



# Workshop: Potenziale von KI-Agenten in der Hochschulbildung

Einsatzmöglichkeiten für Lehre, Lernen und Hochschulorganisation

*Learning AID 2025, 2.9. Hosts: Stefan Göllner (Stifterverband), Andreas Sexauer (KIT)*

# Ablauf (60 Min)

- Einführung: Was sind KI Agenten, wie können sie im Hochschulkontext wirksam werden? – 20 Min (Andreas, Stefan)
- Bewertung von Szenarien anhand von drei Schlüsselfragen – 20 Min
- Vorstellung und Diskussion: Ergebnisse – 20 Min

# Workflows vs. Agents

## **Workflows**

*... are systems where LLMs and tools are orchestrated through predefined code paths.*

... offer predictability and consistency for well-defined tasks



## **Agents**

*... are systems where LLMs dynamically direct their own processes and tool usage, maintaining control over how they accomplish tasks.*

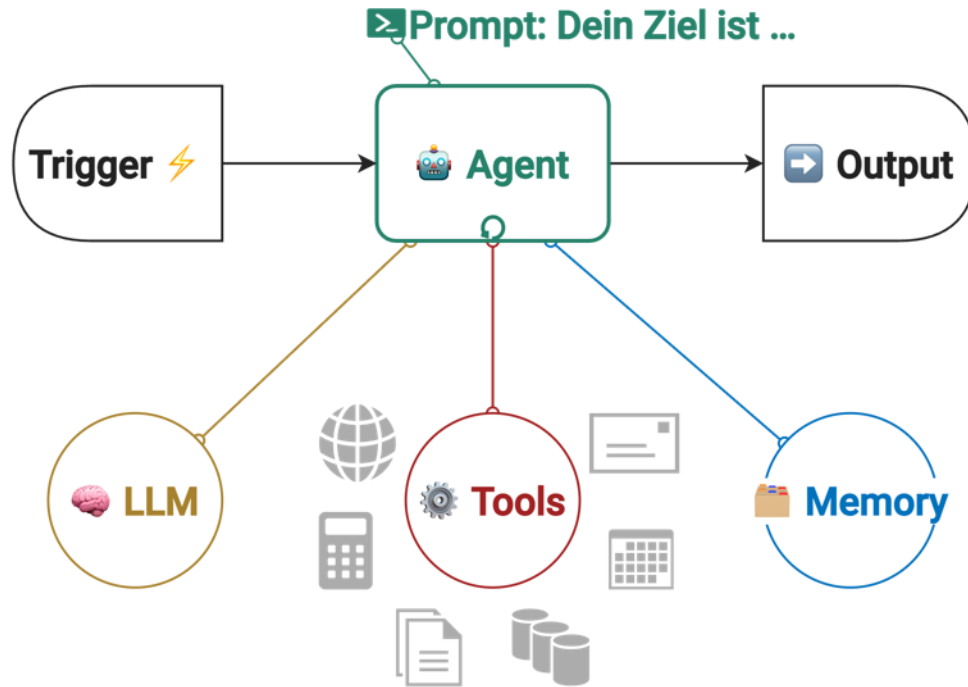
... often trade latency and cost for better task performance

... better option when flexibility and model-driven decision-making are needed at scale



<https://www.anthropic.com/engineering/building-effective-agents>

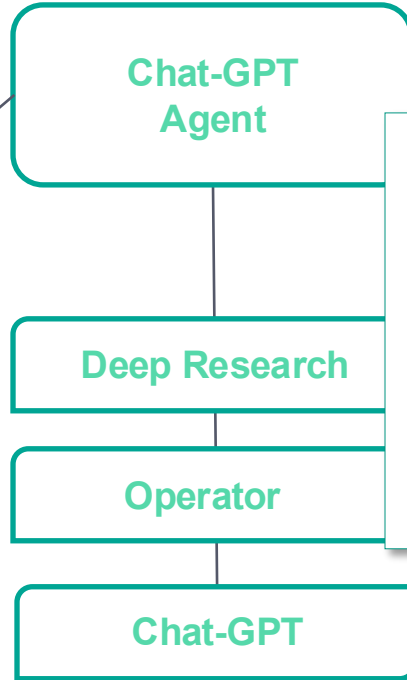
# Ein Agent verfolgt autonom Ziele, statt Workflows abzuarbeiten.



Ein KI-Agent kann seine Umgebung wahrnehmen, komplexe Ziele verfolgen, auf Basis von Beobachtungen und Zielen **eigenständig Entscheidungen über die nächsten Schritte und die Nutzung verfügbarer Werkzeuge treffen**, und potenziell aus Interaktionen lernen. Agenten arbeiten oft in einer Schleife (z.B. Beobachten-Orientieren-Entscheiden-Handeln), nutzen interne Speicher (Gedächtnis) und können eine Reihe von Tools (Software, APIs, Datenbanken) orchestrieren, um ihre Ziele zu erreichen.

# Beispiel: ChatGPT Agent

- o1
- o1 mini
- o3
- 4o



Although the utility is significant, so are the potential risks.



... not something I'd yet use for high-stakes uses or with a lot of personal information until we have a chance to study and improve it in the wild

...we recommend giving agents the minimum access required to complete a task to reduce privacy and security risks.

- KI-Chatbot

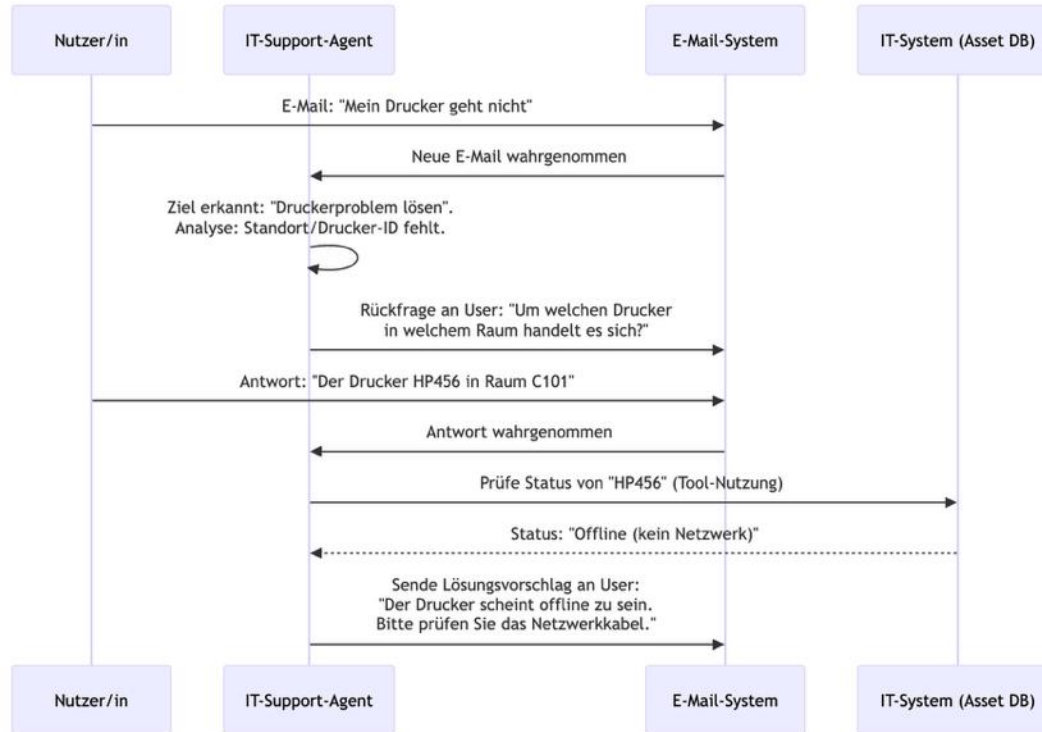
X 17. Juli 2025 · 2,8 Mio. Mal angezeigt

# Demo (n8n)



Andreas Sexauer (ZML),  
Stefan Göllner (Stifterverband),  
Workshop: Potenziale von KI-  
Agenten in der

# Beispiel 1: Informationen beim Eingang erfassen



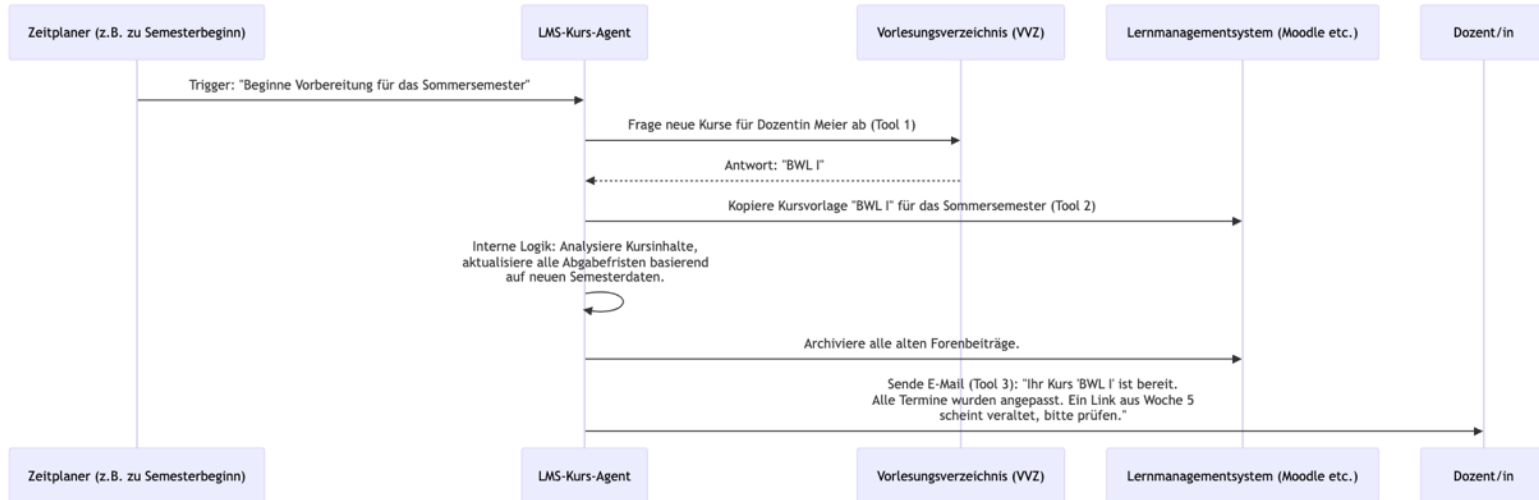
# Beispiel 2: Geplante Überprüfung

## Beispiel: Agent zur automatischen Kurserstellung im LMS

**Ziel (Prompt) des Agenten:** »Dein Ziel: Erstelle zu Beginn der Vorbereitungsphase für jedes neue Semester voll funktionsfähige Kursräume im LMS. Identifiziere wiederkehrende Kurse, passe alle Termine an, archiviere veraltete Inhalte und informiere die Dozierenden über das Ergebnis sowie mögliche Probleme (z.B. defekte Links).«

## Verfügbare Werkzeuge:

- **Vorlesungsverzeichnis (VVZ):** Kurse und zugehörige Dozenten für das neue Semester abfragen.
- **Lernmanagementsystem (LMS):** Kursvorlagen kopieren, Inhalte (Termine, Dateien) ändern, alte Daten archivieren.
- **E-Mail-System:** Benachrichtigungen an Dozierende senden.





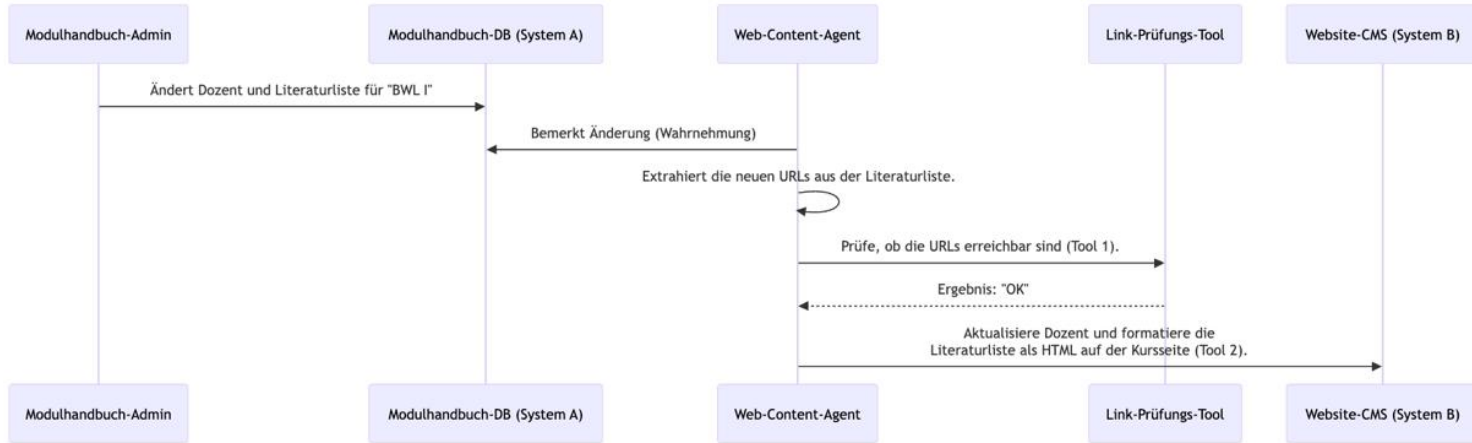
# Beispiel 3: Systemsynchronisation

## Beispiel: Agent für die Aktualisierung der Lehrveranstaltungs-Webseite

**Ziel (Prompt) des Agenten:** »Dein Ziel: Sorge dafür, dass die öffentlichen Kurs-Webseiten immer exakt die Daten aus dem Modulhandbuch widerspiegeln. Validiere alle neuen Informationen, insbesondere externe Links, bevor du sie publizierst. Bei Fehlern, informiere den Verantwortlichen, anstatt falsche Daten online zu stellen.«

## Verfügbare Werkzeuge:

- **Modulhandbuch-DB:** Änderungen an Kursdaten lesen.
- **Link-Prüfungs-Tool:** Erreichbarkeit von URLs validieren.
- **Website-CMS:** Inhalte auf Webseiten aktualisieren.



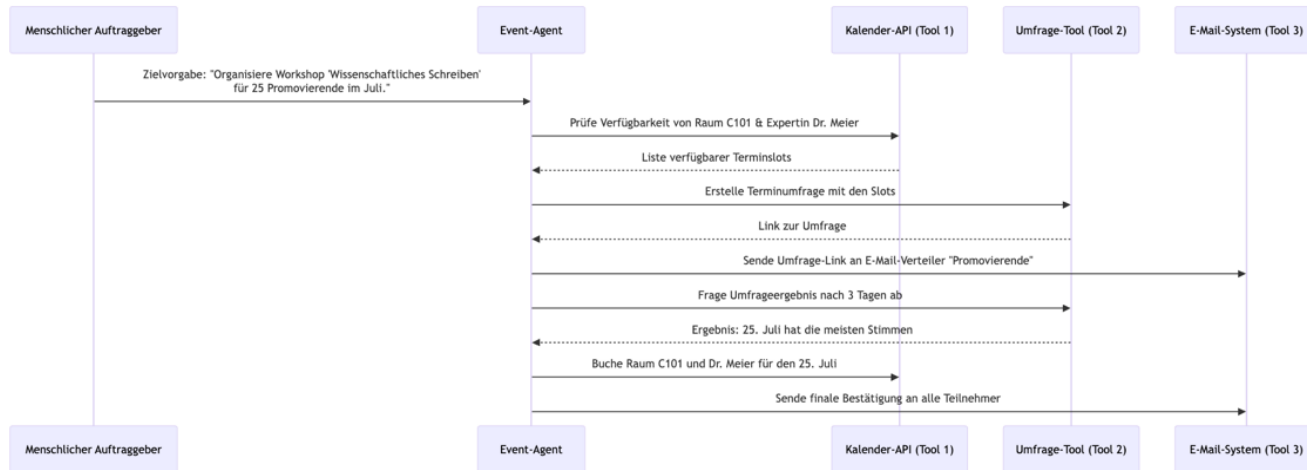
# Beispiel 4: Manuelle Prozesse erweitern

## Beispiel: Agent zur Organisation von Terminen

**Ziel (Prompt) des Agenten:** Dein Ziel: Organisiere einen kompletten Workshop basierend auf einer allgemeinen Anfrage. Kläre selbstständig alle nötigen Schritte: Finde einen passenden Termin für die Zielgruppe und Referenten, buche Räume und Ressourcen und manage die gesamte Kommunikation.

## Verfügbare Werkzeuge:

- **Kalender-API:** Verfügbarkeiten von Personen und Räumen prüfen, Termine buchen.
- **Umfrage-Tool:** Terminumfragen erstellen und auswerten.
- **E-Mail-System:** Anfragen, Einladungen und Bestätigungen senden.





# Sechs Agententypen:



## Zentraler Service-Agent

Ein intelligenter First-Level-Support für alle Service-Einheiten (IT, Studienservice, Bibliothek etc.) vor. Er beantwortet 24/7 Standardanfragen und leitet die wirklich komplexen Fälle an die Mitarbeitenden weiter.



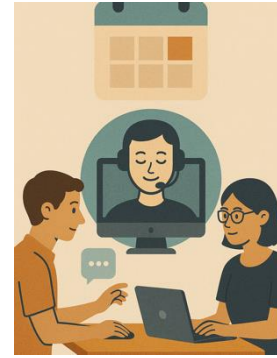
## Regelbasierter Buchungs-Agent

Ob Seminar- und Klausuranmeldungen, Raum- oder Parkplatzvergabe – dieser Agent prüft regelbasiert Voraussetzungen, checkt Verfügbarkeiten und führt Buchung automatisch durch. Schnell, transparent und fehlerfrei.



## Informations- und Umfeld-Monitor

Ein personalisierbarer Radar, der für Forschende neue Paper scannt, für die Hochschulkommunikation die Presse im Blick behält oder die Verwaltung über neue Förderausschreibungen informiert. Schluss mit der Informationsflut!



## Termin- und Meeting-Koordinator

Findet automatisch freie Zeitfenster in den Kalendern von Kolleg:innen, Studierenden oder internationalen Partnern und macht die mühsame Terminabstimmung einfach.



## Text- und Dokumenten-Analyst

Extrahiert aus Meeting-Mitschriften, Transkripten oder Feedbackbögen automatisch Protokolle, Aufgabenlisten und die wichtigsten Erkenntnisse. Pures Wissen, statt unstrukturierter Textwüsten.



## Workflow- und Antrags-Orchestrator

Führt Nutzer:innen intelligent durch komplexe Prozesse wie Dienstreiseanträge oder Beschaffungen, prüft alle Regeln und sorgt für eine reibungslose Datenübergabe an die Zielsysteme (z. B. SAP).

# Arbeitsgruppen: Drei Schlüsselfragen beantworten (20 Min)

## **Fähigkeiten:**

Über welche Fähigkeit sollte der KI-Agent verfügen?

## **Mehrwert:**

Welcher Mehrwert ist ausschlaggebend?

## **Ethische Grenze / Risiko:**

Welche Grenzen müssen gesetzt werden, welche Risiken sind zu berücksichtigen?

# Diskussion und Abschluss (20 Min)

- **Kurzvorstellung der Diskussionsergebnisse (3 Min / Gruppe)**
- **Fazit und Überlegungen zum Anschluss**

# Denkwerkzeuge für KI-Agenten

*Sechs Regeln für autonome Systeme, die helfen, echte Autonomie von Automatisierung zu unterscheiden.*

- 1. Denke in Zielen, nicht in Befehlen.** Ein Agent verfolgt eigenständig ein komplexes Ziel, anstatt nur eine starre Wenn-Dann-Regel auszuführen.
- 2. Suche die menschliche Klebstoffarbeit.** Der größte Mehrwert entsteht dort, wo heute ein Mensch mühsam zwischen Systemen, E-Mails und unstrukturierten Informationen vermitteln muss.
- 3. Frage Was ist passiert?, nicht Wer hat es getan?.** Agenten sollten auf allgemeine Ereignisse reagieren (z.B. eine Abgabefrist), nicht auf das Verhalten einzelner Personen (Profiling). Dies vermeidet verbotenes Profiling und ist eine zentrale Anforderung des EU AI Act sowie der DSGVO.
- 4. Baue auf objektive Auslöser, nicht auf subjektive Annahmen.** Der Agent reagiert auf klare, faktische Trigger wie Fristen, neue Inhalte, Ressourcen-Engpässe oder eingegangene Daten, nicht auf vage Vermutungen.
- 5. Mache den Agenten zum Dirigenten, nicht zum neuen Instrument.** Ein guter Agent nutzt und orchestriert die bereits vorhandenen Werkzeuge (Kalender, LMS, E-Mail), anstatt ein weiteres, isoliertes System zu sein.
- 6. Gib dem Agenten eine Stimme (und einen Notausgang).** Ein autonomer Agent scheitert nicht im Stillen – er fragt bei Mehrdeutigkeiten nach oder übergibt das Problem gezielt an einen Menschen.



# Uses-Cases und Abschlussbewertung mit dem Konzept des Akzeptierten Risikos



## Geführter Denkprozess für die Diskussion:

**Status Quo analysieren:** Welche und wie viele Fehler passieren im heutigen manuellen Prozess? Welche davon sind für uns und unsere Kunden (Studierende etc.) unbemerkt und okay? Bei welchen Fehlern knallt es – also gibt es ernsthafte Konsequenzen?

**Risikogrenze definieren:** Aus dieser Analyse leiten wir ab: Welches Fehlerniveau (Art und Häufigkeit) wäre für den neuen, agentenbasierten Prozess aus institutioneller Sicht akzeptabel?

**Agenten gestalten und messen:** Wie müssen wir den Agenten und seine Leitplanken (z.B. menschliche Freigabeschleifen) gestalten, damit er diese Risikogrenze einhält? Wie können wir seine Leistung und Fehlerquote messen, um sicherzustellen, dass dies erreicht wird?



