

Neue Akteure in
der Hochschultransformation:

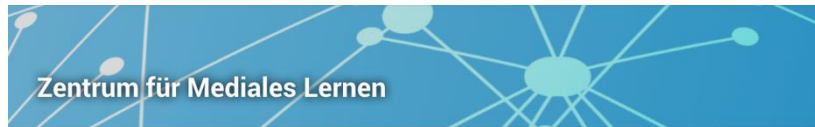
Einstieg in das Arbeiten mit KI-Agenten

hAlgher Education Day 2026:
Fachspezifisch lehren und lernen mit
Künstlicher Intelligenz
06. Oktober 2026, Karlsruhe

Andreas Sexauer (KIT)



Anleitungen und Theorie zum Nachlesen ...



Startseite > GenAI@KIT > Starthilfe mit KI > Agentische KI

Agentische KI

Agentische KI steht für den nächsten großen Durchbruch in der Entwicklung künstlichen Aufgaben selbstständig. KI bewegt sich damit aus dem Chatfenster hinaus in reaktiven und generativen KI.

Was ist ein KI-Agent?

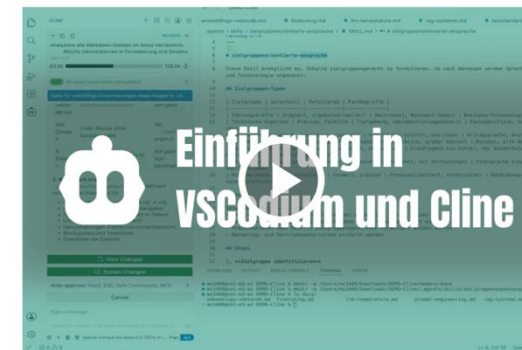
Ein KI-Agent ist ein Softwaresystem, das ein Ziel verfolgt und dafür selbstständig Maßnahmen ausführen kann. Im Unterschied zu herkömmlichen KI-Anwendungen kann ein Agent:

- natürliche Sprache verstehen,
- Informationen auswerten

<https://www.zml.kit.edu/ki-agenten>



<https://hochschulforumdigitalisierung.de/news/publikation-agentische-ki/>



Videoeinführung in das Arbeiten mit VSCode und Cline: Von der Installation bis zur ersten Aufgabe

**Wir stehen an einer Schwelle.
Es gilt das Chatfenster zu
verlassen und KI bei der
Ausführung komplexer Abläufe zu
orchestrieren. Ähnlich wie das
Aussteuern einer
wissenschaftlichen Hilfskraft.**



EXCEL VS. TASCHENRECHNER = KI-AGENTEN VS. KLASSISCHER KI CHAT

KI-AGENTEN: NICHT NUR SCHNELLER – SONDERN FUNDAMENTAL BESSER

TRADITIONELL

TASCHENRECHNER



- Jede Berechnung einzeln durchführen
- Ergebnisse manuell übertragen
- Fehleranfällig
- Zeitaufwendig

EXCEL (TABELLENKALKULATION)



Formeln verknüpfen,
automatische
Neuberechnung
bei Änderungen!



- ✓ Verknüpfte Formeln
- ✓ Automatische Updates
- ✓ Analysen & Auswertungen leicht gemacht
- ✓ **~10x schneller** bei wiederholten Berechnungen!

KLASSISCHER KI CHAT



Jede Aufgabe
einzeln beschreiben,
Kontext immer neu
aufbauen...



- Aufgabe jedes Mal neu erklären
- Kein bleibender Kontext
- Keine Automatisierung
- Manuell und zeitintensiv

KI-AGENTEN

Agenten übernehmen
Workflows, behalten
Kontext, arbeiten
autonom!



- ✓ Autonome Workflows
- ✓ Kontext behalten & nutzen
- ✓ Parallele Aufgaben
- ✓ **~10x schneller** bei repetitiven Wissensarbeit-Aufgaben!

**~10x
SCHNELLER**
bei repetitiven
Wissensarbeit-
Aufgaben!



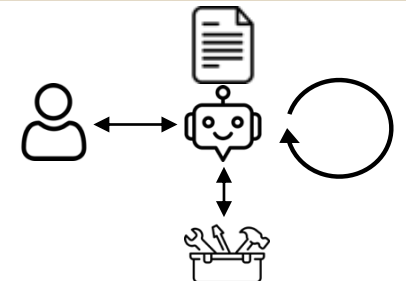
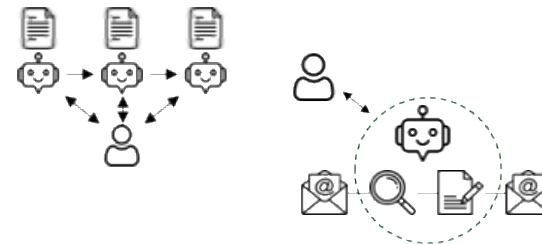
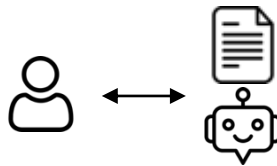
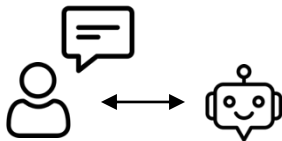
MERKSATZ: Excel hat nicht nur das Rechnen beschleunigt – es hat das **Denken** verändert.

KI-Agenten werden nicht nur die Arbeit beschleunigen – sie werden das **Arbeiten** verändern.

Bild KI generiert

KI-Chatbots – KI-Assistenten – KI-Workflows – KI-Agenten

	KI-Chatbots	KI-Assistenten (CustomGPTs, Gems, etc.)	KI-Workflows	KI-Agenten
Zentrale Merkmale	• Dialoge & Erzeugungen: Antworten, Bilder, Code, ...	• Dialoge & Erzeugungen auf Basis Instruktion & Dokumente	• Vordefinierte Verkettung von Arbeitsschritten / Dialogen	• Bearbeitung von Aufgaben, Entscheidungen (z.B. Werkzeuge)
	← reaktiv →		ausgelöst	ausgelöst / aktiviert
Einsatz für	• Einzelanliegen	• Wiederkehrende Anliegen	• Wiederkehrende Abläufe / Abfolgen von Dialogen	• Aufgaben mit offenen Lösungswegen
Rolle Mensch	• Initiiert & steuert Dialog • Interpretiert Ausgabe	• Konfiguriert (Prompt, Daten) • Prüft / nutzt Ausgabe	• Definiert Ablauf / Übergänge • Prüft / nutzt Ergebnis	• Definiert Auftrag / Ziele • Prüft / nutzt Ergebnis
Beispiel	• Begriffserklärungen durch Chatbot	• Standortbestimmung mit Assessment-Assistent	• Verkettung von Dialogen zu Phasen im Prozess selbstorganisierten Lernens	• Report zu Ergebnissen einer Transfer-Evaluation



Umfrage

Was haben Sie bereits öfters genutzt?

- KI-Chatbots
- KI-Assistenten
- KI-Workflows
- KI-Agenten

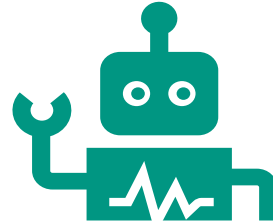
KI-Agenten: unterschiedlich eingesetzt



Klassische Workflows mit Agenten-Unterstützung

Agenten **helfen bei der Erstellung** von Prozessen/Anwendungen als klassischer Business-Prozess in vorhandenen Systemen.

*SAP Joule Studio: Ein **KI-Agent generiert Workflows** für die automatisierte Übertragung von Testergebnissen aus dem E-Prüfungssystem ins Prüfungsmanagement.*



Agenten-Anwendungen (selbstständig agierend)

Agenten **sind das Ergebnis** und werden eingesetzt. Die Agenten selbst können wiederum mit einem Agenten erstellt werden (siehe links).

*Ein **KI-Agent analysiert Rechnungen**, extrahiert Daten und schlägt Buchungssätze vor.*

Agentensysteme genutzt durch die Organisation



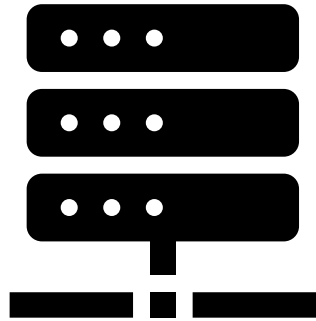
Lokale, generische Agentensysteme (individuelle Verwendung)

Agentic Harness **läuft lokal als generische Anwendung** und wird situativ und individuell in Tätigkeiten verwendet.

*VSCodium + Cline/Hermes: **Lokale KI-Agenten** analysieren Meeting-Protokolle, führen Code-Reviews durch oder extrahieren Wissen aus Projekt-Dokumentationen und erstellen strukturierte Zusammenfassungen – direkt auf dem Dateisystem.*

Individueller, generischer Einsatz von Agenten-Systemen

Die Bestandteile für das agentische Arbeiten



Inferenz per API

z.B. die Modelle
der KI-Toolbox



Agentische Umgebung (Harness)

Cline in VsCodium/
Visual Studio Code



Vorgehensweisen und Tools

Eigene Kompetenz
in der Verwendung

Demonstration KI-Policys und Strategien der neun Landesuniversitäten Baden-Württemberg

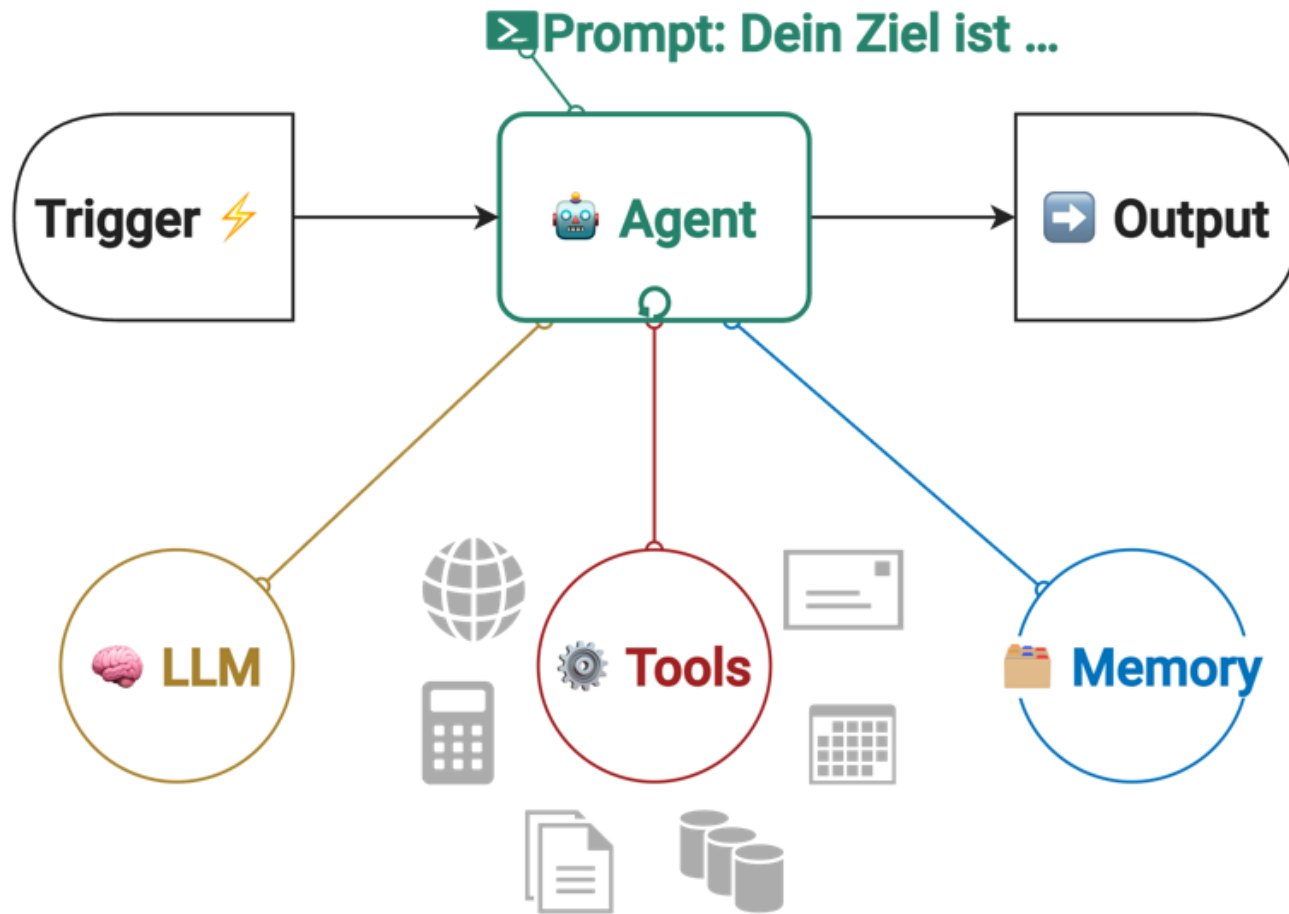


„Erstelle mir zu den in Quellen hinterlegten KI-Regelungen der Hochschulen eine Infografik im HND-BW Layout“



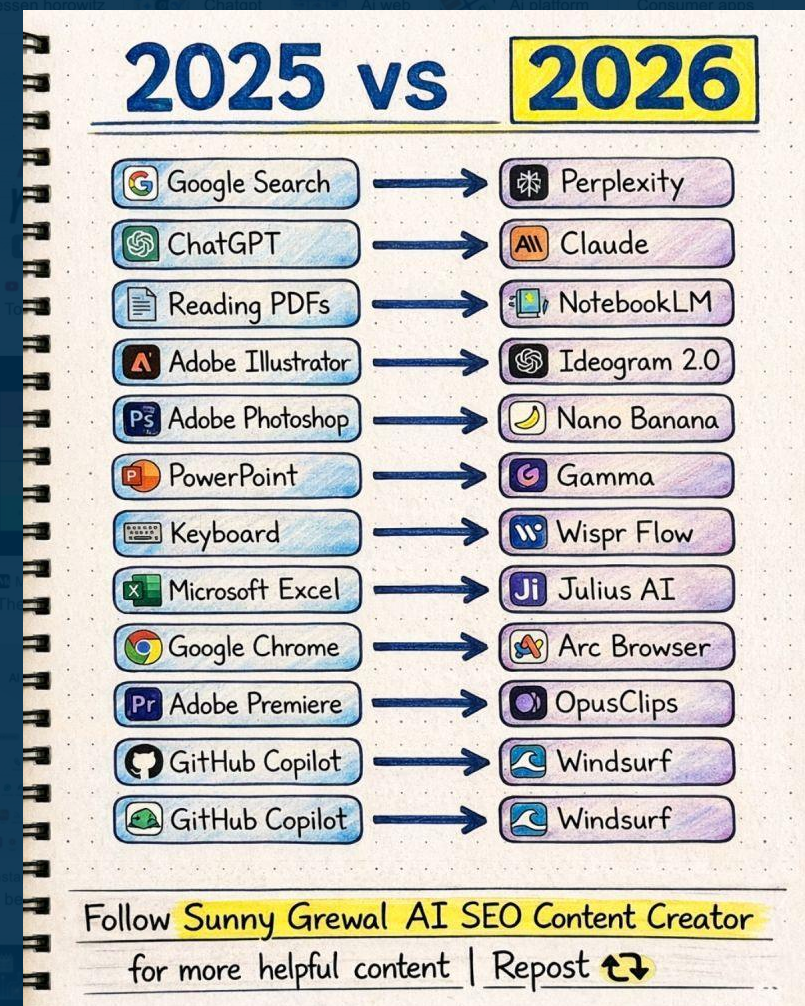
LIVE DEMO

Ein Agent verfolgt autonom Ziele, statt Workflows abzuarbeiten.



- Nimmt seine Umgebung wahr.
- Verfolgt komplexe Ziele.
- Trifft auf Basis von Beobachtungen und Zielen eigenständig Entscheidungen über: nächste Schritte; Nutzung verfügbarer Werkzeuge
- Lernt potenziell aus Interaktionen.
- Arbeitet oft in einer Schleife (z.B. Beobachten – Orientieren – Entscheiden – Handeln).
- Nutzt interne Speicher ("Gedächtnis").
- Orchestriert eine Reihe von Tools (Software, APIs, Datenbanken), um Ziele zu erreichen.

Mehr Tools lösen nicht das Problem



Quellen: LinkedIn Harish kumar, 04.05.2026, https://www.linkedin.com/posts/harishkumar-sh_artificialintelligence-aitools-futureofwork-share-7457014872862613504-15em und AI for Enterprise, <https://www.linkedin.com/posts/ai-tools-2025-vs-2026-%F0%9D%97%95%F0%9D%97%B2%F0%9D%97%B0%F0%9D%97%BC%F0%9D%97%BA%F0%9D%97%B2-%F0%9D%97%AF%F0%9D%97%B2-share-7454665691665879040-cbGG>

Hinter vielen Tools stehen „nur“ Agenten ...

Perplexity Deep Research

- **Research Agent**
- **Ziel:** Bericht zu einem Thema zu erstellen
- **Analysiert** das Thema führt eine **Suche** im Internet und Fachdatenbanken durch.
- **Bewertet** die Suchergebnisse
- **Passt** bei Bedarf die Suche mehrfach **an** und verwendet dazu bereits ermittelte Informationen
- **Erstellt** einen Bericht dazu
- **Wandelt** diesen in eine Infografik, Word oder PDF-Datei **um**.

Notebook LM

- Ist eine **App mit verschiedenen Agenten**
- Verschiedene Agenten für z.B.:
 - Analyse und Zusammenfassung von Dokumenten
 - Erstellen von Audio- und Videozusammenfassungen
 - Interaktive Mindmaps
 - Erstellung von Präsentationen

Claude Desktop

- **KI-Agent** System von Anthropic das direkt auf dem Desktop arbeitet
- Führt unterschiedlichste Aufgaben eigenständig und mehrstufig aus
- Z.B. Lesen, Bearbeiten und Organisieren von Dateien
- Ist ein Beispiel für einen Agent-Harness

Die Lösung ist:

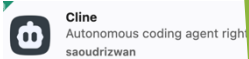
selbst auf der individuellen Ebene generisch einsteigen, ...

- **Ein universelles Agenten-Tool** (Harness) statt vieler Spezialwerkzeuge
- **Selbst steuern** statt Blackbox mit eingeschränkten Anpassungsmöglichkeiten
- **Ein System** statt zahlreicher Lizenzen oder Abos
- Verwendung **hochschuleigener oder lokaler Modelle** statt fehlenden Datenschutzes und fehlender Informationssicherheit

Schritt für Schritt Anleitung Cline in VSCode

Installieren

- VSCode (https://vscode.com/) oder Visual Studio Code (Microsoft App Store) installieren
- In VSCode bzw. Visual Studio Code den Extensions Marketplace öffnen  und nach Cline suchen
- Die Extension



Einrichten

- Cline erscheint in der Seitenleiste als Roboter Symbol . Dieses öffnen und dort in den Einstellungen (Zahnrad oben rechts) die API-Konfiguration vornehmen

Verwenden

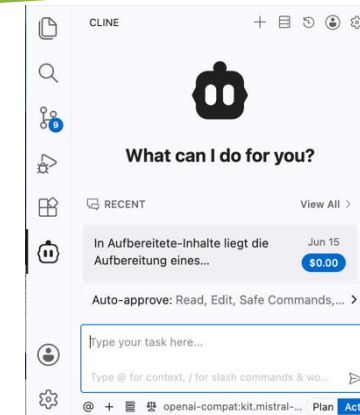
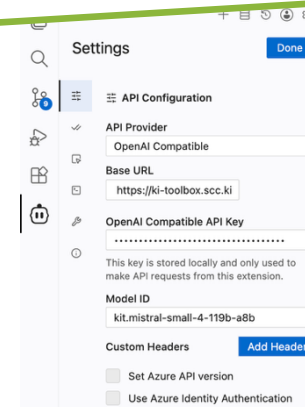
- Aufträge an den Agenten werden im Chatfenster eingegeben.
- Die Modi unten rechts gezielt verwenden:

plant erst, ohne zu ändern
hrt aus und Bearbeitet

hweise zur Verwendung:
s.cline.bot

<https://www.zml.kit.edu/ki-agenten.php>

Cline-Account
anlegen und
freie Modelle von
dort verwenden.



Eigenes Experiment

Erstelle mir zu den in Quellen hinterlegten KI-Regelungen der Hochschulen eine Infografik im HND-BW Layout

Neun Hochschulen im Detail

📅 Stand: Mai 2026

📄 Richtlinie

universität freiburg

Universität Freiburg

Policy zum Umgang mit generativer KI in Studium und Lehre

Drei Ziele: KI-Kompetenzen fördern, KI als didaktisches Assistenzsystem nutzen, Prüfungsintegrität sichern. Kein Verbot, sondern transparenter, chancengerechter Einsatz – die Universität stellt datenschutzkonforme KI-Systeme für alle bereit.

Policy (PDF) ▶

📅 Stand: 30.06.2025

📄 Leitlinien



Karlsruher Institut für Technologie (KIT)

Leitlinien zum Einsatz generativer KI + KI-Strategie

Potenziale verantwortungsvoll erkunden, Verwendung dokumentieren. Nutzer:innen tragen die Verantwortung für den Output; gute wissenschaftliche Praxis, DS-GVO-konforme Systeme, besondere Sorgfalt bei Hochrisiko-KI (Art. 6 KI-VO). KI-Strategie 2026 ergänzt Ziele & Maßnahmen.

Leitlinien & Strategie (PDF, abgelegt) ▶

🔄 Laufend aktualisiert

📄 Grundsätze



Universität Stuttgart

Grundsätze für den KI-Einsatz für Lehrende

KI-Nutzung erlaubt, Regeln transparent im Syllabus, Verantwortung für Input & Output. Bevorzugung des un-

📄 Über heiSKILLS

📄 Leitlinie



Universität Heidelberg

Leitlinie zum Umgang mit KI in Studium und Lehre

KI-Nutzung grundsätzlich erlaubt, nach Abstimmung mit den Prüfer:innen. Pflicht für alle Studienarbeiten: Eigenständigkeits- und Kennzeichnungserklärung inkl. Übersicht der genutzten Tools (Musterformular), ggf. Prompt-Verzeichnis.

Leitlinie (PDF) ▶

📄 Papier: 01/2026

📄 Leitlinien



Universität Konstanz

Papier „KI in Studium und Lehre“

Vom Referat für Lehrfragen entwickelt, in Senat & Ausschuss für Lehre diskutiert; Basis für fachspezifische Richtlinien. Regeln je nach Studienphase und Lernziel; bei Abschlussarbeiten gelten die Regelungen des Zentralen Prüfungsamts.

Seite „KI in der Lehre“ ▶

📅 2023 / 2024

📄 Leitlinie



Universität Tübingen

Leitlinie + Handreichung zu Lehr- & Prüfungskontexten

AG Generative KI berät das Rektorat; Leitlinie (2023): kritisch-reflexiv, transparent, verantwortungsvoll.

📅 2022 / 2023

📄 Strategie



Universität Hohenheim

Strategie „Digitale Transformation“ & SEP 2023–2027

KI & Data Science als Leitthemen (AIDAHO-Zertifikat, ABBA). Senatsempfehlung: generative KI in schriftlichen Prüfungen grundsätzlich als Hilfsmittel zulässig, sofern die Erreichung der Lern- und Qualifikationsziele nicht entgegensteht.

Strategie (PDF) ▶

📄 Beschluss: 15.10.2025

📄 Richtlinie



Universität Mannheim

KI-Richtlinie (Rektoratsbeschluss)

Verbindliche Regeln (§ 1–7): zentrales KI-Register mit Freigaben, Rektoratszustimmung für Hochrisiko-KI-Systeme, sensible Daten nur in freigegebenen Systemen, Letztverantwortung beim Menschen. Merkblätter zu Grundlagen, Risiken & Nachhaltigkeit ergänzen.

KI-Richtlinie ▶

📄 Beschluss: 14.10.2025

📄 Richtlinie

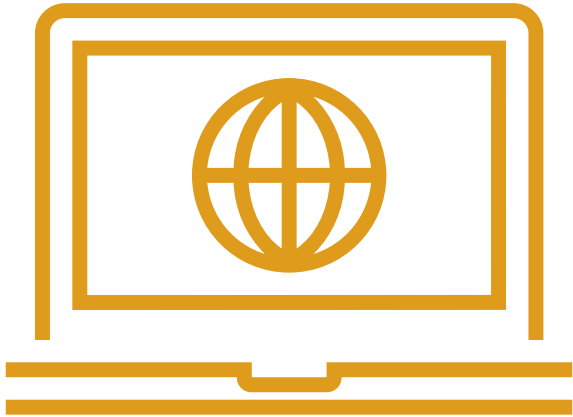


Universität Ulm

Richtlinie zur KI-Nutzung zu dienstlichen Zwecken

Grundanforderungen: DSGVO-Informationen, Opt-out beim Training, löschrare Verlaufsprotokolle, dienstliche

Eigenes Probieren in Gruppen



Vorbereitete Rechner mit VsCodium, Cline Plugin und API-Key für lokales Modell des KIT.



Vorbereitetes Verzeichnis mit den KI-Policies und Strategien der neun Universitäten



Aufgabe: Erstellung einer Infografik als Übersicht
Probieren Sie eigene Ansätze aus, verändern Sie das Ergebnis nach eigenen Vorstellungen!



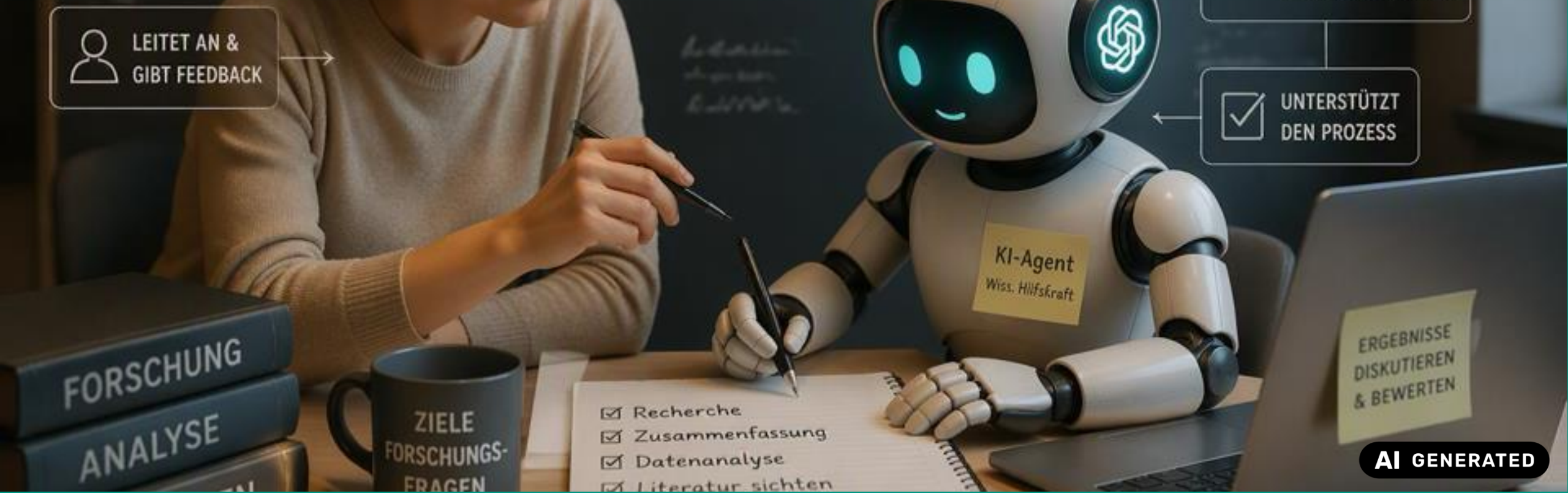
Notieren auf Moderationskarten:

- Bedeutung für die eigene Arbeit
- Bedeutung für das Studium



Diskussion der Ergebnisse und Erfahrungen

- Wie ist es Ihnen ergangen? Was hat geklappt, welche Probleme gab es? Wie zufrieden sind Sie mit dem Ergebnis?
- Was bedeutet dies für Ihre eigene Arbeit? Welchen Nutzen, welche Probleme sehen sie?
- Was bedeutet dies für das Studium in Ihrem Fach?



Du weißt bereits wie du
den Agenten richtig
verwendest!

Der perfekte KI-Agent ist nur so gut wie du steuerst!

Klare **Zielvorgabe**

Prompt gibt Ziel vor

Zuerst Vorgehen **planen** lassen,
dann **umsetzen**

Erst **Plan-** dann **Act-Modus**

Unverhandelbare **Vorgaben**
machen

Rules geben klare Regeln vor

Arbeitsanweisungen für häufig
benötigtes

Skills sind zu befolgende
Arbeitsanweisungen für öfters
benötigte Dinge

Arbeitswerkzeuge geben

Tools bereitstellen

Eine Aufgabe nach der anderen
(Kopf frei für neues)

Für neue Aufgaben neue Chats
anfangen (kein **Context-Rot**)

Ergebnisse prüfen und
**Zwischenergebnisse definieren und
vorlegen lassen**

Agent in kleineren in sich
geschlossenen Arbeitspaketen arbeiten
lassen (**Human in the Loop**)

Notwendiges **Material mitgeben**

Kontext für die Aufgabe in Form
von Dokumenten ...

Canvas zur KI-Agenten Verwendung

Zu erledigende Aufgabe
(Was soll am Ende erreicht werden?)



Vorgehen planen (Plan-Modus)
(Mit welcher Frage kann der Agent das Vorgehen erst einmal planen?)



Kontrolle behalten (Human in the Loop)
(Mit welchen Zwischenergebnissen soll der Agent Feedback einholen?)



Datenbasis (Kontext)
(Welchen Inhalt braucht der Agent dafür?)



Beurteilung
(Wie kann ich das Ergebnis beurteilen?)



Risiko begrenzen
(Was darf auf keinen Fall passieren?)



Vorgaben (Rules)
(Welche Konventionen sollen beachtet werden?)



Anleitungen (Skills)
(Für welche wiederkehrend Teilaufgaben sollten Anleitungen bereitgestellt werden?)



Arbeitsmittel (Tools)
(Gibt es bestimmte Werkzeuge wie Zugriff auf andere Daten, die der Agent braucht?)



Kontrollierter Handlungspielraum für den Agenten

- VSCodium / Visual Studio Code arbeiten mit sogenannten „**Workspaces**“. Ein Workspace ist immer ein Dateiverzeichnis mit Inhalten.
- Ein Verzeichnis wird mit *File -> Open Folder* als Workspace geöffnet.
- Beim ersten öffnen, muss mit *Manage* im Kopf das Verzeichnis zu den *Trusted Folders* hinzugefügt werden, damit der Agent hier aktiviert ist.

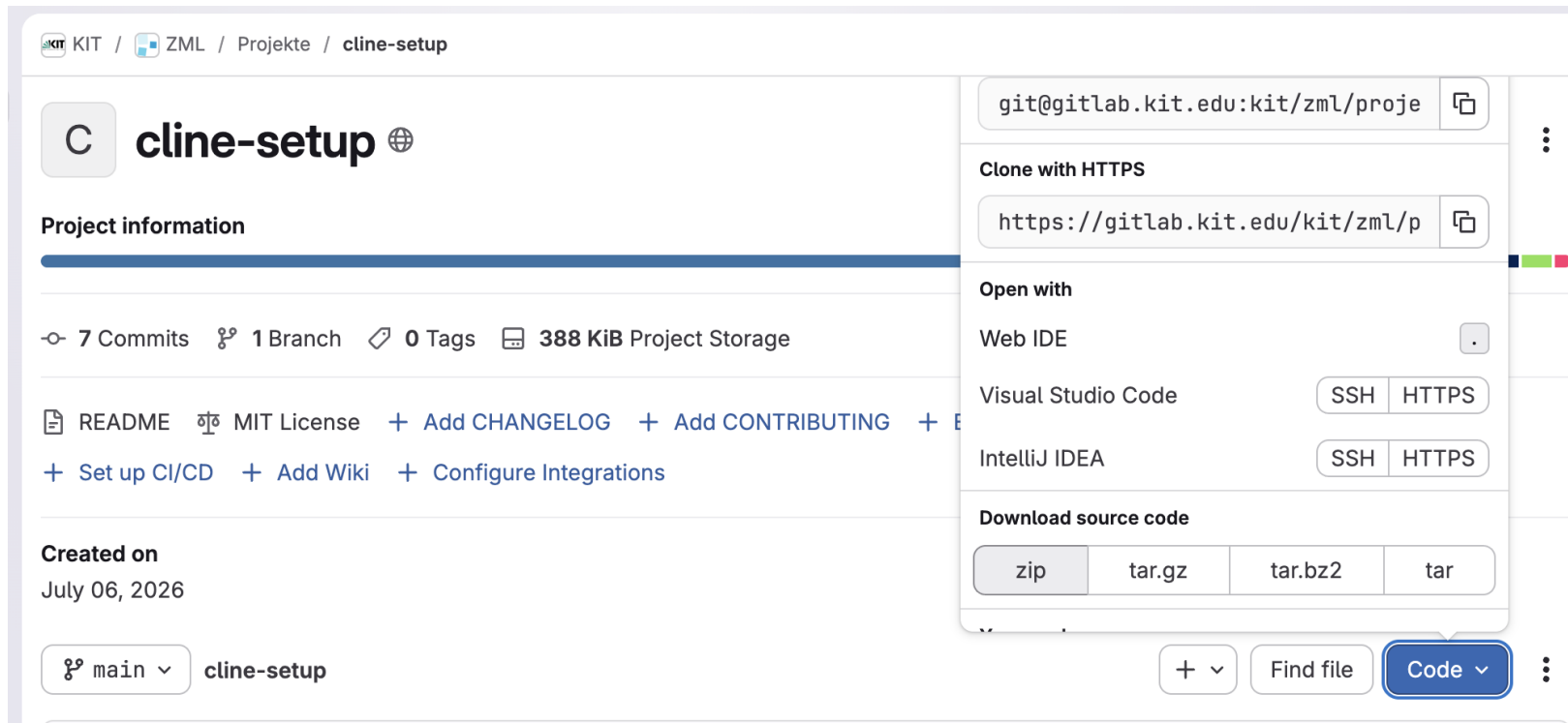
 Restricted Mode is intended for safe code browsing. Trust this folder to enable all features. [Manage](#) [Learn More](#)



- Der Cline-Agent arbeitet auf den Dateien in diesem Verzeichnis:
 - Es ist keine gute Idee den kompletten Fileserver zu öffnen.
 - Lege ein Projektverzeichnis für den Agenten an, lege die notwendigen Dateien als Kopie dort rein und öffne dieses Verzeichnis als Workspace.
- Der Cline-Agent fragt bei Dateioperationen nach, du entscheidest, ob dies gerade Sinn macht.
- **Lokale Modelle verwenden verhindert unkontrollierten Datenabfluss in die Cloud**

Das Starterpaket für Cline mit Alltagshelfern

<https://gitlab.kit.edu/kit/zml/projekte/cline-setup>





AGENTIC USAGE MIT VSCODIUM & CLINE

CHEAT SHEET FÜR EINSTEIGER*INNEN AM KIT

1. WAS IST EIN KI-AGENT?

TRADITIONELLER KI-CHAT

- ✗ Jede Aufgabe einzeln beschreiben
- ✗ Kein bleibender Kontext
- ✗ Manuell & zeitintensiv
- ✗ Ergebnisse manuell übertragen



KI-AGENT (CLINE)

- ✓ Behält Kontext autonom
- ✓ Führt Workflows aus
- ✓ ~10x schneller bei repetitiven Aufgaben
- ✓ Automatische Updates

WAS KANN CLINE?

Autonomer Coding-Agent direkt in VSCode, der:

- 📄 Dateien lesen & schreiben
- 📄 Terminal-Befehle ausführt
- 🔍 Code analysiert & refaktoriert
- 📁 Projekte strukturieren kann
- 📄 Dokumentationen erstellt



MERKSATZ: KI-Agenten werden nicht nur die Arbeit beschleunigen – sie werden das Arbeiten verändern.

2. INSTALLATION – DIE WICHTIGSTEN SCHRITTE



STARTERPAKET EINRICHTEN

git clone <https://gitlab.kit.edu/kizml/projekte/cline-setup.git>
Im cline-setup-Ordner in Cline-Chat eingeben: „Führe alle Anweisungen in README.md aus“

GLOBAL VERFÜGBAR MACHEN

Skills & Rules global nutzen:

Win: C:\Users\USERNAME\cline\skills\
Documents\Cline\Rules
Mac: ~/.cline/skills/
~/Documents/Cline/Rules

3. ERSTE KONFIGURATION

API-ZUGANG KIT KI-TOOLBOX

1. Anmelden an ki-toolbox.scc.kit.edu
2. Einstellungen → API-Schlüssel
3. Neuen Schlüssel generieren (sk-...)

CLINE KONFIGURIEREN

Settings → OpenAI Compatible

Base URL: <https://ki-toolbox.scc.kit.edu/api/v1>
API Key: sk-...
Model ID: siehe Tabelle rechts

– VERFÜGBARE MODEL IDS (AUSWAHL)

MODELL	MODEL ID	CONTEXT	USE CASE
Qwen 3.5	kit.qwen3.5-397b-a17b	128K	Allrounder, Coding
MiniMax M2.7	kit.minimax-m2.7-229b	256K	Lange Dokumente
Mistral Small 4	kit.mistral-small-4-119b-a8b	32K	Schnelle Tasks

Beispielpreise pro 1M Tokens (Qwen 3.5, Stand Mitte 2026)
Input ~\$0,60 Output ~\$2,50 (nur Orientierung)

4. DEIN PERFEKTER HIWI – DIE DENKWEISE

CLINE ALS DEIN PERSÖNLICHER HIWI

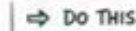
- 📄 Literatur recherchieren
- 📄 Daten erheben & aufbereiten
- 📄 Protokolle schreiben
- 📄 Code testen & reviewen
- 📄 Dokumente verwalten



– USE-CASE CANVAS „MEIN PERFEKTER HIWI“



ZIEL
Welche Ziele verfolgst du mit deinem Agenten?



DO THIS
Welche Aufgaben soll der Agent lösen?



FÄHIGKEITEN
Welche Fähigkeiten und Qualifikationen soll er mitbringen?



TOOLS
Welche Tools und Schnittstellen braucht er?

WAS MACHT EINEN GUTEN HIWI

- ✓ Klare Anweisungen geben
 - ✓ Zwischenergebnisse prüfen (Human-in-the-Loop)
 - ✓ Werkzeuge bereitstellen
 - ✓ Konventionen vorgeben
 - ✓ Eine Aufgabe nach der anderen
- ✗ Nicht alles auf einmal erwarten
 - ✗ Nicht ohne Kontrolle laufen lassen
 - ✗ Keine unklaren Ziele setzen



5. ERSTE GEHVERSUCHE

5.1 PLAN-MODE VS. ACT-MODE

PLAN MODE | ACT MODE

5.2 DEIN ERSTER TASK

5.3 MEMORY BANK INITIALISIEREN

Initialisiere die Memory Bank

5.4 DOKUMENTE KONVERTIEREN

6. SKILLS & RULES – DIE 3 SÄULEN VON CLINE

ZUSAMMENSPIEL

Deine Anfrage

6.1 RULES (Standards)

Immer einzuhalten!

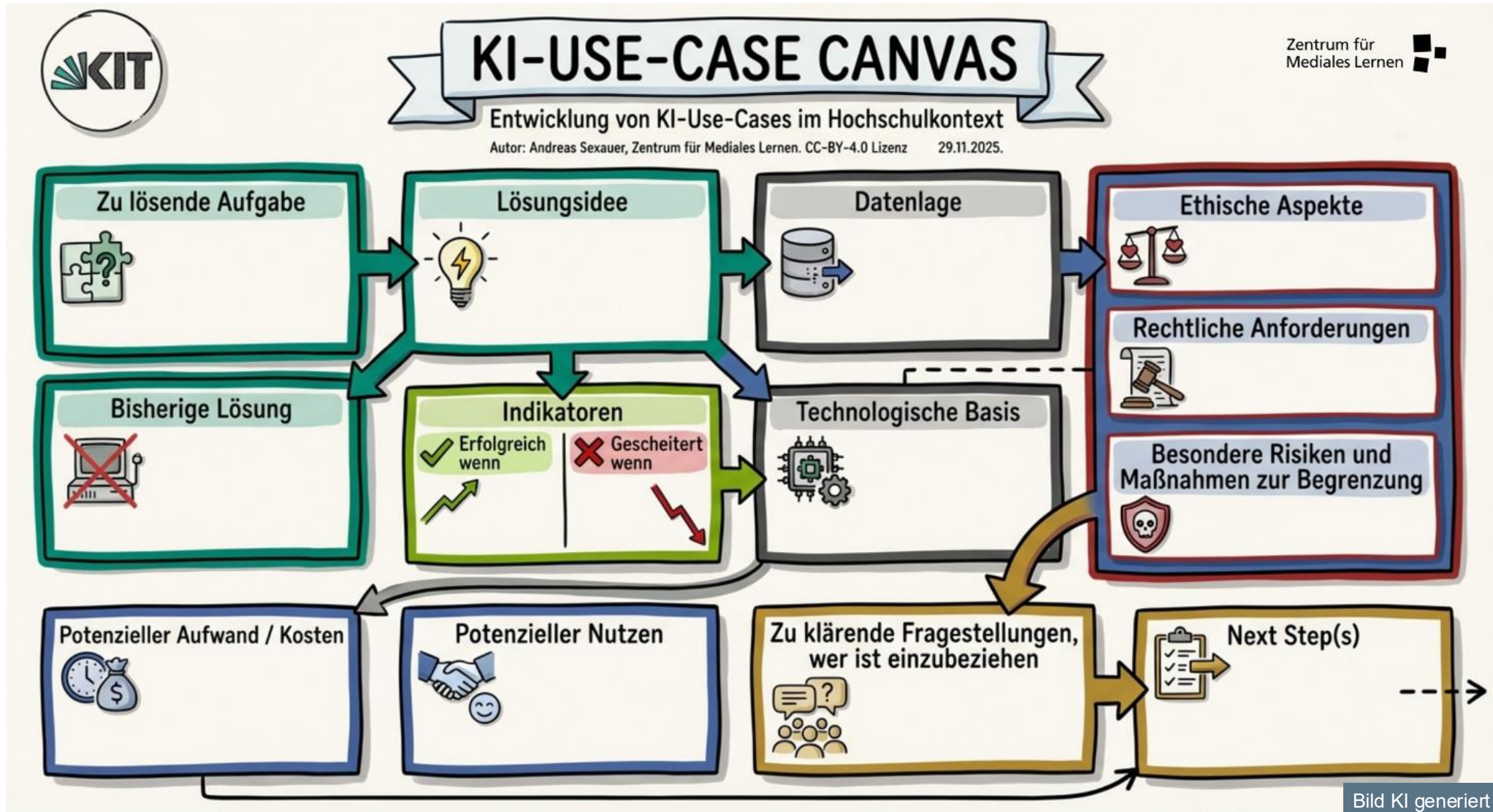
6.3 TIPPS: PR

Bild KI generiert

Cheat-Sheet

<https://www.zml.kit.edu/downloads/cheat-Sheet-ki-agenten.pdf>

Den Use-Case vollständig betrachten



Ressourceneinsatz im Blick behalten

Eigener „Verbrauch“

- <https://my.litellm.scc.kit.edu>
- Budget für Cloud-Modelle erweitern
- Lokale Modelle \$0:
 - kit.deepseek-v4-flash
 - kit.glm-5.3-flash

Modelle vergleichen

- Claude Opus 5.5: Price (1M tokens):
\$4.40 in, **\$22.00** out, \$1.10 cache read, \$13.75 cache creation
- GPT-6.1 Sol: Price (1M tokens):
\$2.40 in, **\$12** out

aber

- Marktpreis GLM 5.3:
\$0.05 in, **\$0.50** out
- Marktpreis Deepseek Flash 4:
\$0.02 in, **\$0.80** out

Projektweise tracken

- Auf my.litellm.scc.kit.edu individuelle API-Keys mit getrennten Budgets erstellen.
- Diese bekommen getrennte „Usage-Reports“.



Fragen/Diskussion?