

KI-Microlearnings @ Ohm



Nächste Termine 10.00-11.30 Uhr

- 23.04.26 **Lust auf KI! KI macht Freude im Arbeitsalltag**, Prof. Dr. Y. Weiß
- 06.05.26 **Datenschutz & Ethik leicht erklärt**, J. Scheel
- 20.05.26 **KI und pdf-Dokumente** – Inhalte finden/ zusammenf., C. Schieber
- 16.06.26 **Mit KI produktiver schreiben**, D. Vode
- 15.07.26 **Wie kann ich in der KI-Welt gesund bleiben?**, Prof. Dr. K. Richter
- ? . 07.26 **Bilder und Diagramme mit KI erstellen**, K. Wendrich

Microlearnings für Lehrende

- 19.05.26 16.00-17.30 **Generative KI in der Lehre** –
Lehrmethoden für niederschweligen Einsatz, B. Meissner
- 12.06.26 10.00-11.30 **Eigenleistung in Prüfungen** –
trotz oder mit generativer KI?, B. Meissner
- 02.07.26 14.00-15.30 **Wieviel KI braucht meine Lehrveranstaltung?**, B. Meissner

KI-Microlearnings @ Ohm

Herzlich Willkommen zu

**Datenschutz und
rechtskonformer Umgang
mit Microsoft Copilot**

Dr. Johanna Scheel – Lukas Bischof Hochschulberatung





Lukas Bischof Hochschulberatung – Wir empowern Menschen & Teams an Hochschulen!

Dr. Johanna Scheel

Trainerin bei der Lukas Bischof Hochschulberatung

- Aus der Hochschule: Erfahrungen an der Schnittstelle zwischen Lehre, Organisationsentwicklung und Programmgestaltung
- Zertifizierte KI-Managerin

Themen

- KI für Hochschulen
- Orientierungs(studien)programme, Einführung & Optimierung
- Studiengangs-/Programmentwicklung
- Reflexionskompetenz, Selbstmanagement und Effizientberatung



1. Grundlagen und Rahmenbedingungen



Funktionsweisen und Begriffe

Klassische
Programmierung
und
Automatisierung

Studienplanung →
Modul B kann erst belegt
werden, wenn Modul A
bestanden ist.

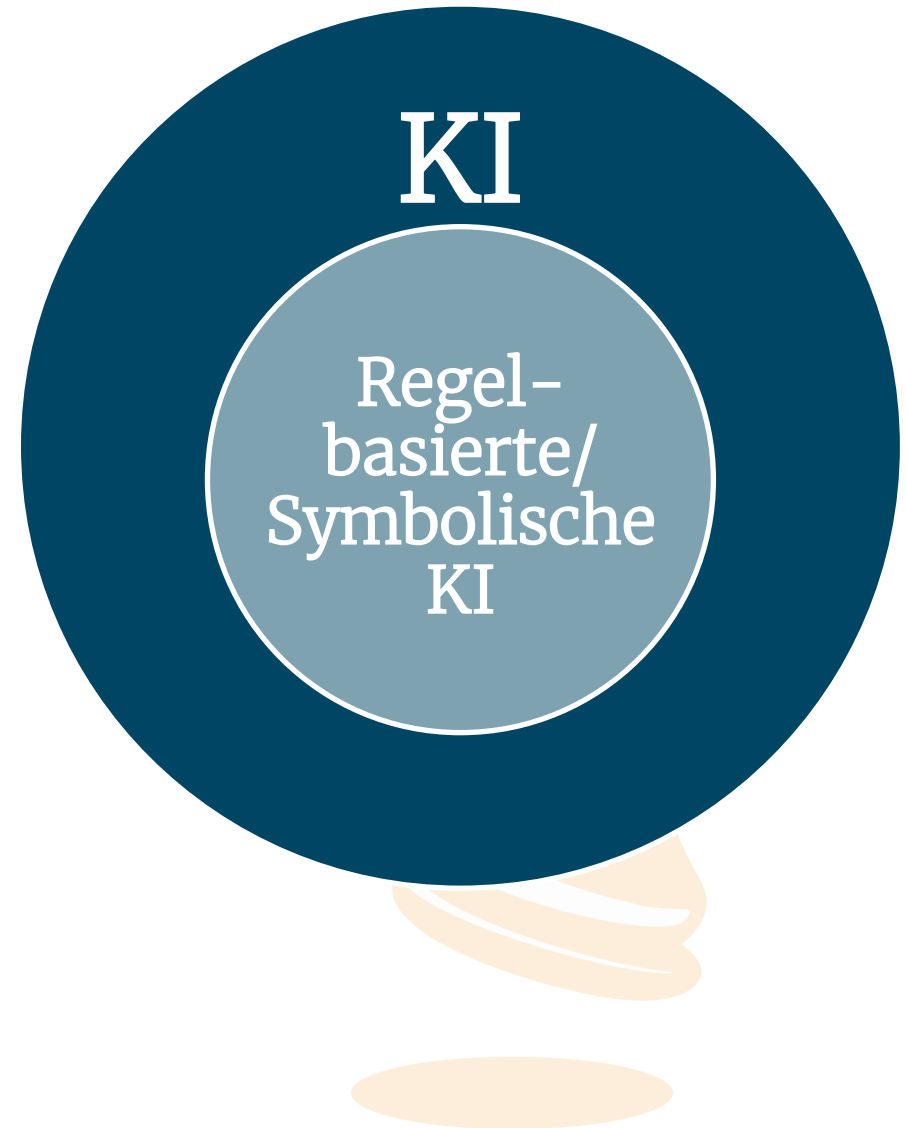
KI



Funktionsweisen und Begriffe

Speichert Wissen in Form von (Menschen-lesbaren) Begriffen und Regeln. So komplex, dass der Output intelligent wirkt.

Raum-/Stundenplan-Optimierung:
Variablen (Kurs×Raum×Zeit), Constraints (Kapazität, Ausstattung, Verfügbarkeit), Ziel (Minimiere Leerlauf, max. Auslastung).

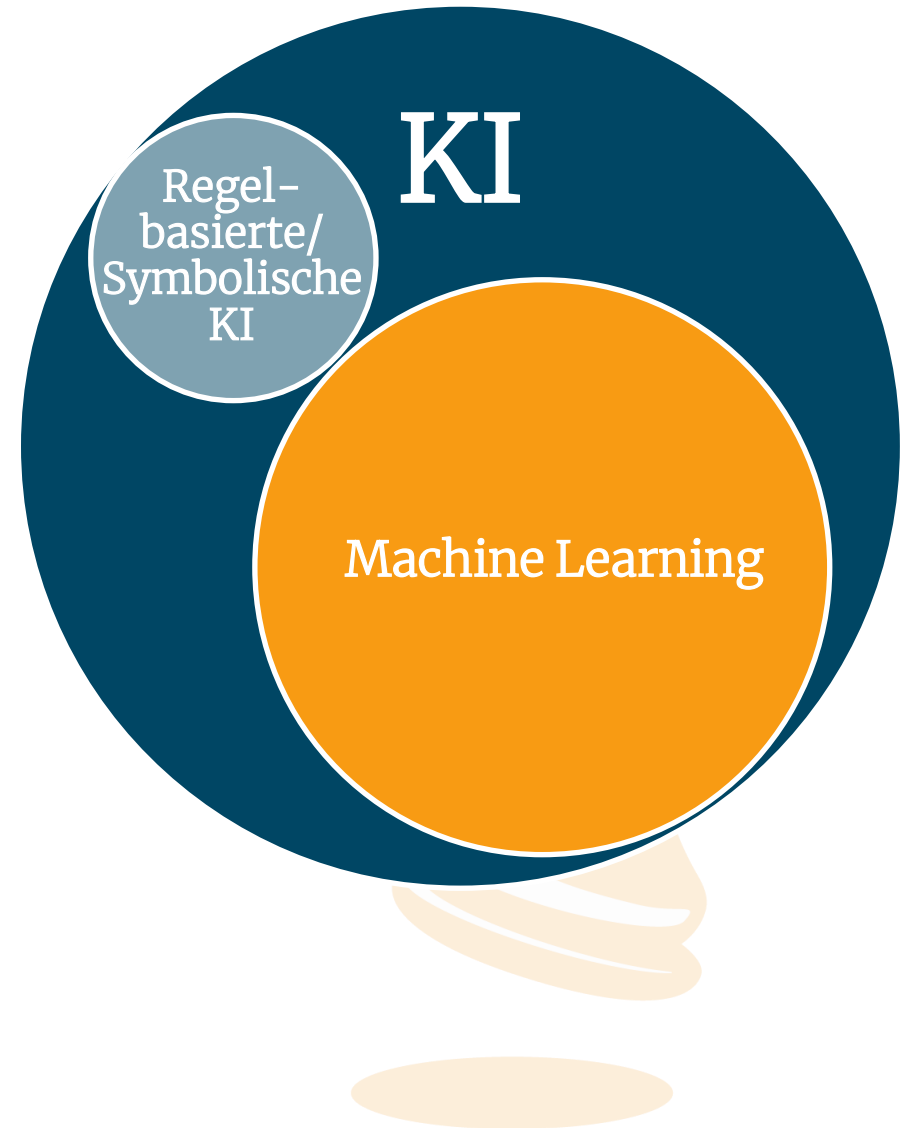




Funktionsweisen und Begriffe

"Modelle" speichern Wissen in Form von Mustern; (selbst) gelernt aus (historischen) Daten statt harten Regeln; der Output wird statistisch errechnet.

Studienabbruch-Vorhersage: Variablen (Studierende × Merkmale wie Notendurchschnitte, Anwesenheitsraten, Online-Lernaktivitäten, sozio-demografische Daten), historische Daten & Modell, Ziel: frühzeitiges Erkennen und Beraten





Funktionsweisen und Begriffe

„Neuronale Netze“ speichern Wissen in Form geschichteter Verarbeitungsschritte/Transformer-architektur; sie lernen diese Strukturen aus sehr großen Datenmengen → hoher Rechenaufwand → leistungsfähig bei komplexen Anforderungen.

Output: „Generative KI“ → Bild, Text, Video, Sprache, ...

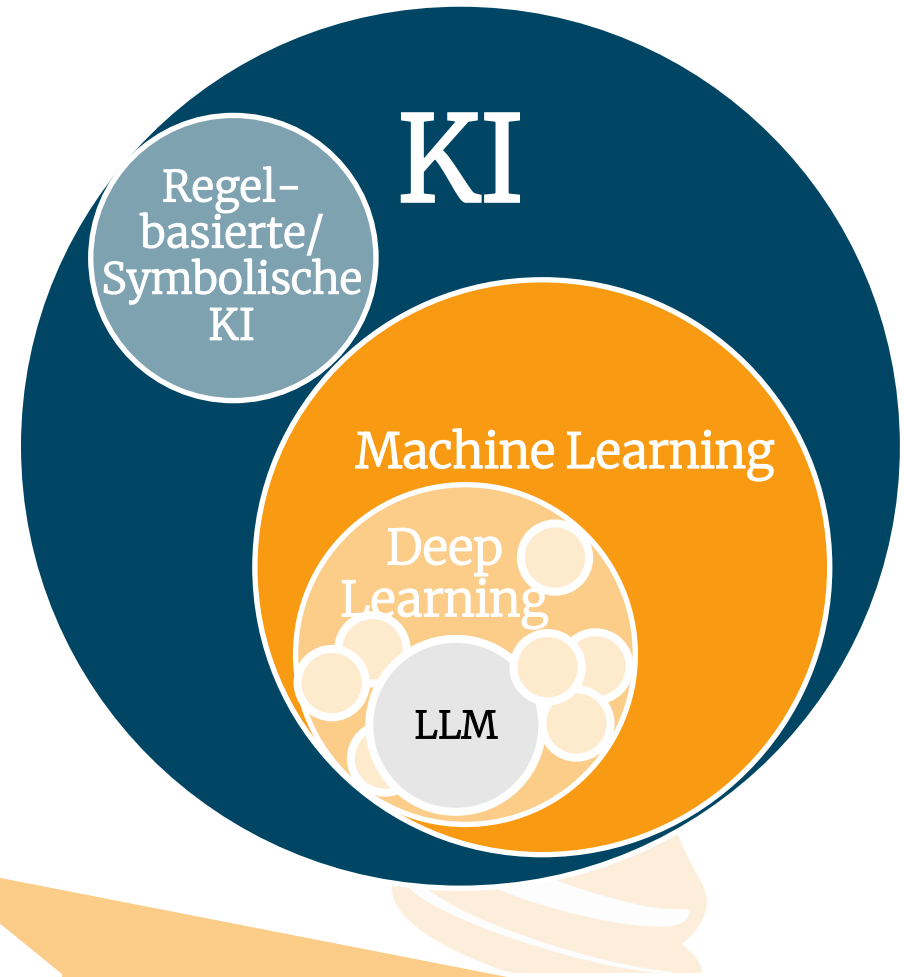
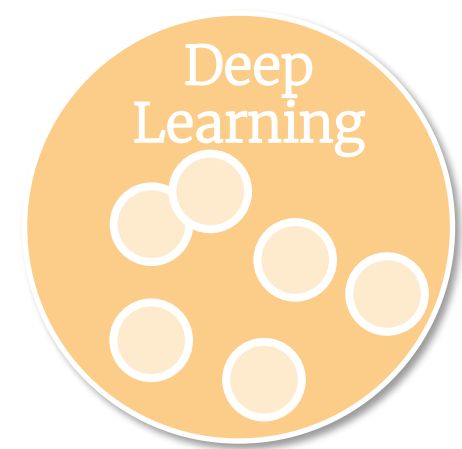


Bild-, Sprach- und Textverarbeitung jeglicher Art: ChatGPT / Copilot-Chat; weitere Chatbots, Bild-Analyse, Sprach- und Audioanalyse/Übersetzung...



Deep-Learning-Modelle (bspw. LLM): Basisdaten

Trainingsdaten

„Training“ des Modells mit riesigen Datensätzen (Text, Bilder, Audio, Video), aus denen **Muster** erlernt werden.

Danach KEIN Zugriff mehr auf diese Daten = ein Modell ist **keine Datenbank!** Output = statistisch!

Modellgewicht: Schwerpunkt der Daten

Output-Generierung: „Black Box“.
Outputdaten: ggf. Verzerrung,
Fehlergenerierung, Urheberschaft.

Inferenzdaten

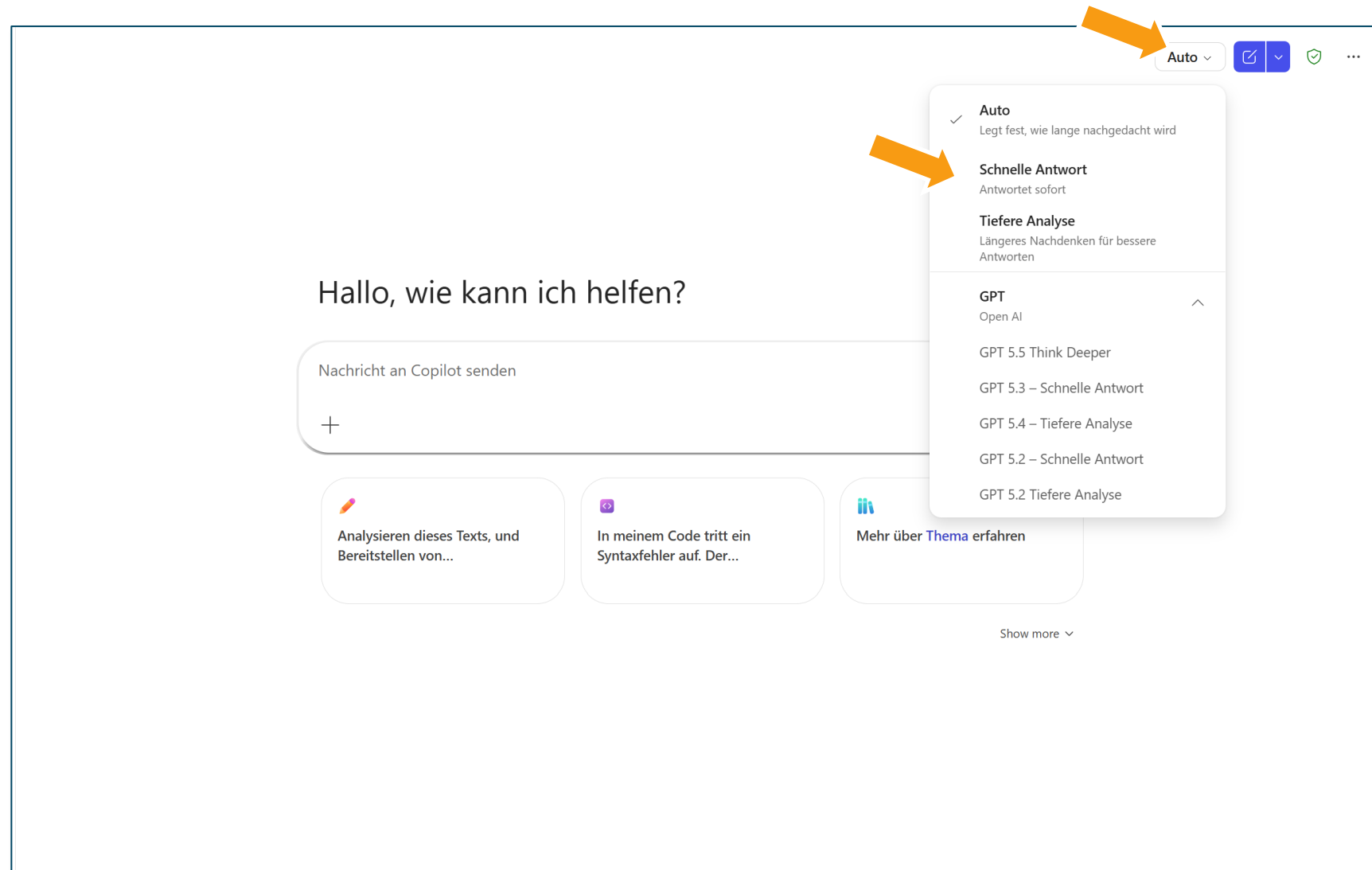
ALLES was in der Nutzung passiert:

- **Eingaben** (Text, Bild, Video, Audio)
- **Logfile** (IP, Zeitstempel, Metadaten)
- Browser- & Gerätedaten
- Ggf. Anmeldedaten (Email, Klarname)

→ werden außerhalb des Modells in der (Plattform-/Cloud-)Infrastruktur des Herstellers/Anbieters gespeichert

Datenverantwortung bei Input,
Sensibilität gegenüber
Datenverarbeitung

Copilot-Modelle = ChatGPT-Modellfamilie

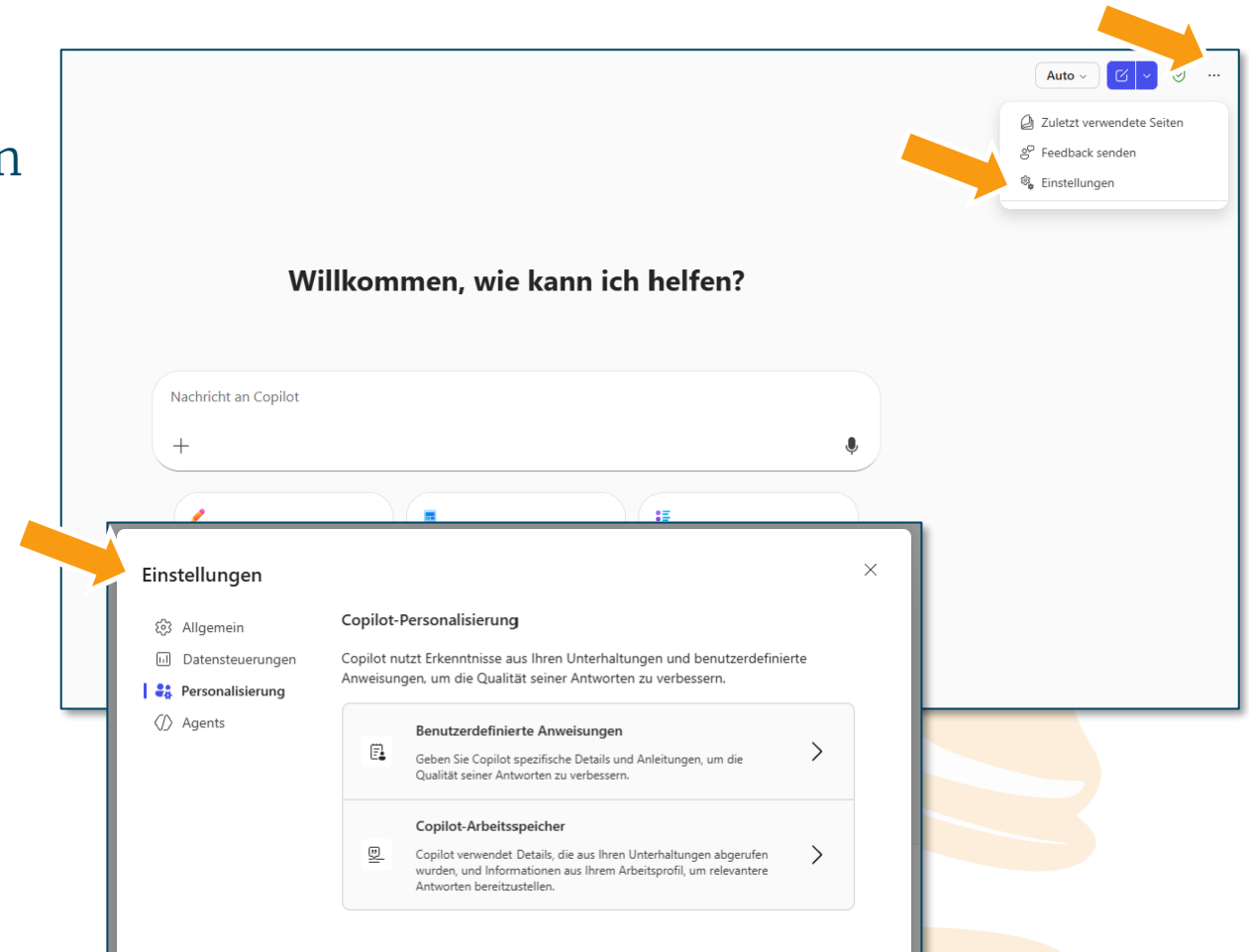




Basisdaten: Wissenszugaben in LLMs

Dauerhafte Wissenszugabe

- **institutionell**: „Finetuning“ von Modellen oder zusätzliche System-Prompts
- **individuell**:
 - „**Merken**“ von Chatinhalten (= „Erinnerung“ / „Memory“)

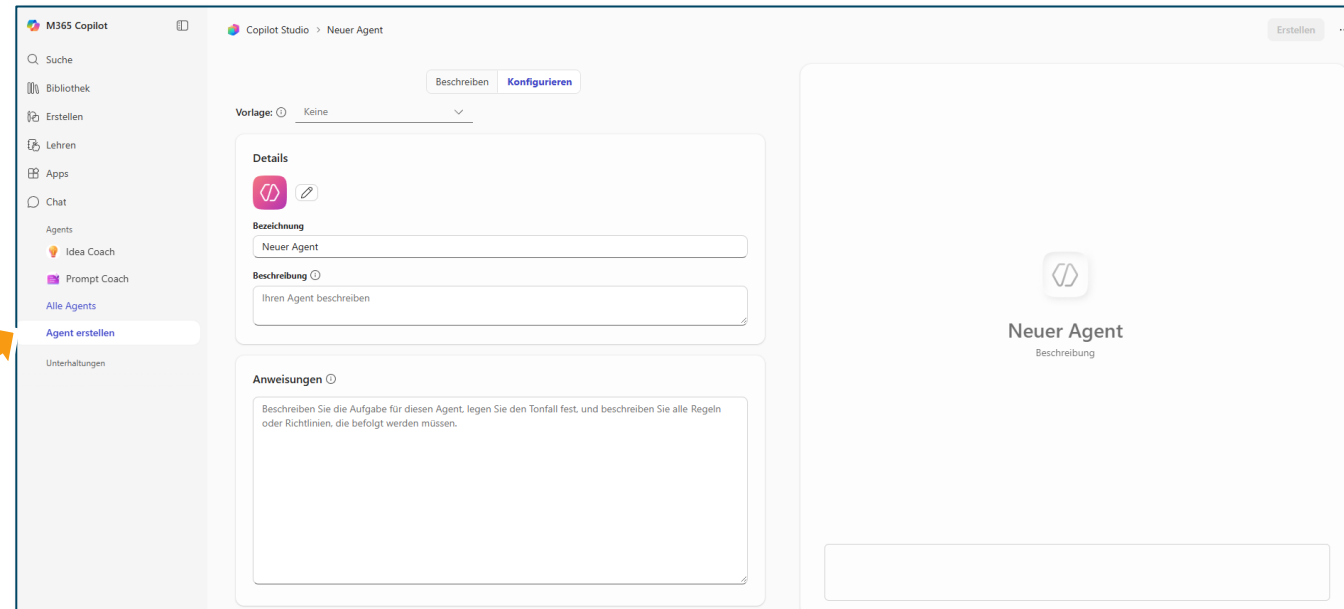




Basisdaten: Wissenszugaben in LLMs

Dauerhafte Wissenszugabe

- **institutionell**: „Finetuning“ von Modellen oder **zusätzliche System-Prompts**
- **individuell**:
 - „Merken“ von Chatinhalten (= „Erinnerung“/ „Memory“)
 - **themenbezogene Wissensspeicher RAG (Retrieval-Augmented Generation)**: Eigene „GPT“ (bei ChatGPT) oder Copilot „Agenten“ → Webseiten hinzufügen/ Noch keine Dateizugabe





Basisdaten: Wissenszugaben in LLMs

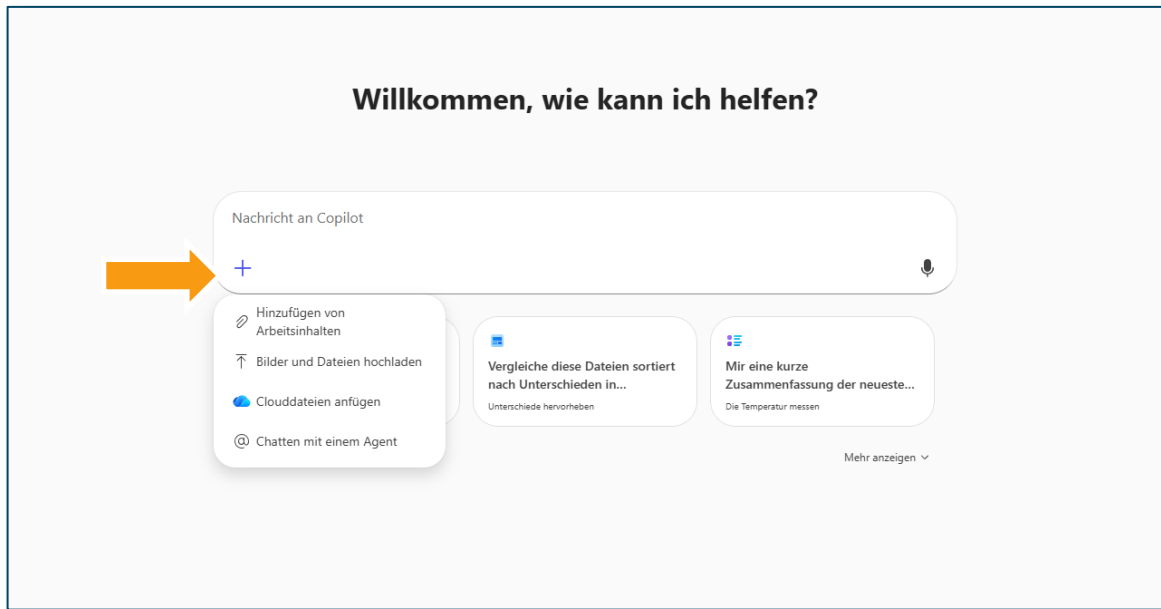
Temporäre Wissenszugaben

RAG (Retrieval-Augmented Generation)

Modell hat während der Inferenz zusätzlich **temporären Zugriff** auf externe Wissensquellen

- Web
- Gegebene Medien (Dokumente, Tabellen, Bilder, Screenshots...).

Das Modell bleibt **dasselbe**, es bekommt aber durch die Suchergebnisse/die Dateieingabe **zusätzlichen Kontext**.





Umgang mit Daten

Inferenzdaten

Was gebe ich dem Modell?

Datenverarbeitung

Was macht die KI-Infrastruktur mit den Daten?

Ausgabedaten

Welche Risiken entstehen durch den Output?

RISIKEN:

- Metadaten (Ort, Zeit, Gerät, IP, Session-Daten etc.)
- Personen-bezogene Daten
- Biometrische Daten (Bild, Stimme, Körpermerkmale)
- sensible Daten
- Fremde Inhalte (Urheberrecht)

- (bei externen Tools)
- Verwendung für Modell-Training
 - Speicherung und Auswertung
 - Weitergabe (Third-Party-Services)

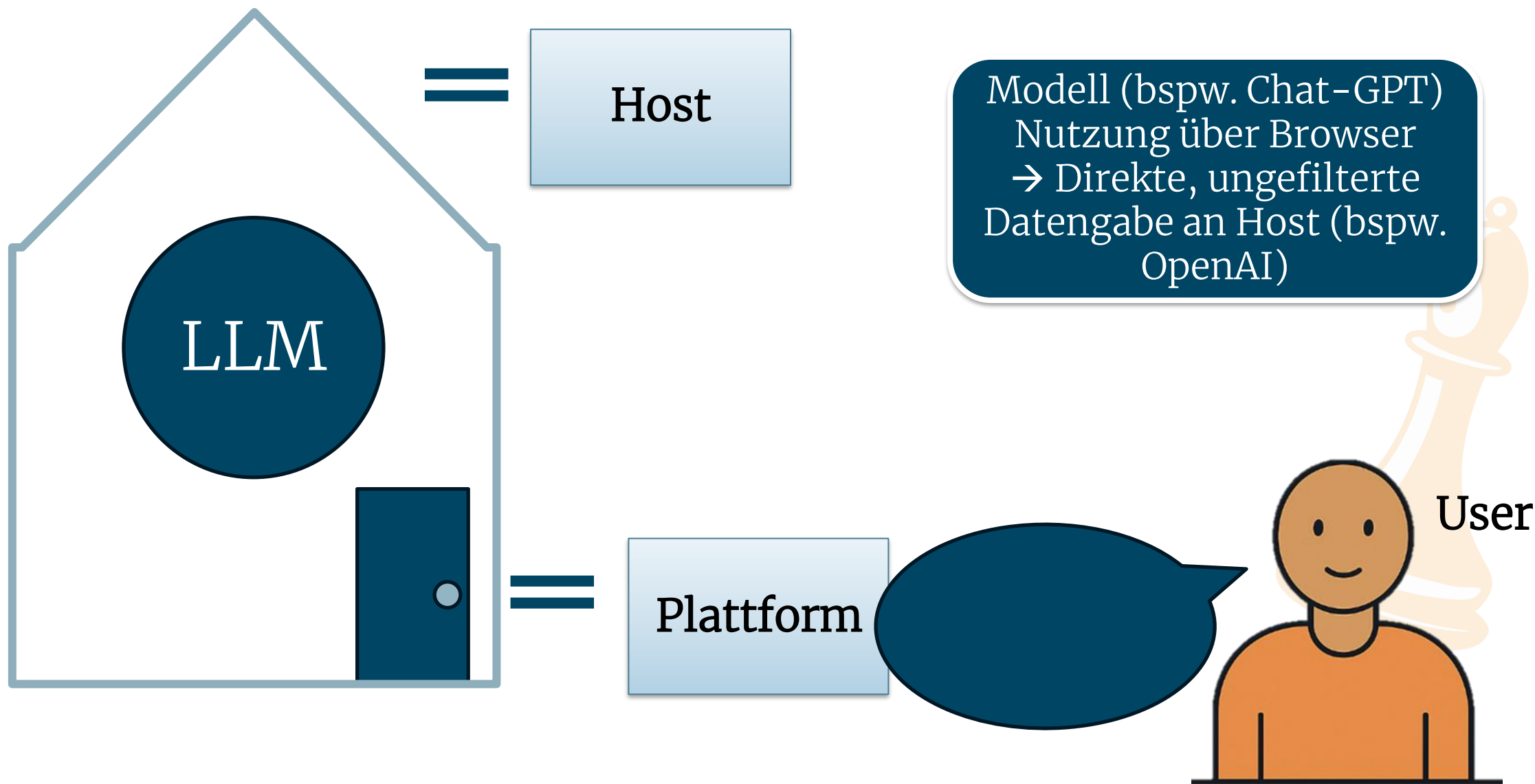
- Bias / verzerrte Darstellungen
- Deepfakes / Ähnlichkeitsrekonstruktion
- Fehlinformationen / Halluzinationen
- Rechteverletzungen durch generierte Medien (Urheberrecht)



**KI-Kompetenz
bedeutet auch
Datenschutzkompetenz**

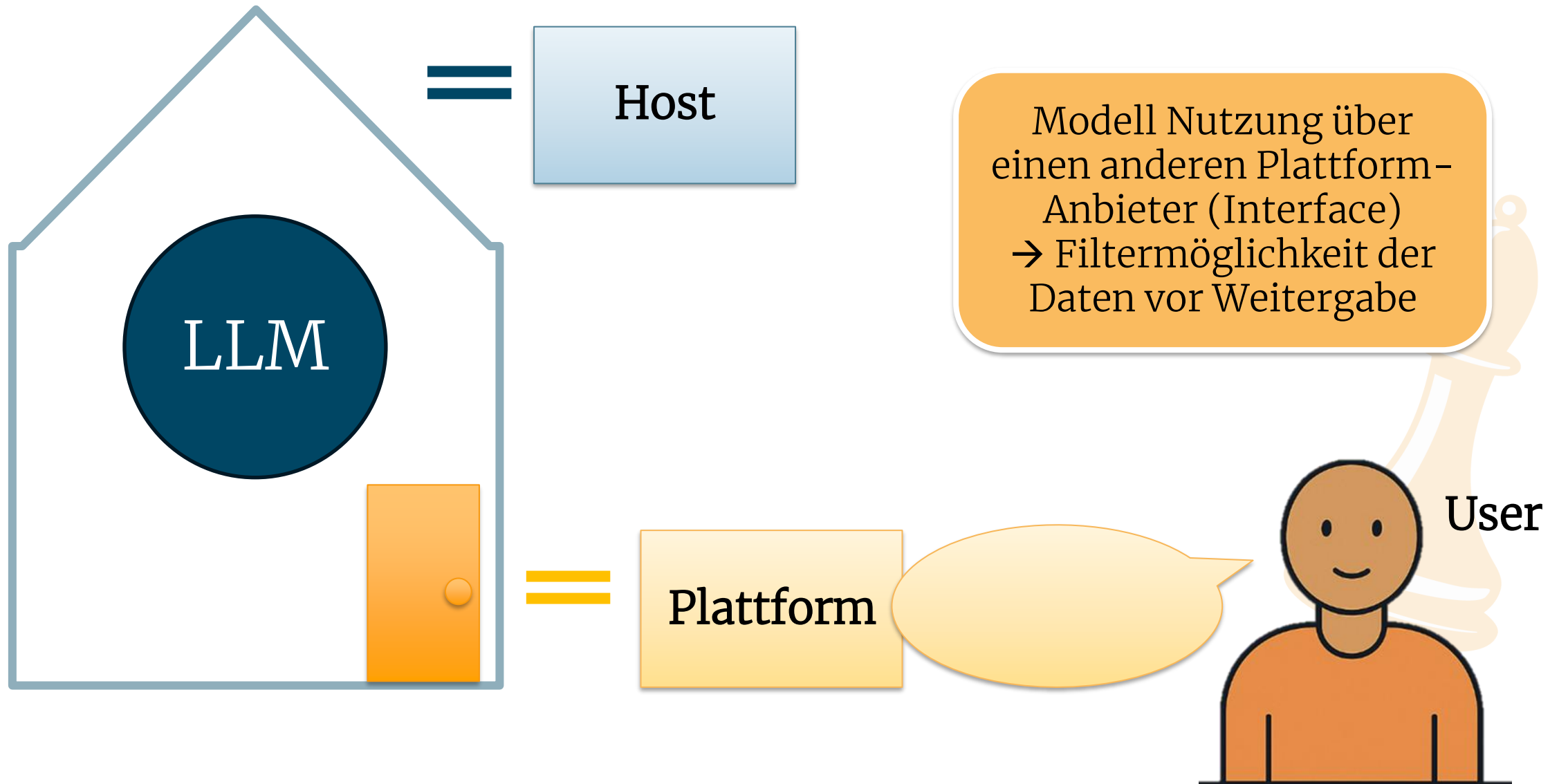


Datenfluss bei der KI-Nutzung – Szenario 1



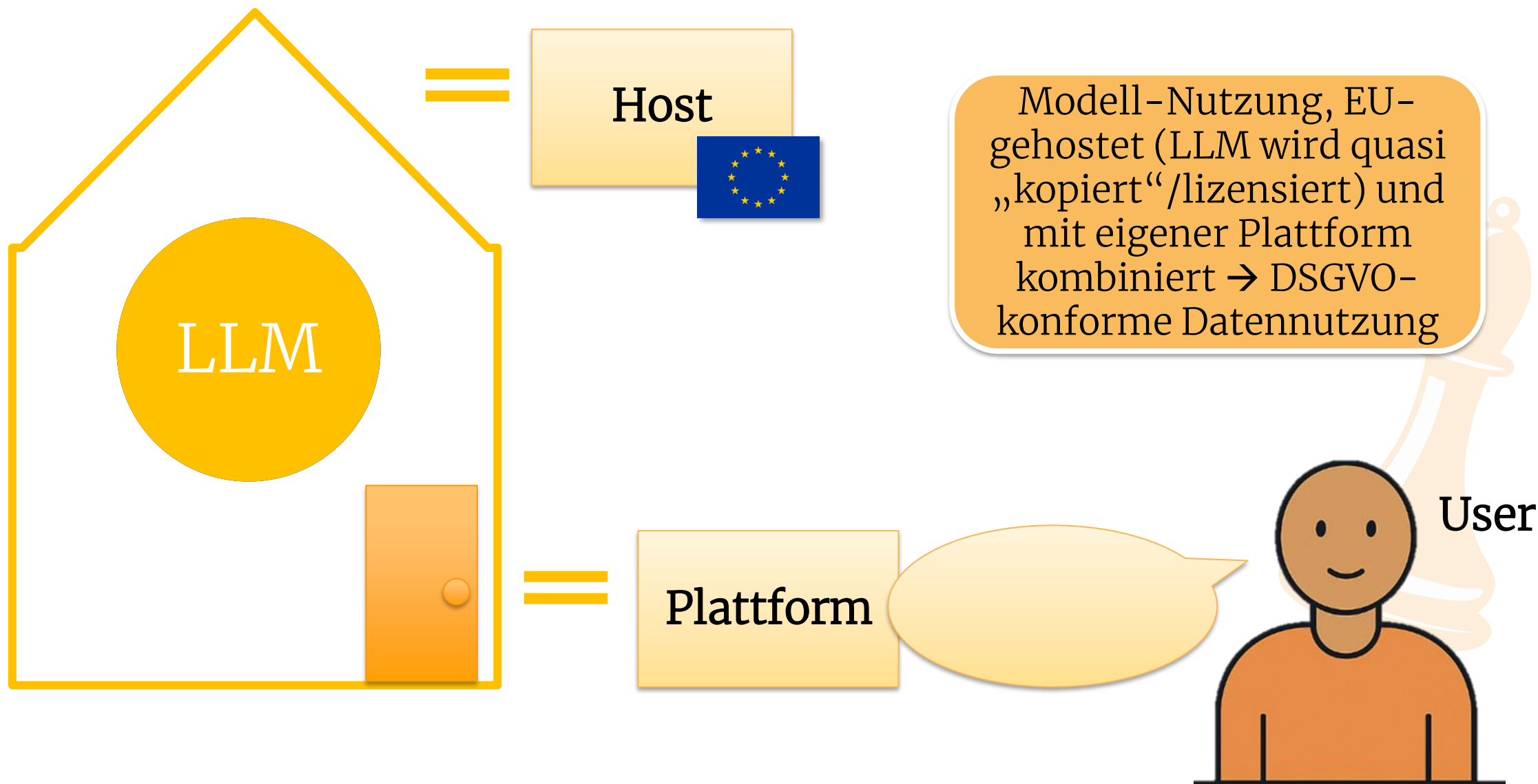


Datenfluss bei der KI-Nutzung – Szenario 2



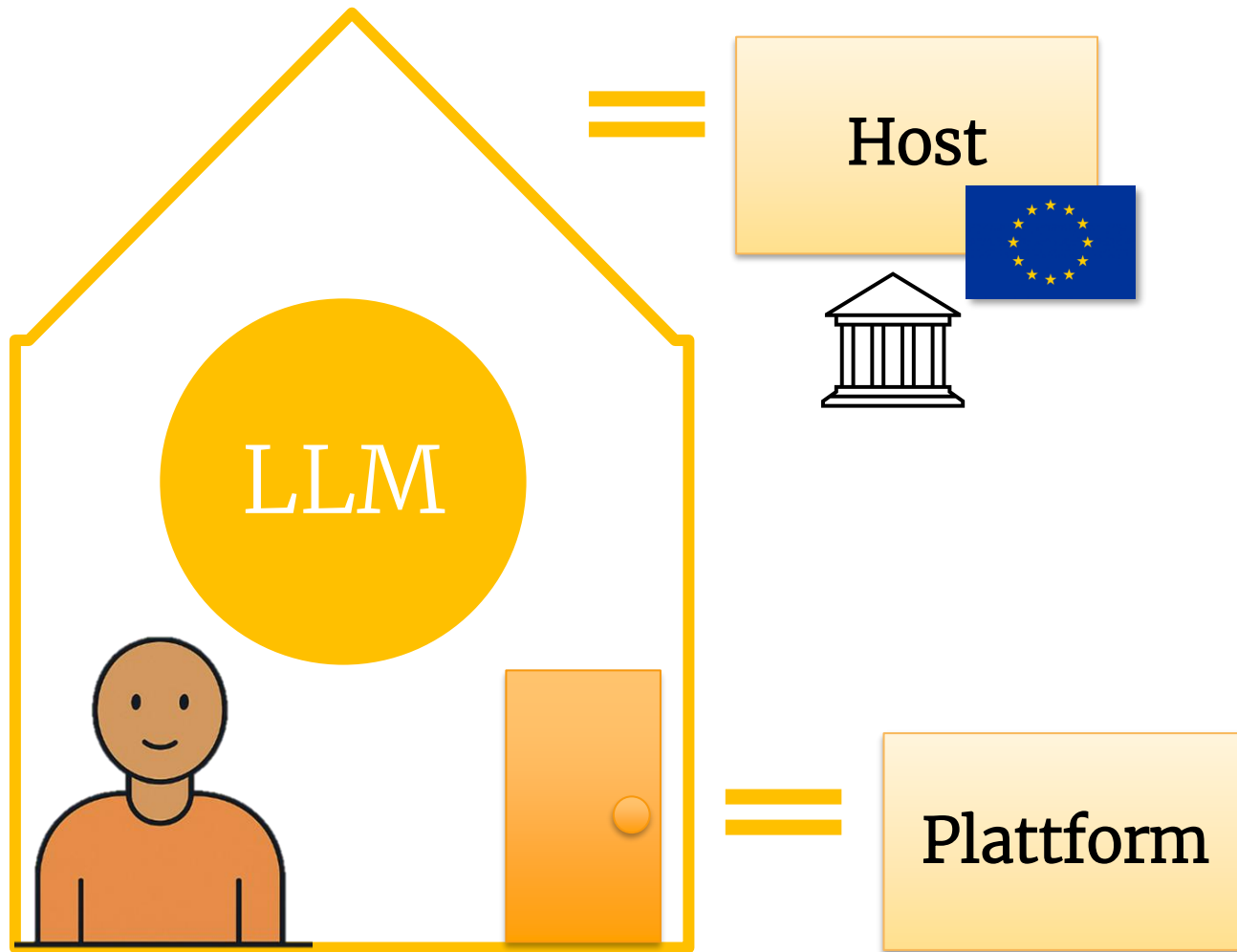


Datenfluss bei der KI-Nutzung – Szenario 3





Datenfluss bei der KI-Nutzung – Szenario 4

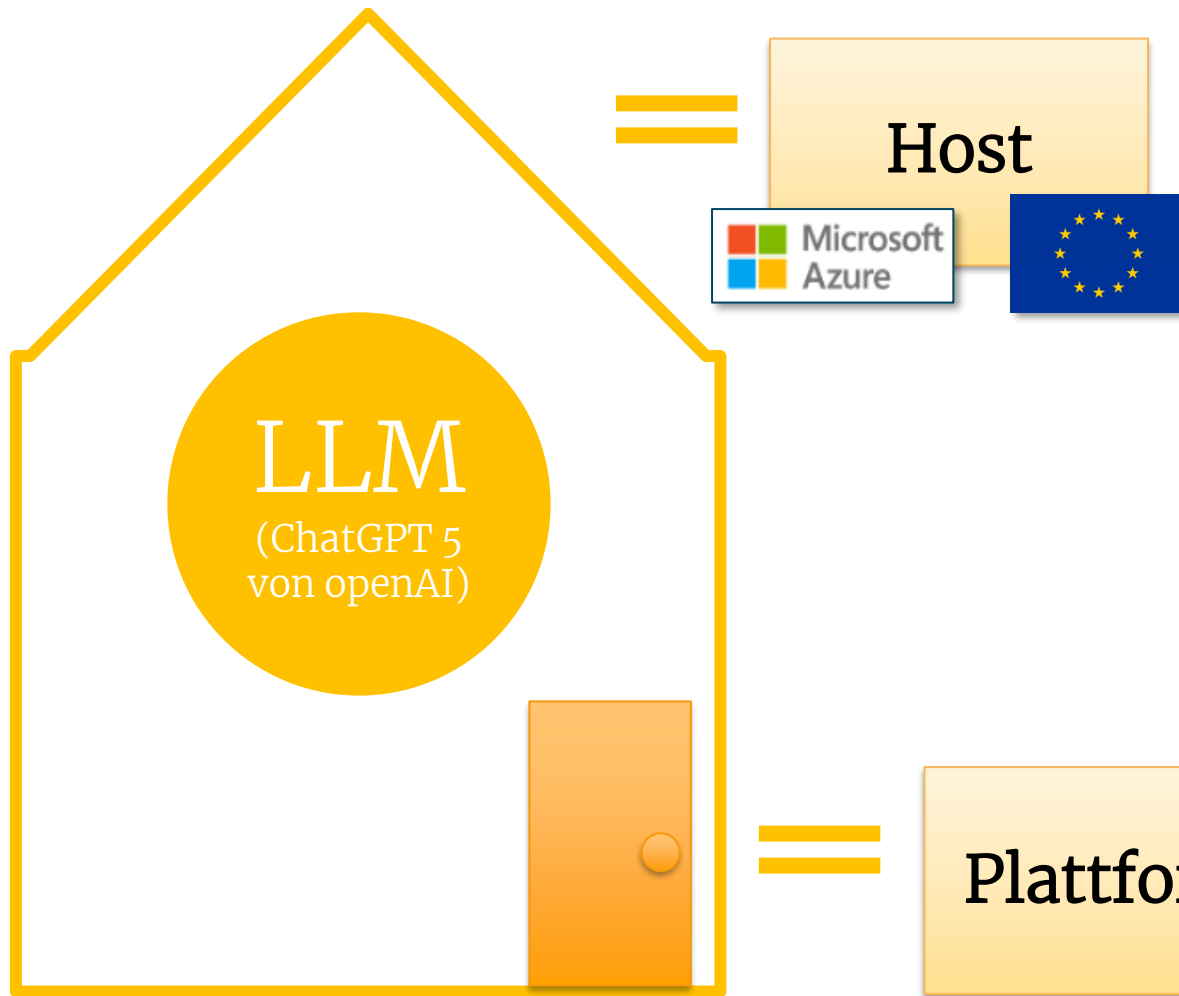


Modell wird lokal (on Premises) gehostet mit eigener Plattform
→ volle eigene/ institutionelle Kontrolle über die Daten





Datenfluss bei der KI-Nutzung – an der OHM



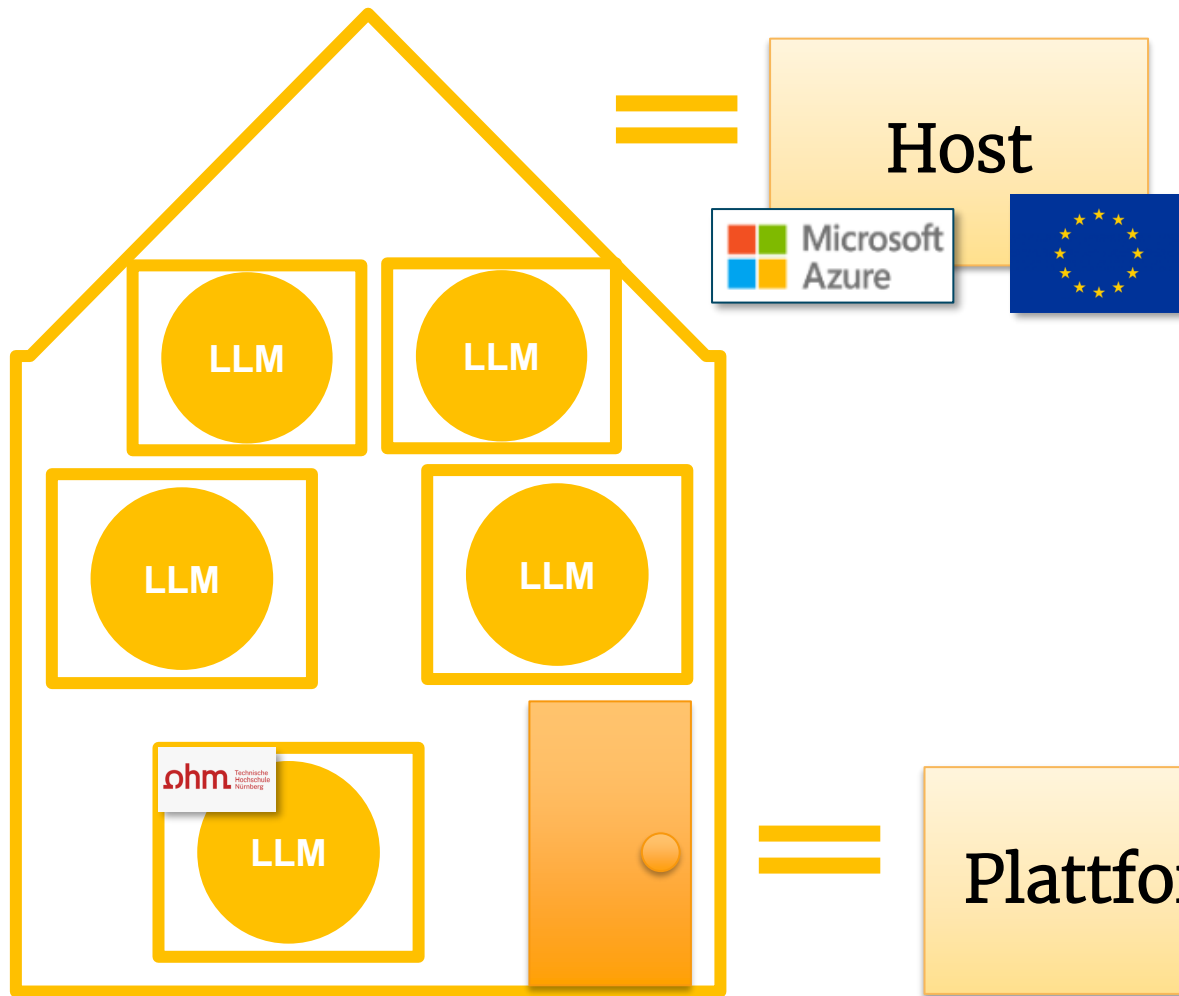
Szenario 3/4



- LLM: ChatGPT-5-Familie, „Orchestrator“: Microsoft (Azure AI)
- Copilot-Chat: In der EU auf den Servern von Microsoft in einzelnen Tenants (=Mandanten/ Datenisolierung & Verschlüsselung) gehostet



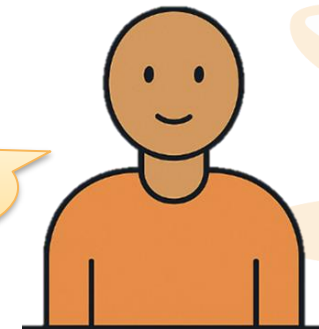
Datenfluss bei der KI-Nutzung – an der OHM



Szenario 3/4

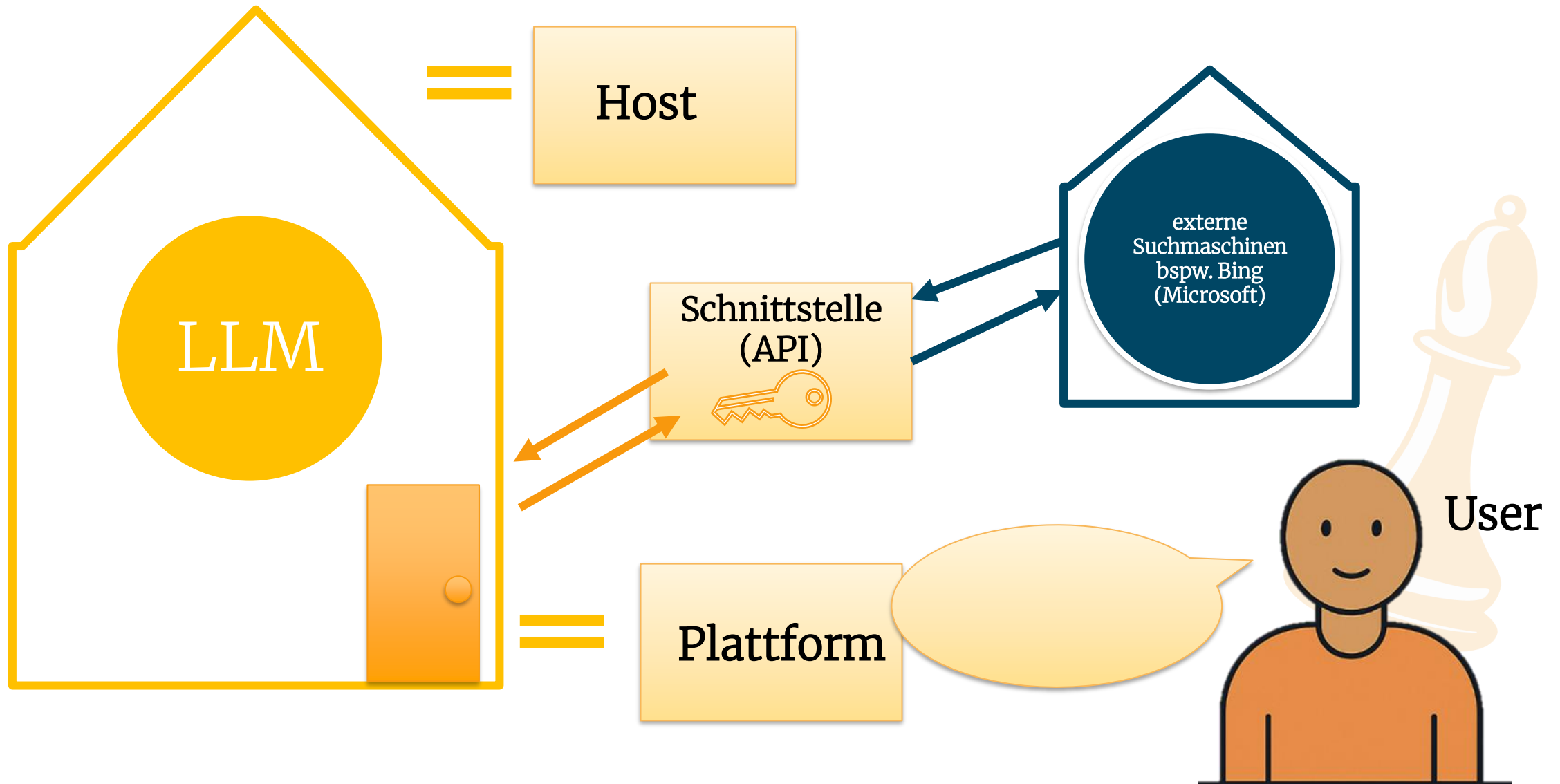


- LLM: ChatGPT-5-Familie, „Orchestrator“: Microsoft (Azure AI)
- Copilot-Chat: In der EU auf den Servern von Microsoft in einzelnen Tenants (=Mandaten/ Datenisolierung & Verschlüsselung) gehostet
- Keine Weiterverwendung der Daten, DSGVO greift
- Sichere Schnittstelle von Microsoft zur Verfügung gestellt und angepasst: Einloggen über TH-Nürnberg-Account





Datenfluss bei der KI-Nutzung – mit Websuche



Umgang mit Daten

EU KI-VO & DSGVO

1. Regularien & Verbote

KI-VO: Nur *bestimmte* Praktiken verboten (z. B. biometrische Massenüberwachung): Risikokategorien definiert und reglementiert.

DSGVO: Personenbezogene & sensible Daten → **strenge Bedingungen**, aber kein generelles KI-Input-Verbot: es gilt: Minimierung, Zweckbindung, Erforderlichkeit.

2. Pflichten (für Nutzer*innen & Institutionen)

Abwägung: Risiko einschätzen. Welche Daten gebe ich ein? → Minimierung!

Transparenz: Dritte informieren, (auf)klären wo Daten landen

Dokumentation: Abwägung & Nutzung dokumentieren

3. Verantwortung

Nutzer: Einhaltung der geltenden Regularien (DSGVO, KI-VO, interne Richtlinien). Keine unnötigen personenbezogenen oder sensiblen Daten in externe KI eingeben!

Institution: Richtlinien, Freigaben, sichere Tools bzw. AV-Verträge bereitstellen.

Risikoanalysen und Governance sicherstellen



Umgang mit Daten



Hochschuleigene Richtlinien

Welche Regelungen gelten für (über KI-VO hinaus) für mich?

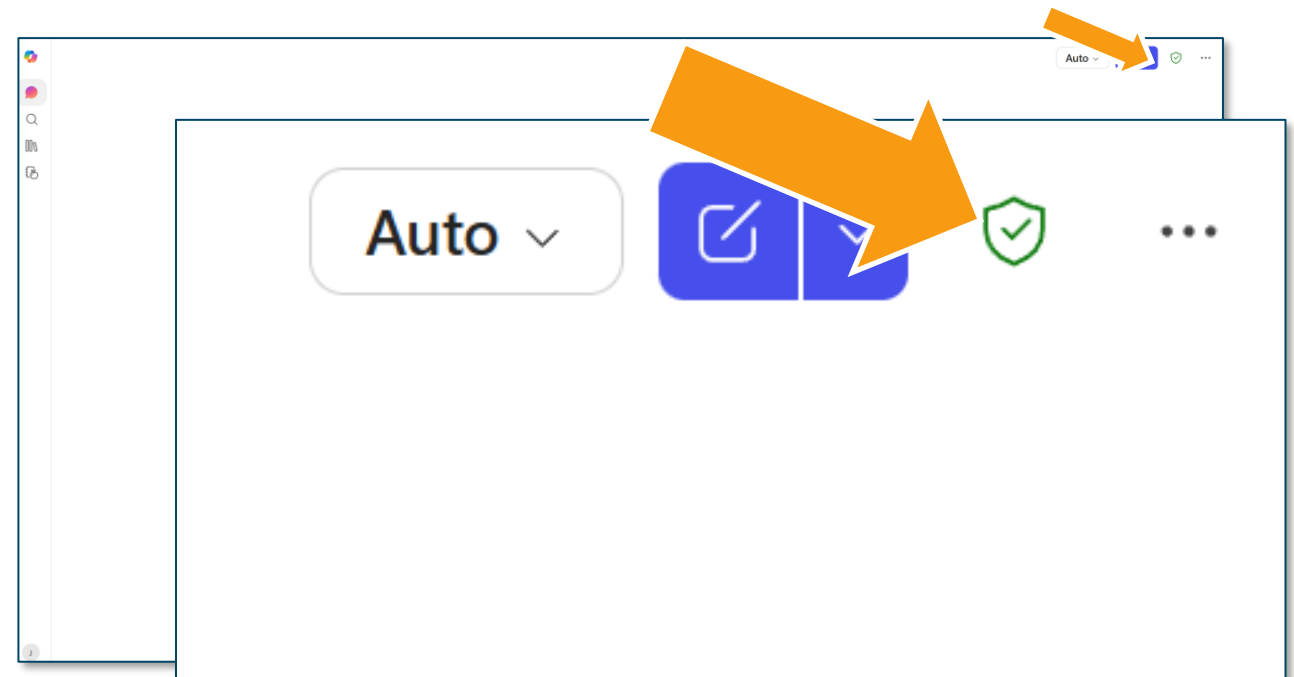
- Eigene Hochschul-Richtlinien/Compliances
- Für Forschung bspw. European Living Guidelines, ggf. DFG, BMFTR, andere Fördermittelgeber...

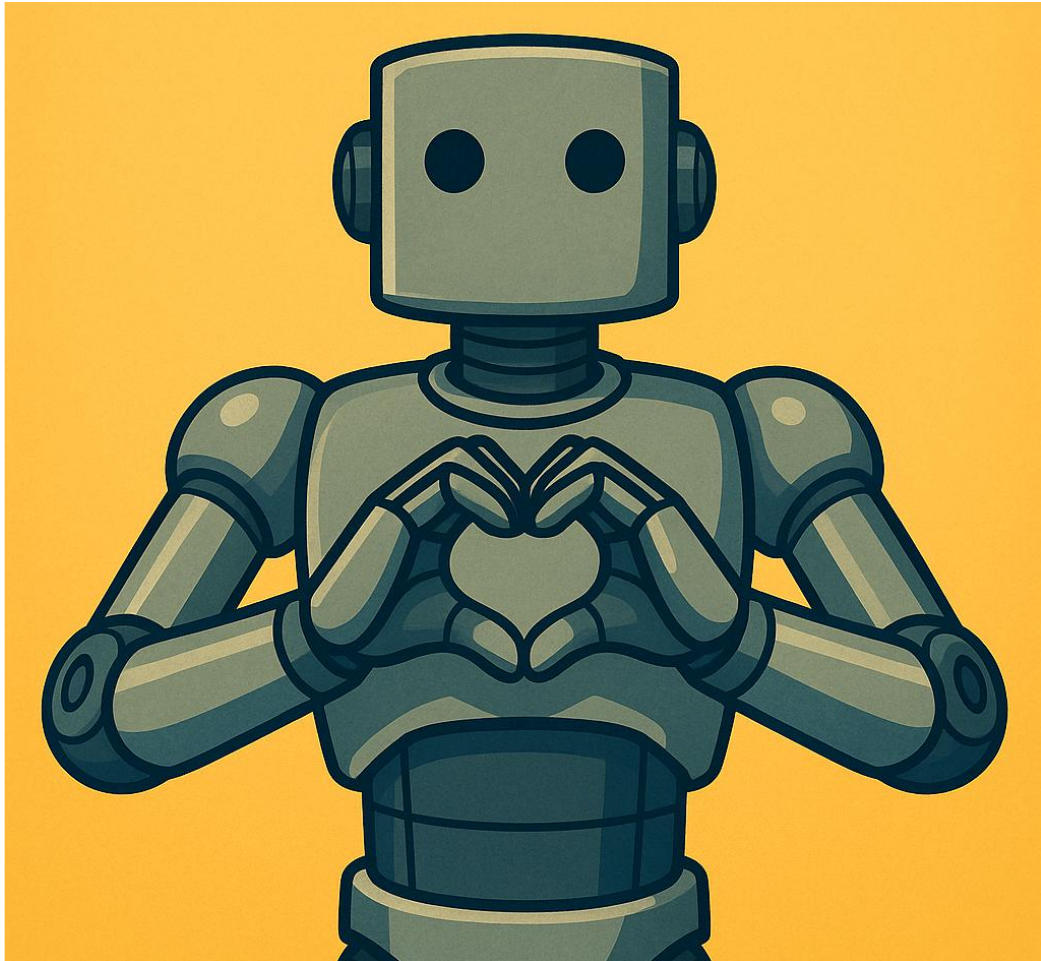
Inwiefern konkretisieren diese in ihren Vorgaben/Richtlinien die EU KI-VO arbeitspraktisch für MEINEN Arbeitsalltag?





OHM Richtlinie und Copilot-Datenschutz





**Vielen Dank, dass
Sie dabei waren!**

Johanna.scheel@lukasbischof.eu

LinkedIn: Johanna Scheel