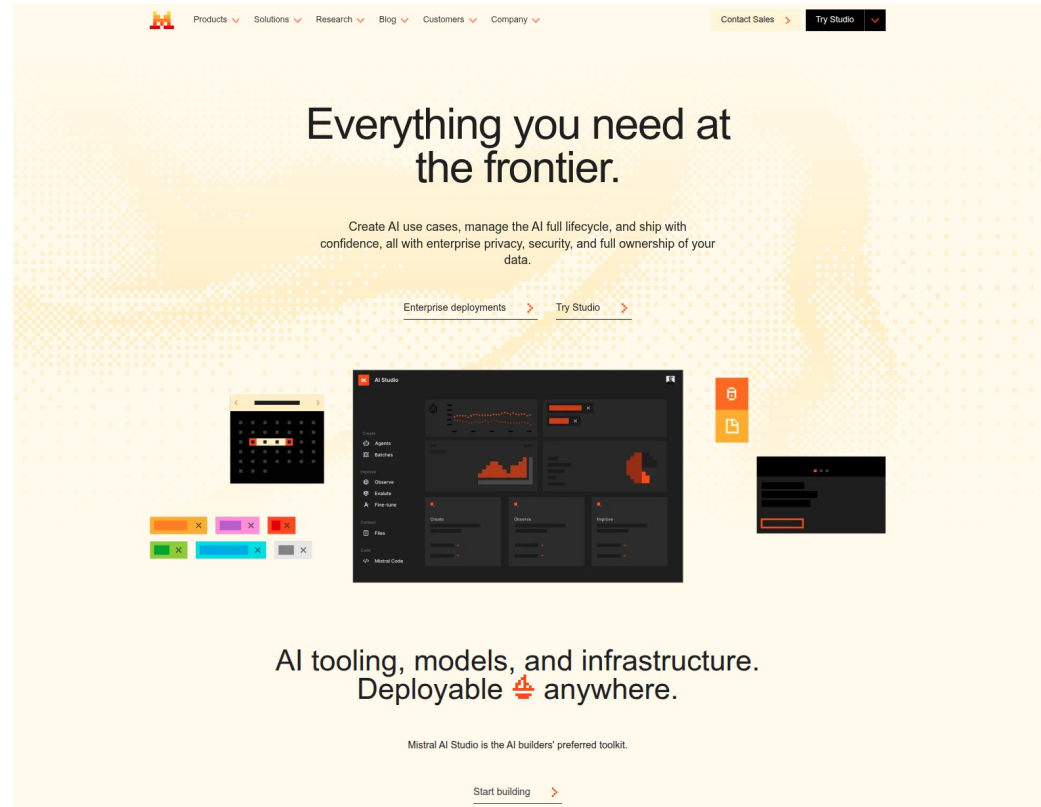
Mistral Agent / AI Studio & n8n AI Agent

<https://mistral.ai/products/studio>



AI Studio Mistral & n8n AI Agent

<https://mistral.ai/products/studio>

The image shows the landing page for Mistral AI Studio. The page has a light yellow background with a subtle pattern of small dots. At the top, there is a navigation bar with links for Products, Solutions, Research, Blog, Customers, and Company. On the right side of the navigation bar, there are links for Contact Sales and Try Studio. The main heading is "Everything you need at the frontier." Below this, a subheading reads: "Create AI use cases, manage the AI full lifecycle, and ship with confidence, all with enterprise privacy, security, and full ownership of your data." There are two links below the subheading: Enterprise deployments and Try Studio. The central part of the page features a large, dark-themed screenshot of the Mistral AI Studio interface, which displays various charts, graphs, and data visualizations. To the left of the main screenshot, there are several smaller, colorful icons representing different AI models or tools. To the right, there is a small, dark-themed screenshot of a terminal or command prompt. At the bottom of the page, the text reads: "AI tooling, models, and infrastructure. Deployable anywhere." Below this, a small line of text states: "Mistral AI Studio is the AI builders' preferred toolkit." At the very bottom, there is a link for Start building.



AI Studio Mistral & n8n AI Agent

Kurze Vorführung zum Vergleich aller drei Realisierungsplattformen



TEAM – Toll Ein Agent Macht's

Handout

4

- Playbooks, Role Description & Setup



TEAM – Toll Ein Agent Macht's

5

- Engineering mit AI:
Vibe Mode & CAISE



Engineering mit AI: Vibe + CAISE

• VIBE Mode

“Good Vibrations” Coding

Im VIBE Mode arbeiten Mensch und KI frei und kreativ zusammen – ideal für Brainstorming, Spezifikation und schnelle Prototypen.

- Anwender arbeiten überwiegend instinktiv auf diese Weise oder nutzen KI als Orakel
- KI ist Partner im Flow → schnelle Impulse, unkonventionelle Lösungen.
- „Spaghetti“ ist hier erlaubt, sogar erwünscht – Hauptsache, Ideen entstehen.
- Vergleich: Jazz-Improvisation im Studio.

• CAISE Mode

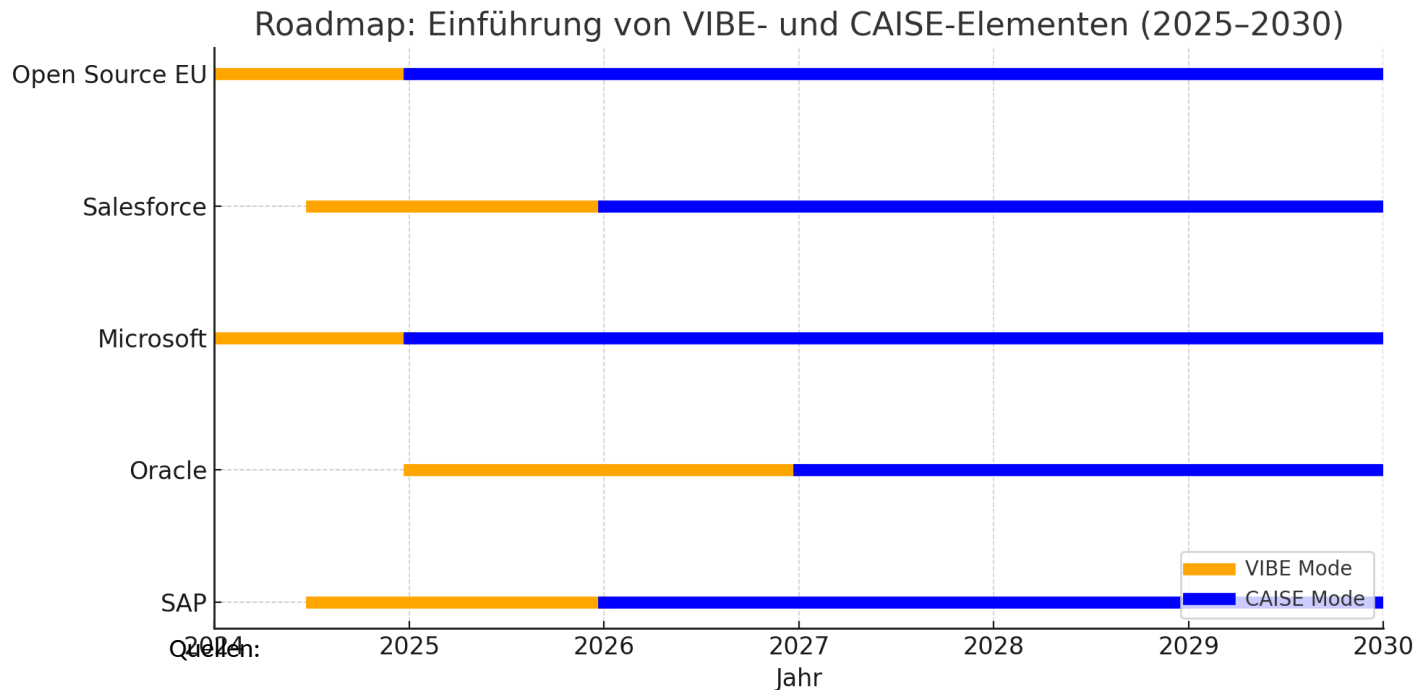
Collaborative AI Systems Engineering

„CAISE macht aus Kreativität ein strukturiertes, dokumentiertes und nachhaltiges Engineering, in dem Mensch und KI zusammenarbeiten und der Mensch die Verantwortung behält.“

- Notwendig für **Teamarbeit, Umsetzung, Nachhaltigkeit.**
- Rollen und Dokumentation verhindern Chaos.
- Ergebnisse sind nachvollziehbar, testbar, wiederverwendbar.
- Vergleich: Das improvisierte Thema wird in eine Partitur gegossen und vom Orchester aufgeführt.



Engineering mit AI: Vibe + CAISE



Anmerkung: die jeweiligen Hersteller verwenden eigene Bezeichnungen für CAISE

- SAP & OpenAI Partnerschaft: <https://openai.com/global-affairs/openai-for-germany>
- SAP Business AI / Joule: <https://www.sap.com/products/artificial-intelligence.html>
- Microsoft Copilot Strategy: <https://blogs.microsoft.com/blog/2023/11/15/copilot-everywhere/>
- Oracle AI Services: <https://www.oracle.com/artificial-intelligence/>
- Salesforce Einstein GPT: <https://www.salesforce.com/de/products/einstein/ai/>



Engineering mit AI: Vibe + CAISE

Fazit

- Beides ist sinnvoll und ergänzt sich.
- Problematisch wird es nur, wenn Firmen ***n*ie** aus dem VIBE Mode rauskommen
→ dann entstehen unwartbare „KI-Spaghetti-Ergebnisse“.
- Durch CAISE werden VIBE Ergebnisse nachhaltig nutzbar
 - Ideen → VIBE
 - Umsetzung → CAISE



TEAM – Toll Ein Agent Macht's

