CAIR4 Use Case: GPAI-Modelle

Steckbrief:

KI-fachlich:	Beschreibung
Typ	KI-System zum Vergleich von mehreren GPAI-Modellen
KI-Modell	drei parallele GPAI-Modelle für die gleiche Aufgabe
Interaktion	Prompt-basiert; Eingabe einer Frage wird von drei GPAI-Modellen unterschiedlich beantwortet; wichtig: Zeitpunkt des „Knowledge-Cutoff“ also der Zeitpunkt der letzten Trainingsdaten
Technik	Generative Sprachmodelle; Abfragen über einen gemeinsamen Controller mit der Funktion „handle_query“
Besonderheit	Auswahl der KI-Modelle direkt in der Use Case Oberfläch. Anzeige von Antwortdauer und Anzahl der Zeichen der Antwort.
Verwendung	Testumgebung zum Vergleich von verschiedenen GPAI-Modellen.

Rechtlich	Einordnung *
KI-System i.S.d. EU AI Act?	Ja, KI-System i.S.v. Art. 3 Nr. 1 EU AI Act; sogar KI-System mit allgemeinem Verwendungszweck Art. 3 Nr. 66 EU AI Act
GPAI-Modell involviert?	Ja, Integration mehrerer KI-Modelle mit allgemeinem Verwendungszweck i.S.v. Art. 3 Nr. 63 EU AI Act, mehrere zur parallelen Nutzung
Pflichten?	Der Kontext der Auswahl mehrerer GPAI-Modelle macht es offensichtlich, dass es eine Interaktion mit einer KI ist, daher grds. keine Kennzeichnung erforderlich, siehe Art. 50 (1) EU AI Act.
DSGVO relevant?	grds. nicht, aber es ist nicht auszuschließen, falls personenbezogene Daten für Testzwecke verwendet werden und ein Speichern z.B. von Sessions erfolgt.
Risikoklasse?	grds. mittlere Risikoklasse, aber offensichtlichkeit, s.o. bei Pflichten. Aber: Im Einzelfall auch hohe Risikoklasse möglich, z.B. im Kontext von Gesundheit oder Finanzbranche.
Open Source?	Sonderfall: 1. abhängig von den verwendeten KI-Modellen; 2. grds. möglich, da aufgrund Offensichtlichkeit nicht kennzeichnungspflichtig, siehe Art. 2 (12), Art. 50 (1) EU AI Act.

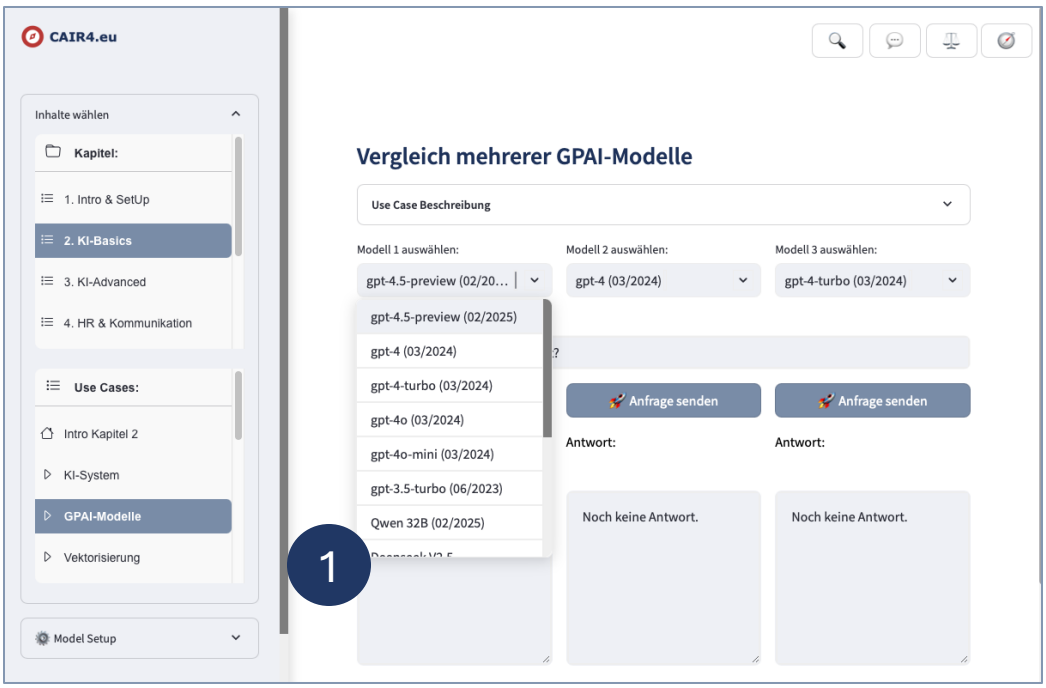
* Die Einordnungen sind exemplarisch. Entscheidend ist immer der Einzelfall.

Weitere Details wie der Quellcode können im CAIR4 Use Case Explorer und den Standard-Funktionen abgerufen werden.

CAIR4 Use Case: GPAI-Modelle

Beschreibung:

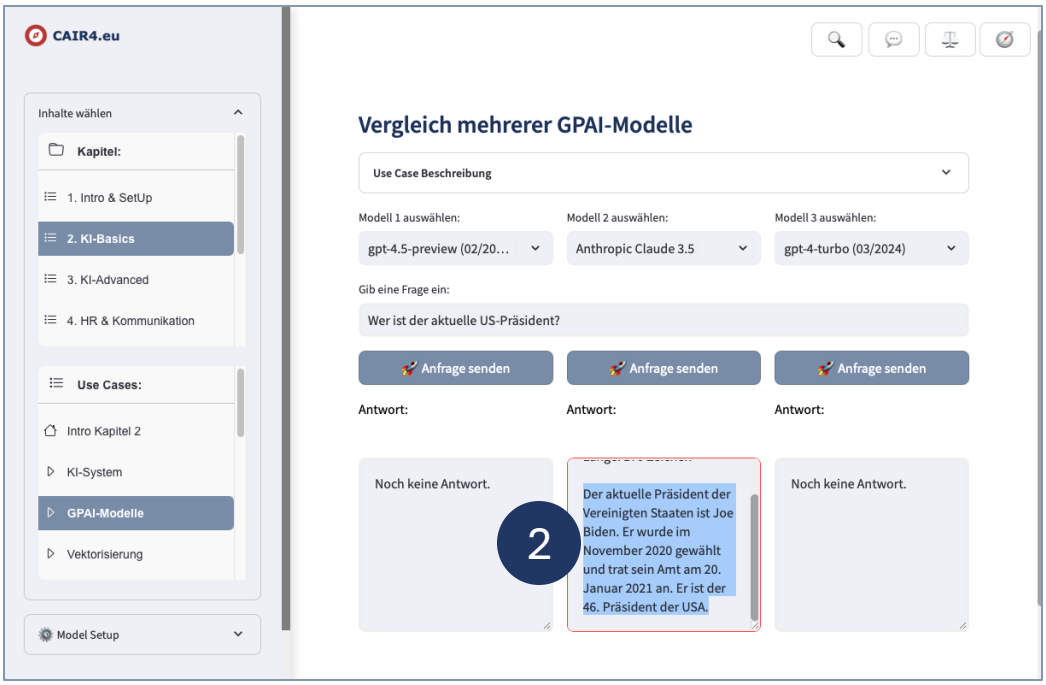
- Der CAIR4 Use Case „GPAI-Modelle“ ist ein KI-System mit allgemeinem Verwendungszweck im Sinne von Art. 3 Nr. 1, 66 EU AI Act, da gleich mehrere KI-Modelle mit allgemeinem Verwendungszweck im Sinne von Art. 3 Nr. 63 EU AI Act integriert sind (GPAI-Modelle) .
- Die Anbindung ist auf GPAI-Modelle beschränkt, die als Service via API verwendet werden können.
- Der Use Case ermöglicht einen Direktvergleich von KI-Modellen im Hinblick auf Antwort-Qualität, Antwort-Geschwindigkeit und Antwort-Umfang.
- Bild 1 zeigt, wie die zum Vergleich verwendeten GPAI-Modelle direkt im Use Case ausgewählt werden können.

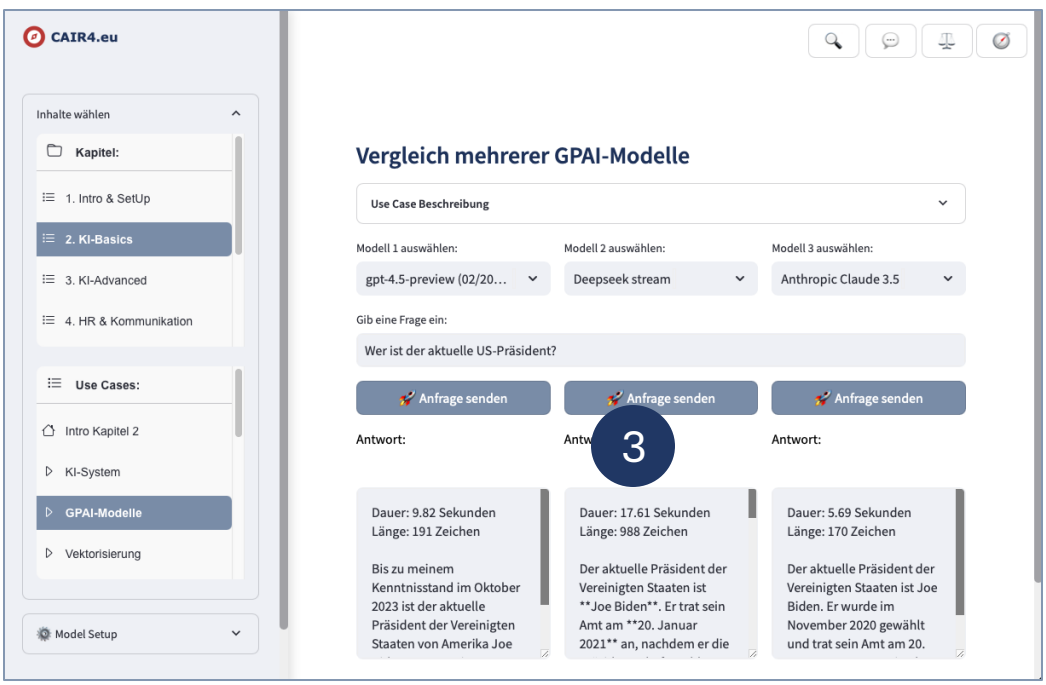


- Im Pulldown gut erkennbar: Das offizielle Datum des so genannten „Knowledge-Cut-Offs“. Im GPAI-Modell sind nach diesem Datum keine Trainings-Informationen mehr integriert worden. Neuere Daten kann das GPAI-Modell nicht wissen.
- Selbst Ereignisse, die vor dem Knowledge-Cut-Off geschehen sind, müssen nicht eintrainiert bzw. aktualisiert worden sein. Somit können Daten, die vor dem Cut-Off liegen, trotzdem fehlen, wenn sie nicht entsprechend aktualisiert wurden.

CAIR4 Use Case: GPAI-Modelle

- Bild 2 zeigt: Gibt man eine Frage ein, erscheint unter dem GPAI-Modell die Antwort. Neuere Informationen, wie die der US-Präsidentschaft, kann das Modell nicht geben.





- Bild 3 zeigt, wie stark Reaktionszeit, Länge und Qualität der Antworten voneinander abweichen können. Selbst das gleiche Modell gibt immer wieder andere Antworten. Dies ist ein wichtiges Kennzeichen für autonome, datenbasierte Entscheidungen.

Fachliche Begriffe:

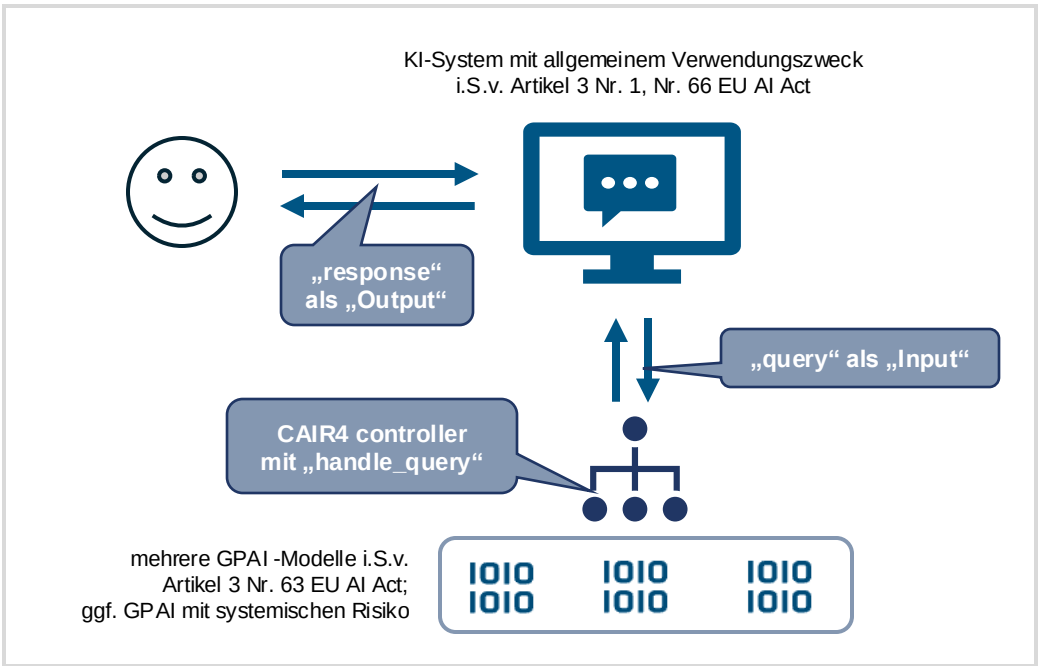
Der Blick in den Quellcode zeigt, dass die verschiedenen Modelle alle den gleichen Controller als „Weiche“ verwenden:

Beispiel: `from controllers.CAIR4_controller import handle_query`

Jede Prompt-Abfrage des „user“ wird im Sinne eines „guery“ versendet, die als „response“ des „assistant“ beantwortet wird:

Beispiel:
```
response, tokens_used, costs, references = handle_query(
query=user_input, use_case=use_case, context=context,
model_name=model_name, )
```

Die Grundstruktur von KI-System, GPAI-Modellen und Controller:



- Der EU AI Act besagt in Art. 3 Nr. 1, 66, dass ein KI-System, dass eines oder mehrere KI-Modelle mit allgemeinem Verwendungszweck integriert, als KI-System mit allgemeinem Verwendungszweck anzusehen ist.
- Im Hinblick auf die integrierten GPAI-Modelle ist unabhängig davon zwischen Modellen mit und ohne „systemische Risiken“ zu unterscheiden, Art. 3 Nr. 65 i.V.m Art. 55 EU AI Act. Diese unterliegen erhöhten Anforderungen.
- Es sind bei GPAI-Modellen daher nicht nur die Qualität und der Preis ein wichtiger Aspekt, sondern auch die mit den systemischen Risiken einhergehenden Auflagen, die ggf. auf den Anbieter des KI-Systems übergehen können.