

Wie bewerte ich als Rechtsanwält:in KI-Tools im Legal- Bereich?

Dr. iur. Jan Reinhardt, Rechtsanwalt* und Software-Entwickler

*eingetragen in der Liste gemäss Art. 28 BGFA, zgl. Schleswig-Holsteinische RAK

Gliederung

- Grundlagen zu Large Language Models (LLMs) und Tool-Nutzung
- Wie prüfe ich, wo ich allgemeine und spezialisierte KI-Tools sinnvoll einsetzen kann?
- Beispiel: Prüfung zweier konkreter Use Cases
- Häufige Werbeaussagen und konkrete Empfehlungen des Merkblattes
- Fazit

Warum ein Merkblatt und warum ein Webinar?

- Grosse Aufmerksamkeit um «KI-Tools» im Legal-Bereich, diverse Anbieter kontaktieren Rechtsanwält:innen immer wieder telefonisch oder per E-Mail
- Bewertung und Vergleich der Angebote fällt oft schwer, da 1. Fachwissen fehlt und 2. sehr weitgehende Werbeaussagen erfolgen
- Merkblatt des BAV gibt Hilfestellung mit der Empfehlung, detaillierte Nachfragen an Anbieter zu stellen
- Hierzu auch Online-Fragebogen, welcher trotz Aufforderung durch einzelne Rechtsanwält:innen noch von keinem Anbieter ausgefüllt wurde

Grundlagen zu Large Language Models (LLMs) und Tool-Nutzung

Was meine ich mit «KI-Tools» im Legal-Bereich?

«Künstliche Intelligenz»

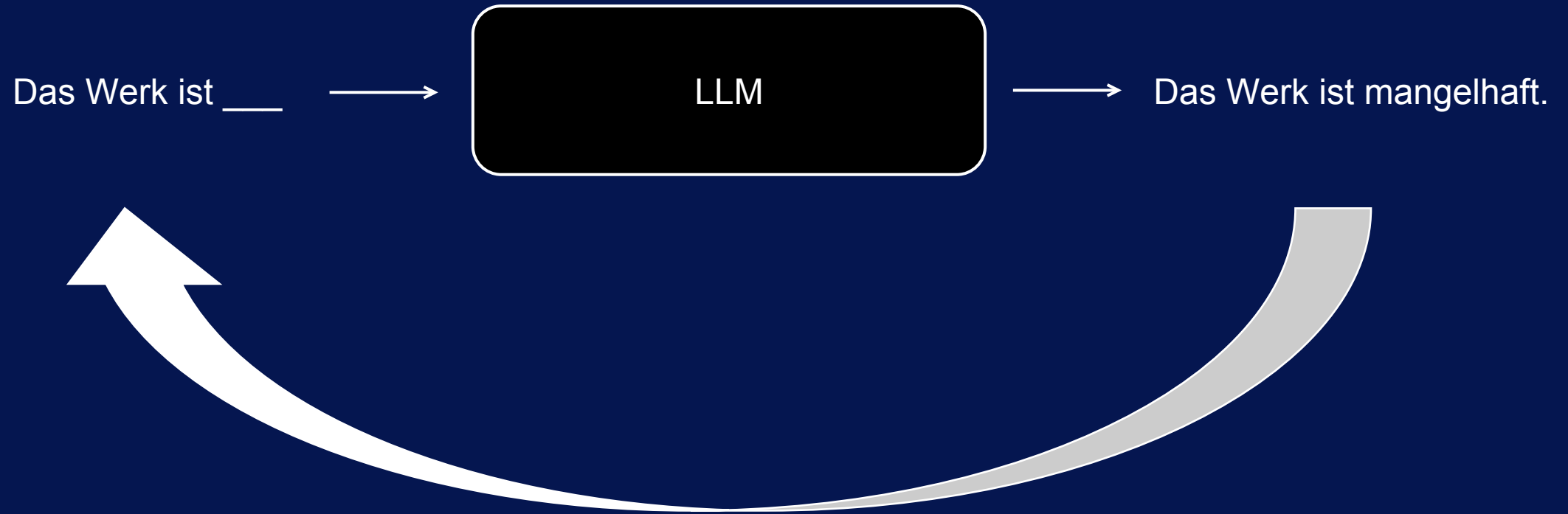
Machine Learning

Transformer

Generative Pretrained
Transformer (GPT) / Large
Language Model (LLM)

Text-Embedding-Modelle für
Suche und Klassifikation

Allgemeines zu LLMs



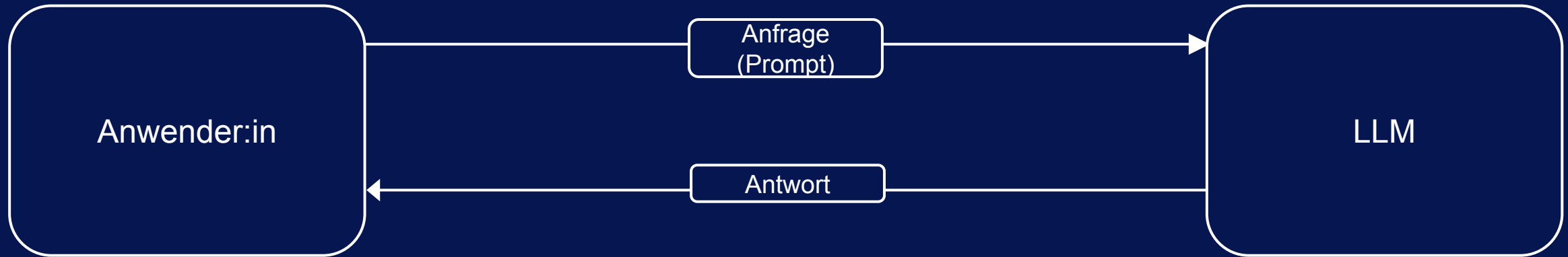
Allgemeines zu LLMs

- Interne Repräsentation von Konzepten, aber kein Wissen, kein Lernen und kein Denken, sondern (sehr effektive) Wortvorhersage
- Relevanz im juristischen Kontext
 - Risiko der «Halluzination», grosse Fehler sind oft ebenso wahrscheinlich wie kleine Fehler und ebenso schwer zu erkennen => Alle Antworten müssen eingehend geprüft werden!
 - Probleme mit Priorisierung bei Vielzahl an Instruktionen und grossen Projekten
 - An Trainingsstand gebunden => kann veraltete Rechtslage zugrunde legen
 - Effektivität hängt stark von Verfügbarkeit von Trainingsdaten ab => Tendenziell stark bei Routinefällen und klar umgrenzten Fragestellungen, tendenziell schwächer bei umfangreichen, randständigen Fällen
- Ein LLM kann nie Verantwortung gegenüber der Klientschaft übernehmen, daher darf es nie kritische Entscheidungen treffen!
- Antworten von LLMs sind praktisch nicht reproduzierbar => Weder der Prompt noch die Antwort sind eine Quelle, sondern nur die vom LLM angegebenen Quellen!

Ein Client verbindet LLMs mit anderer Software (Tools)

- Durch ein Tool kann ein LLM (durch Text gesteuert) vieles von dem tun, was auch ein Mensch mit einem Computer kann: Datenbanken aller Art durchsuchen, Dokumente bearbeiten und sonstige Handlungen ausführen
- Tools müssen aber verfügbar sein, bei öffentlichen Daten oft Tools verfügbar, bei urheberrechtlich geschützter Literatur demgegenüber selten
- Tools müssen zudem mit dem jeweils verwendeten Client verbunden werden, bei ChatGPT / Claude / Gemini müssen Sie das selbst tun, bei speziellen KI-Tools für den Schweizer Rechtsmarkt sind nützliche Tools oft bereits «vorinstalliert»
- Teilweise entwickeln die Anbieter eigene, spezialisierte Tools für ihre Software und stellen diese nur mit ihrem Produkt bereit
- => Bequemere Einrichtung und Verfügbarkeit spezialisierter Tools sowie Datenquellen gehören zu den Hauptversprechen der Anbieter im Rechtsbereich

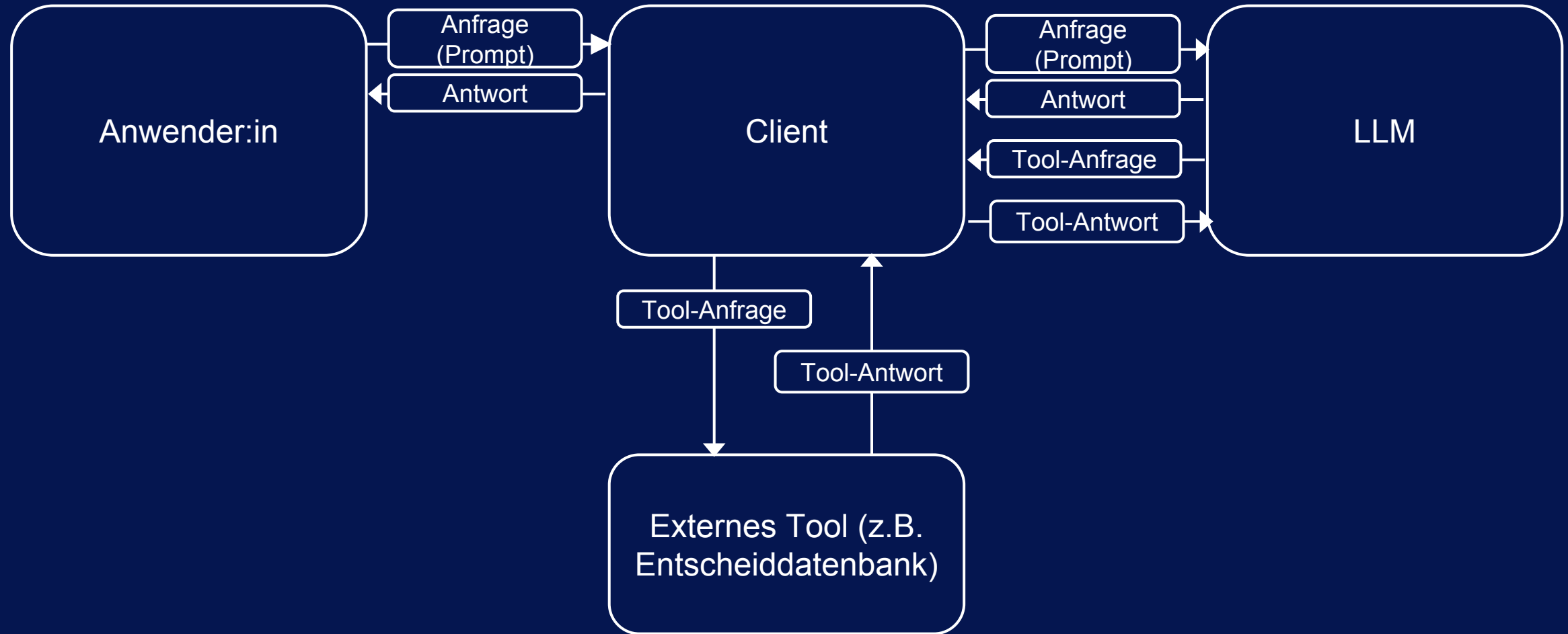
Ein Client verbindet LLMs mit anderer Software (Tools)



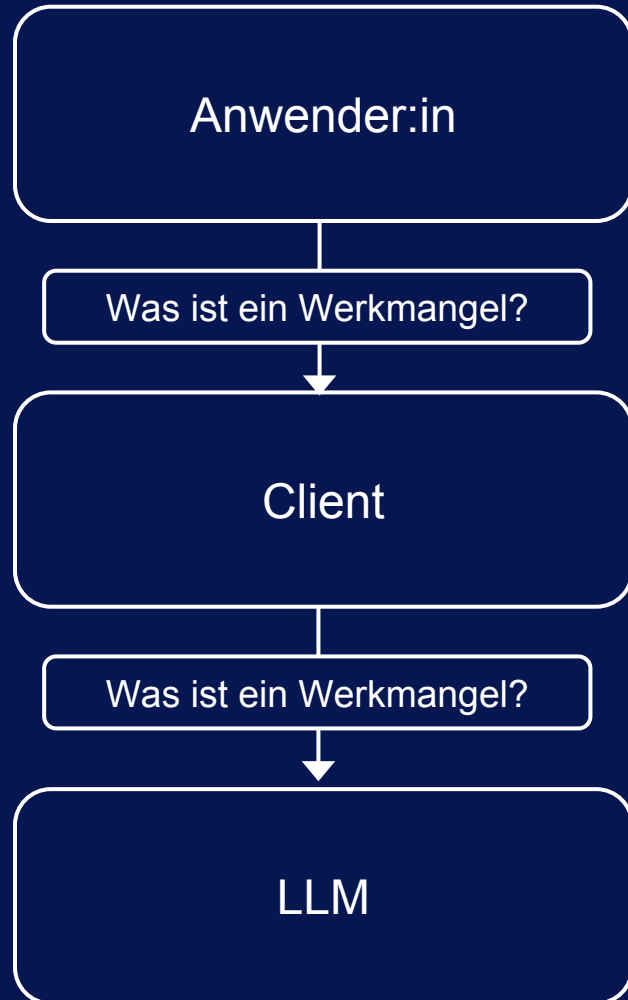
Ein Client verbindet LLMs mit anderer Software (Tools)



Ein Client verbindet LLMs mit anderer Software (Tools)



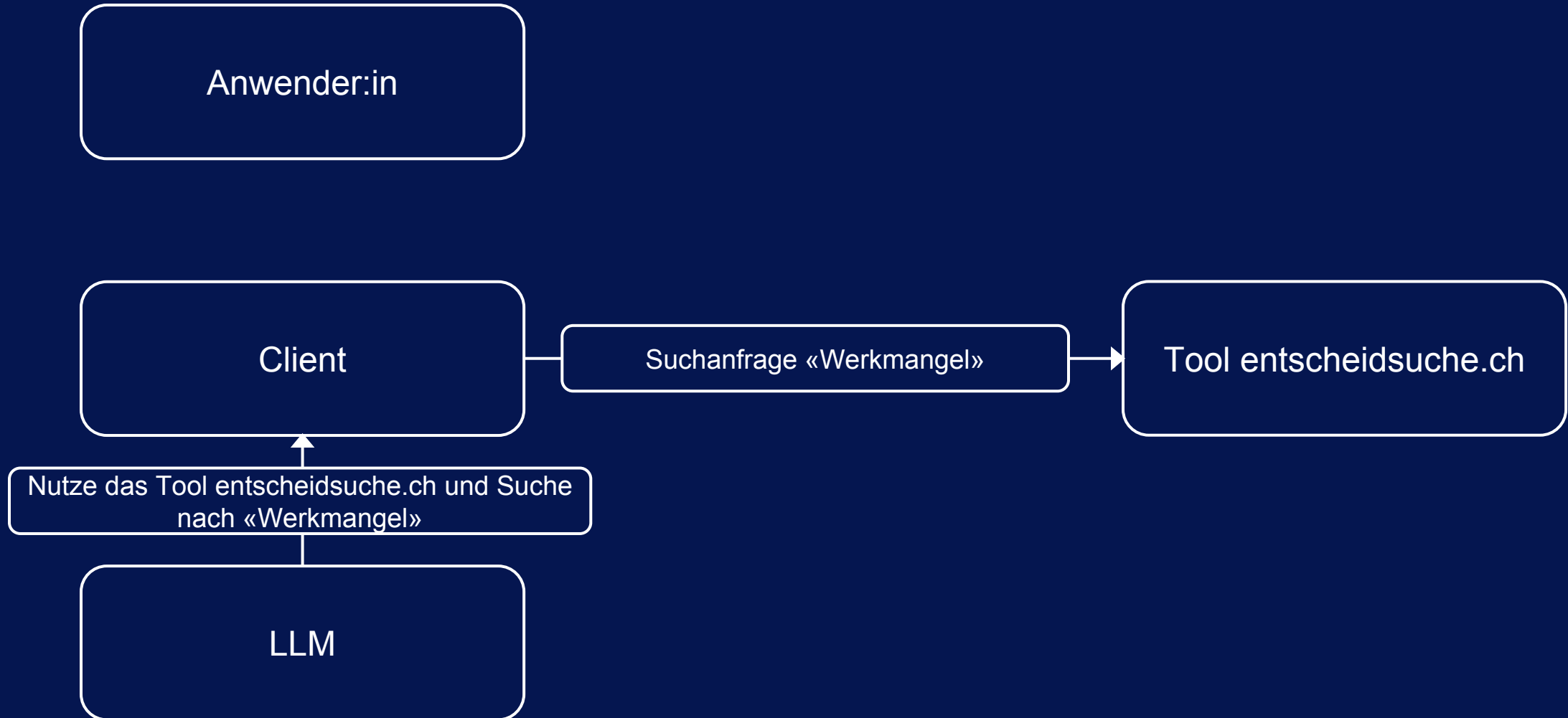
Beispiel: Verwendung einer Entscheiddatenbank



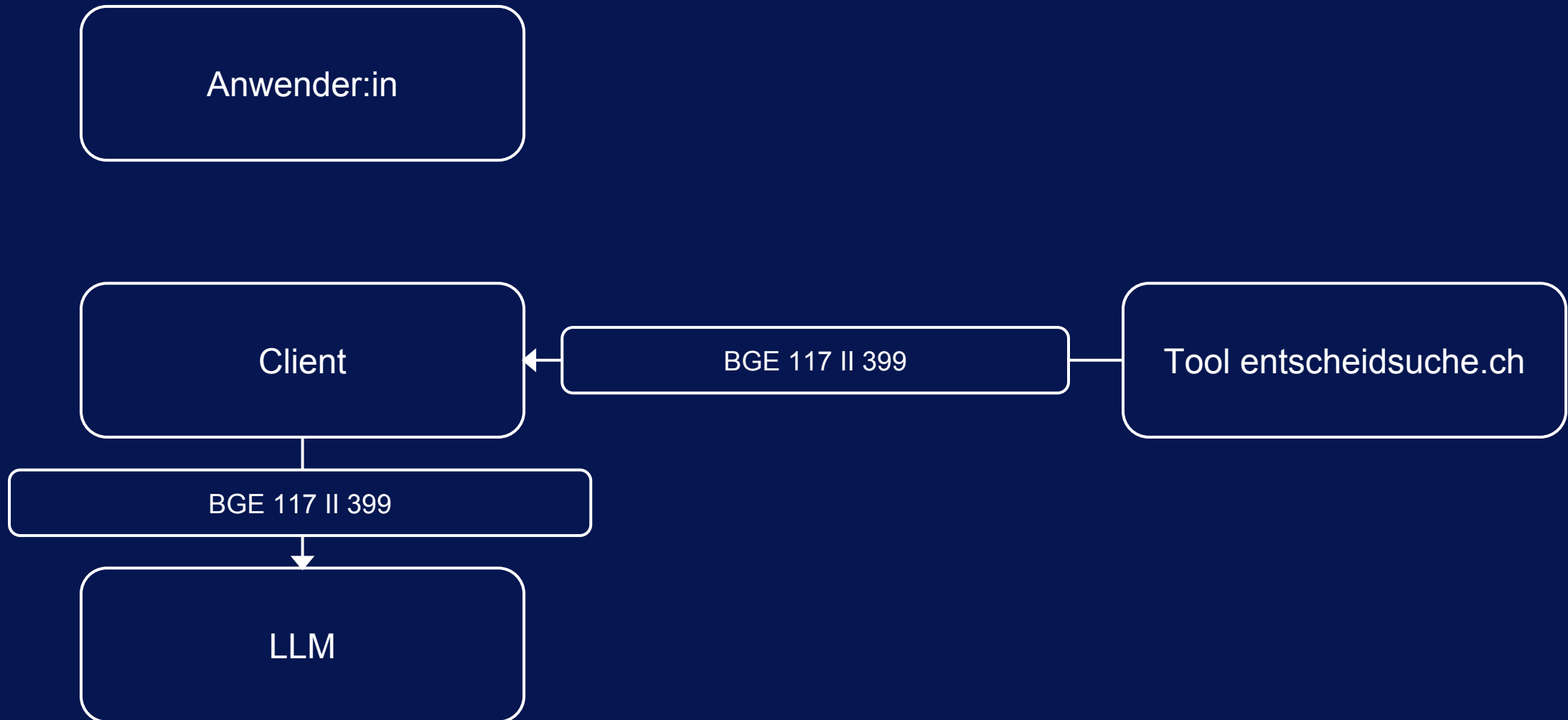
Beispiel: Verwendung einer Entscheiddatenbank



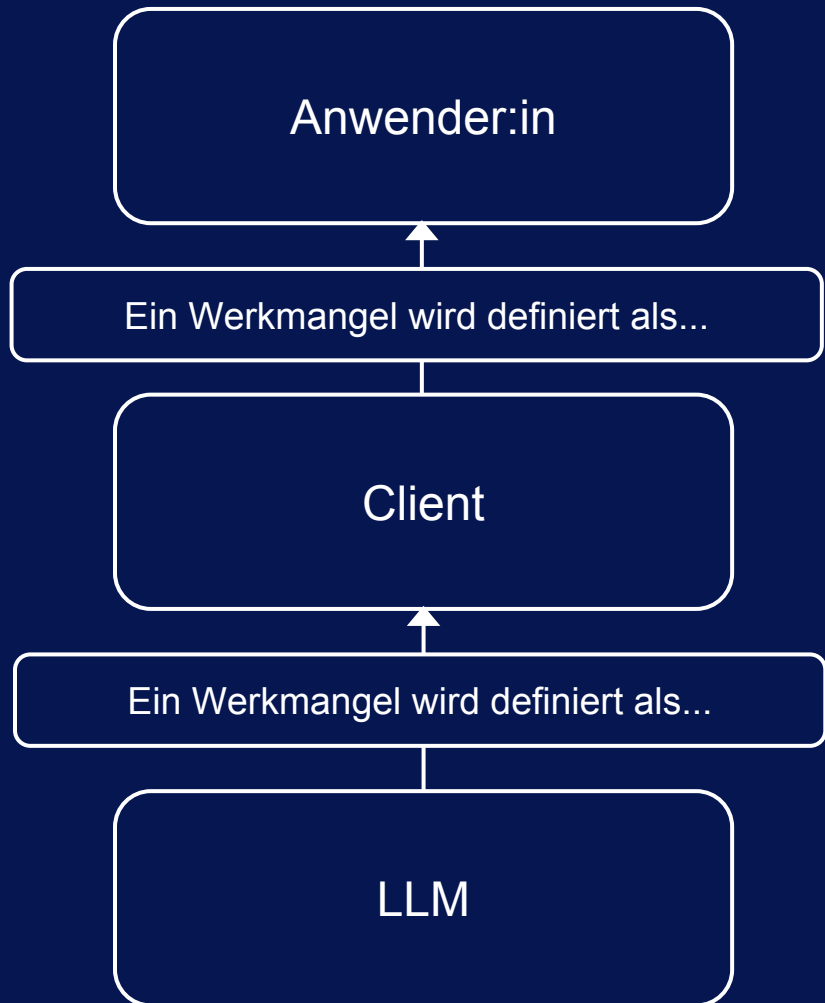
Beispiel: Verwendung einer Entscheiddatenbank



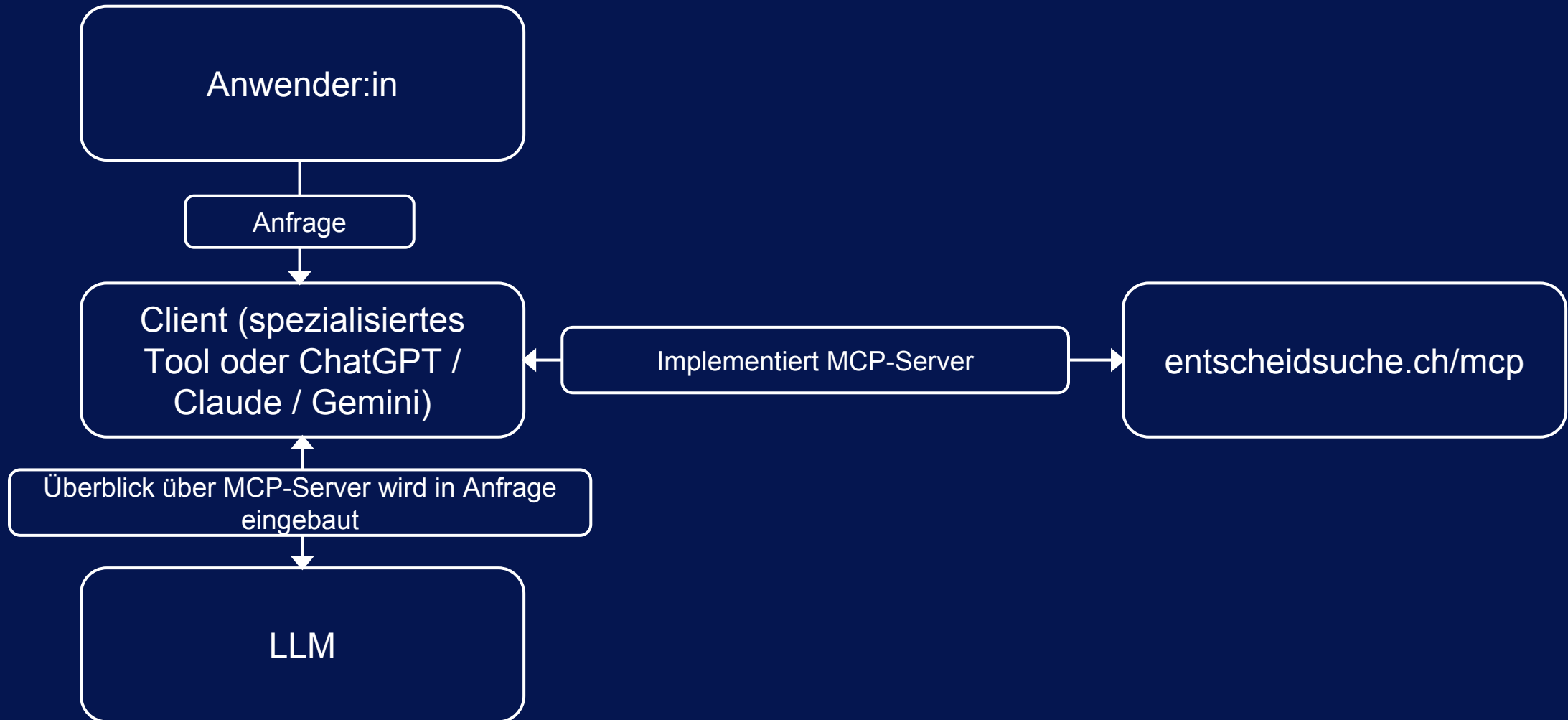
Beispiel: Verwendung einer Entscheiddatenbank



Beispiel: Verwendung einer Entscheiddatenbank

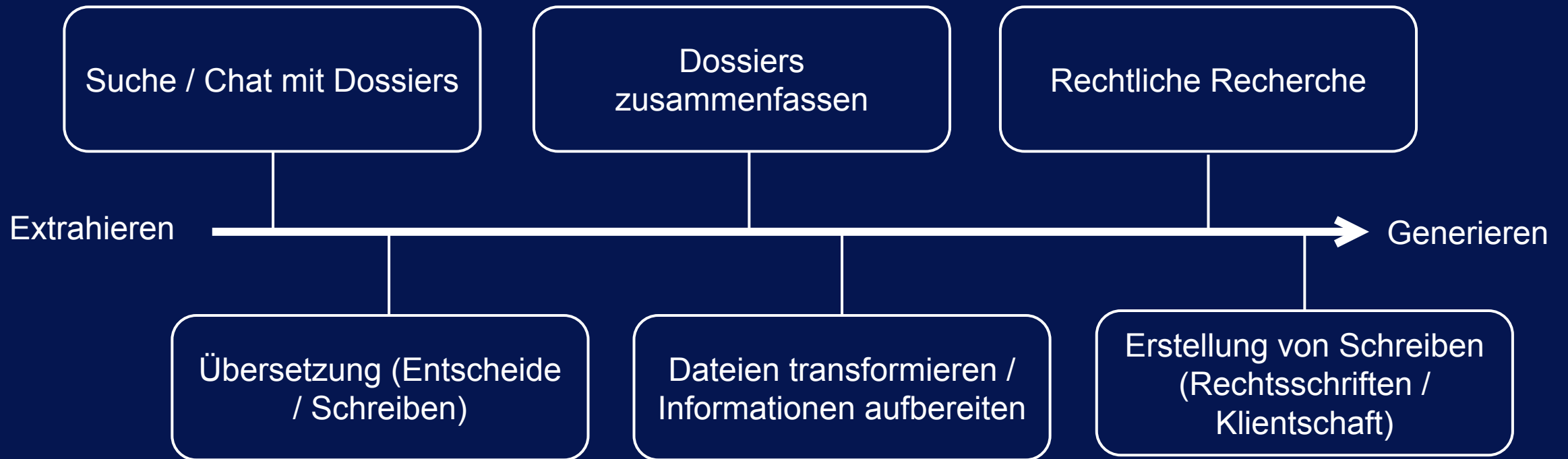


Model Context Protocol (MCP) als einheitlicher Standard

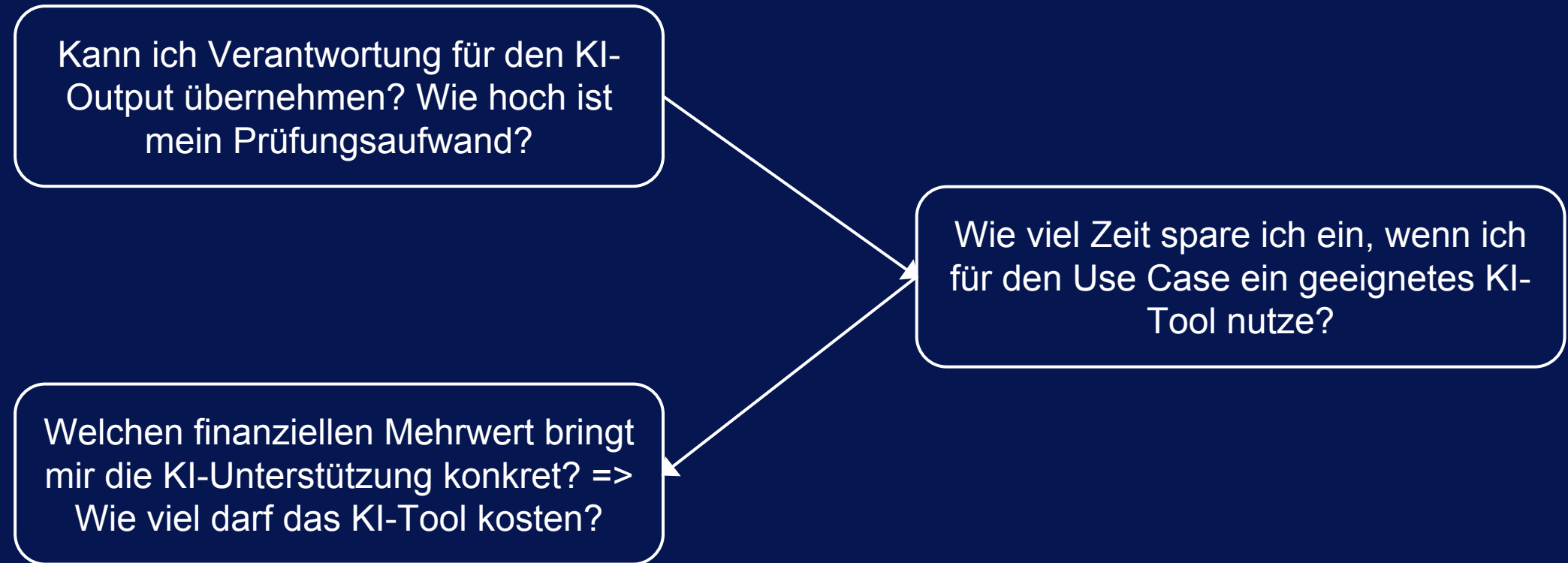


Wie prüfe ich, wo ich allgemeine und spezialisierte KI-Tool sinnvoll einsetzen kann?

Häufige Use Cases für LLMs im Legal-Bereich



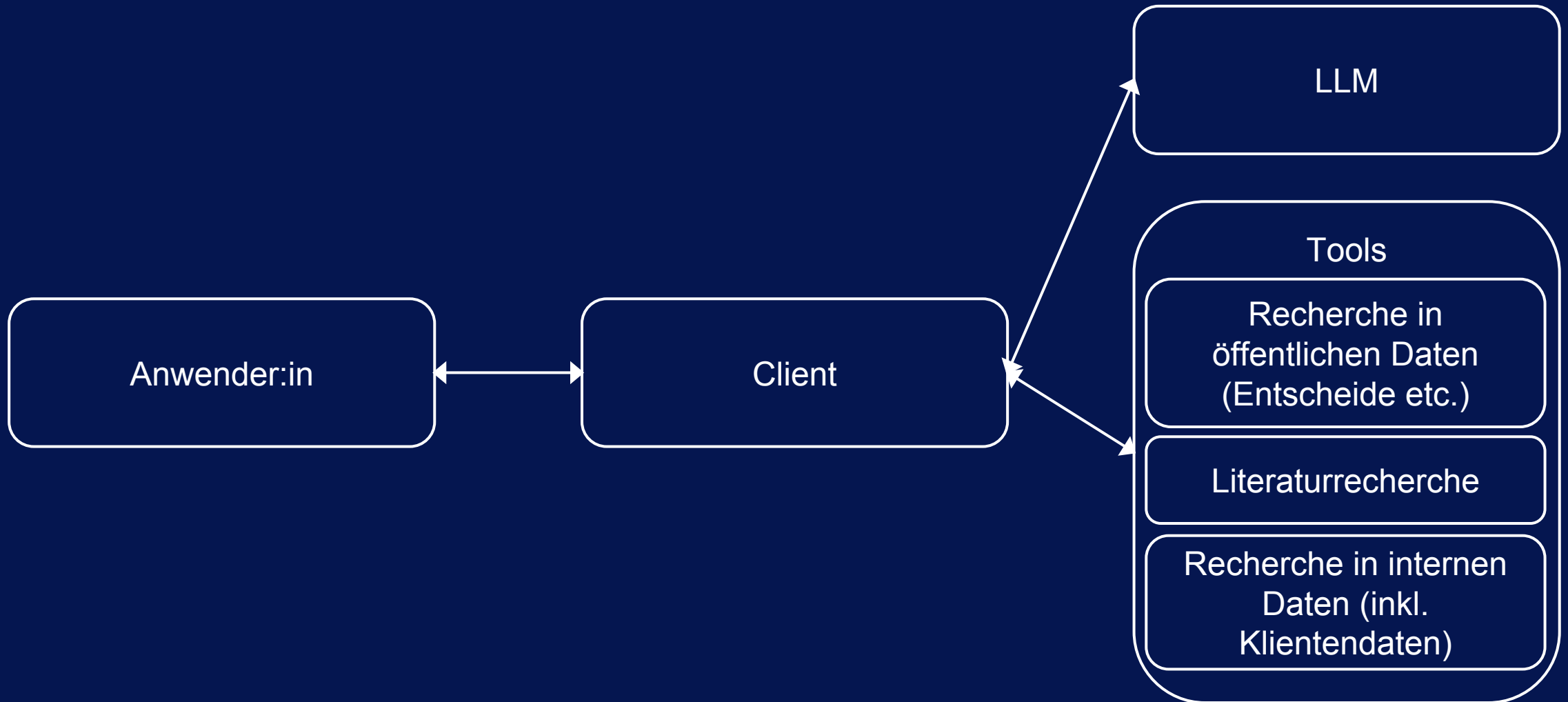
Prüfung von Use Cases



Welche Vorteile versprechen spezialisierte KI-Tools im Legal-Bereich?



Häufige Bestandteile von LLM-Anwendungen im Legal-Bereich



Häufige Datenquellen im Legal-Bereich

Gerichtsentscheide

Sonstige öffentliche
Quellen, insb.
Merkblätter und
Rundschreiben von
Behörden,
Onlinekommentar

Juristische
Fachliteratur

Eigene Daten
(interne Vorlagen,
Dossiers mit
Klientendaten,
„anonymisierte“ Dos-
siers)

Woher kann ich LLMs beziehen? Berufsgeheimnis?

Lokale Hardware /
LLM-Workstation
oder LLM-Server in
der Kanzlei

LLM-Hardware in
der Schweiz (Tool-
Anbieter oder
Schweizer Anbieter
für LLM-Inferenz
oder leistungsfähige
VPS)

Sog. Hyperscaler
(insb. Microsoft
Azure und Google
Cloud) mit
Datenresidenz in
der Schweiz und
Zusatzvereinbarung
en, hilfsweise
Datenresidenz in
der EU

Sog. Hyperscaler
(insb. Microsoft
Azure und Google
Cloud) mit
Datenresidenz in
den USA und ggf.
Datennutzung für
LLM-Training

Möglichkeiten für KI-Nutzung im Legal-Bereich

Eigenentwickeltes Tool mit lokalem LLM
=> allenfalls für sehr grosse Kanzleien

Standard-Chatbot (z.B. Claude,
ChatGPT) mit Tools via MCP

Eigenentwickeltes Tool mit LLM von
Drittanbieter => ebenfalls für kleinere
Kanzleien kaum rentabel

Spezialisiertes KI-Tool von Schweizer
Anbieter

«Anonymisierung»

Die Schweizerischen Bundesbahnen SBB, ein Institut des öffentlichen Rechts, welches als Kernaufgabe Dienstleistungen im öffentlichen Verkehr erbringt, führten im Jahr 2017 eine Ausschreibung durch.

70 % Person

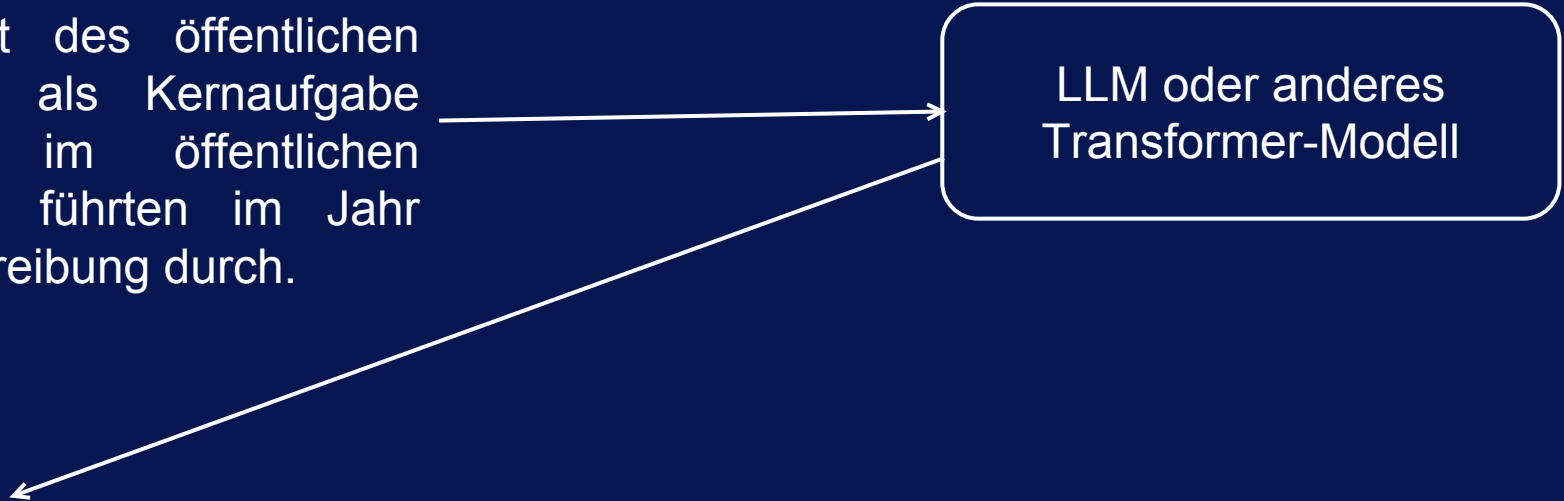
95 % Jahr

Kleine statistische
Modelle wie Microsoft
Presidio

Die [Person], ein Institut des öffentlichen Rechts, welches als Kernaufgabe Dienstleistungen im öffentlichen Verkehr erbringt, führten im Jahr [Jahr] eine Ausschreibung durch.

«Anonymisierung»

Die Schweizerischen Bundesbahnen SBB, ein Institut des öffentlichen Rechts, welches als Kernaufgabe Dienstleistungen im öffentlichen Verkehr erbringt, führten im Jahr 2017 eine Ausschreibung durch.



```
graph LR; A[Die Schweizerischen Bundesbahnen SBB, ein Institut des öffentlichen Rechts, welches als Kernaufgabe Dienstleistungen im öffentlichen Verkehr erbringt, führten im Jahr 2017 eine Ausschreibung durch.] --> B(LLM oder anderes Transformer-Modell); B --> C[Die [Person], ein Institut des öffentlichen Rechts, welches als Kernaufgabe Dienstleistungen im öffentlichen Verkehr erbringt, führten im Jahr [Jahr] eine Ausschreibung durch.];
```

LLM oder anderes
Transformer-Modell

Die [Person], ein Institut des öffentlichen Rechts, welches als Kernaufgabe Dienstleistungen im öffentlichen Verkehr erbringt, führten im Jahr [Jahr] eine Ausschreibung durch.

Zusammenfassung: Wie prüfe ich einen Use Case?

1. Ist der Use Case wirtschaftlich sinnvoll? Zu welchem Preis?
2. Welche Datenquellen braucht der Use Case?
3. Wie kann ich diese Daten rechtskonform nutzen? Braucht es ein spezialisiertes Tool?
4. Wie kann ich ein LLM rechtskonform mit diesen Daten nutzen?
5. Lohnt sich ein spezialisiertes Tool aus Gründen der Stabilität?

Beispiel: Prüfung zweier konkreter Use
Cases

Use Case 1: Zusammenfassung umfangreicher Akten

1. Verantwortung für den Output: Jedenfalls aus anwaltlicher Vorsicht ist es m.E. unzulässig, auf eine Zusammenfassung gleich welcher Art zu vertrauen. Der Zeitersparnis steht ein erhebliches Risiko gegenüber.
2. Datenquellen: Dossier mit Klientendaten, juristische Quellen demgegenüber weniger relevant
3. Sowohl LLM als auch KI-Tool müssen den Einsatz mit Klientendaten ermöglichen. Lokales Modell und Tool mit Betrieb in der Kanzlei und ohne Internetzugriff m.E. zulässig, alle anderen Bezugsformen derzeit Gegenstand rechtlicher Risikobewertung. Standard-Chatbots unzulässig.

Use Case 2: Recherche zu einer abstrakten Rechtsfrage

1. Verantwortung für den Output: Positive Treffer können validiert werden und sparen Zeit, aber Rückausnahmen müssen selbständig geprüft werden
2. Datenquellen: Öffentliche Daten (Entscheide, Onlinekommentar, Merkblätter von Behörden etc.), juristische Fachliteratur
3. Für öffentliche Daten und abstrakte Rechtsfragen kann m.E. grds. ein allgemeiner Chatbot mit MCP-Servern eingesetzt werden (z.B. Entscheidungsuche MCP, Onlinekommentar MCP). Nicht öffentliche juristische Fachliteratur erfordert ein spezialisiertes Tool mit Lizenz zur Verwendung der jeweiligen Daten => Kosten-Nutzen-Abwägung.
4. **WICHTIG:** Abstrakte Rechtsfrage darf keine Rückschlüsse auf konkreten Fall / Klienten zulassen!

Häufige Werbeaussagen und konkrete
Empfehlungen des Merkblattes



Es ist zu beobachten, dass einzelne in Werbekontexten gemachte Aussagen von Anbietern zu ihren KI-Tools bestenfalls missverständlich sind. Geltend gemachte Verbindungen mit renommierten Institutionen sind deshalb ebenso zu prüfen wie Angaben zu den Fähigkeiten und Nutzungsbedingungen der offerierten Produkte. Vor einem Vertragsschluss sind auch die Vertragsbedingungen zu prüfen. Namentlich sollte geprüft werden, ob der Vertrag allfällige mündliche oder per Email getätigte Zusagen des Anbieters abbildet.



Es ist nach derzeitigem Stand der Technik nicht möglich, faktisch unrichtige Aussagen durch ein KI-Tool (sogenannte Halluzinationen) gänzlich auszuschliessen. Jeglicher Output eines KI-Tools muss händisch überprüft werden. Ebenso ist es nach derzeitigem Stand der Technik nicht möglich, alle Kategorien von Personendaten in einer Datei mit hundertprozentiger Genauigkeit in der erforderlichen digital-forensischen Tiefe zu erkennen. Bei jeder durch KI-Tools ausgeführten Aufgabe sollte daher der Aufwand für eine eingehende händische Überprüfung in die Kosten-Nutzen-Abwägung einbezogen werden.



Weil weder Suchergebnisse noch juristische Texte in jedem Fall als objektiv richtig oder falsch bewertet werden können, sondern diese Einschätzung oft subjektiver Natur ist, sind Angaben des Anbieters zu Effizienzsteigerungen sowie allfällige Benchmarks für juristische KI-Tools mit Vorsicht zu betrachten. Dies gilt insbesondere dann, wenn ein Anbieter an der Erstellung des Benchmarks mitgewirkt hat. Es ist insofern im Voraus nicht möglich, zuverlässig einzuschätzen, wie gross der Nutzen eines KI-Tools für die eigene Tätigkeit sein wird oder ob überhaupt ein Mehrwert entsteht.



Empfehlung 1: Fragen Sie den Anbieter, ob er die KI-Modelle selbst betreibt. Ist dies nicht der Fall: Fragen Sie weiter, von welcher Unternehmung die KI-Modelle ggf. bezogen werden. In jedem Fall sollten Sie fragen, an welchen Orten die betreffenden Server stehen und an welchen Orten sonstige Datenverarbeitung durch den Anbieter sowie allfällige dritte Unternehmungen erfolgt (z.B. für den Betrieb des Frontends des KI-Tools, für Supportzwecke und Weiterentwicklung). Fragen Sie auch, welche KI-Modelle verwendet werden und ob Sie nach Vertragsabschluss über Veränderungen in diesem Bereich informiert werden.



Empfehlung 2: Fragen Sie den Anbieter, ob a) er selbst, b) die Unternehmung, welche die KI-Modelle bereitstellt, oder c) Dritte die in der Datenbank gespeicherten Dokumente sowie die Anfragen, welche Sie an das Tool stellen, technisch einsehen können. Fragen Sie weiter, ob und ggf. welche Vereinbarungen bestehen, um eine Einsichtnahme rechtlich zu verhindern. Fragen Sie sowohl für die von Ihnen hochgeladenen Dateien als auch für Ihre Anfragen weiter, welche Datenverarbeitungsschritte auf welchen Servern erfolgen, von wem diese Server an welchem Standort jeweils betrieben werden und ob die Daten für das Trainieren der auch von anderen genutzten Modellen verwendet werden.



Empfehlung 3: Falls der Anbieter mit besonderer juristischer Expertise seines KI-Tools wirbt: Fragen Sie, worin diese besteht. Grundsätzlich denkbar ist, dass der Anbieter ein eigenes LLM mit juristischen Daten trainiert oder ein bestehendes Basismodell mit juristischen Daten nachtrainiert, also ein Feintuning durchgeführt hat. Dies wird derzeit jedoch angesichts der hohen Kosten, der begrenzten Auswirkung auf die Antwortqualität und der raschen Entwicklung der Modelle selten durchgeführt. Meist beruht die «Expertise» vielmehr auf vorformulierten Prompts sowie der Einbindung externer Datenquellen wie Entscheid-, Literatur- und Gesetzesdatenbanken. Hierzu können Sie nachfragen, welche externen Datenquellen eingebunden wurden, aus welcher Quelle diese stammen und inwiefern die Lösung über die Websuche oder die Einbindung eines MCP* (bspw. OpenCaseLaw) in einen generalisierten Chatbot wie ChatGPT oder Claude hinausgeht.

* Das MCP (Model Context Protocol) ist ein Standard für Programmierschnittstellen, welche es LLMs erlauben, auf externe Datenbanken und Werkzeuge zuzugreifen. Der Begriff wird hier (wie im allgemeinen Sprachgebrauch) zudem für eine Schnittstelle verwendet, welche dem MCP-Standard folgt.



Empfehlung 4: Falls der Anbieter den Eindruck erweckt, seine Lösung schliesse Halluzinationen aus, ist Skepsis angebracht. Ein vollständiger und garantierter Ausschluss von Halluzinationen ist derzeit auch bei Einbindung externer und interner Datenquellen technisch nicht möglich. Möglich ist lediglich bei angegebenen Fundstellen die automatisierte Überprüfung, ob die Fundstelle existiert und ggf. einem zuvor erkannten Rechtsgebiet zugeordnet ist. Inhaltliche Aussagen des KI-Tools können derzeit überhaupt nicht zuverlässig überprüft werden. Sie können weiter nachfragen, ob der Anbieter eine verschuldensunabhängige Haftung für Folgeschäden einer Halluzination übernimmt.



Empfehlung 5: Vergleichbares gilt für die automatisierte Anonymisierung von Dateien. Fragen Sie den Anbieter, welche Kategorien von Personendaten erkannt werden und ob der Anbieter eine Garantie der vollständigen Anonymisierung gibt. Fragen Sie weiter, ob die Anonymisierung durch ein KI-Modell erfolgt und welche Datenverarbeitungsschritte die Dateien vor der Anonymisierung durchlaufen. Fragen Sie nach Tests und Testergebnissen hinsichtlich der Anonymisierung.



Empfehlung 6: Fragen Sie den Anbieter, ob es Nachweise oder zumindest Referenz-Kanzleien gibt, die für ausgewählte anwaltliche Geschäftsprozesse einen Effizienzgewinn durch die Anwendung des KI-Tools belegen können.



Empfehlung 7: Gerne können Sie dem BAV die Antworten der KI-Tool-Anbieter zukommen lassen. Der BAV stellt sie in geeigneter Art und Weise allen Mitgliedern zur Verfügung. Alle Fragen können auch direkt im Onlineformular beantwortet werden: <https://form.jotform.com/260965005190050>

Fazit

1. Es gibt keinen «one size fits all»-Ansatz, sondern der konkrete Use Case entscheidet.
2. KI-Einsatz ist immer eine Abwägung zwischen eigener Verantwortung und wirtschaftlichen Aspekten. Preisfindung und Vergütungsmodelle sind im Fluss.
3. Anbieter:innen spezialisierter KI-Tools im Legal-Bereich treffen teilweise sehr weitgehende Werbeaussagen. Diese sollten kritisch geprüft und bei den Anbietern nachgefragt werden.
4. Als Rechtsanwält:in sollten Sie zunächst prüfen, welche Use Cases Ihnen in Ihrer Praxis gewinnbringend erscheinen, deren finanziellen Nutzen bewerten und dies den verschiedenen Angeboten gegenüberstellen. Dabei sollten Sie die Transparenz der jeweiligen Angebote und das Vorliegen von «Red Flags» berücksichtigen.

Fragen

Senden Sie spätere Fragen gerne an jan.reinhardt@hyqu.ch