

Modifikation von GPAI-Modellen und ihre Rechtsfolgen

Eine Fallstudie

Tim Schmetzer

Osborne Clarke

Herbstakademie 2025

Main Tasks Libraries Languages Licenses
Other

Tasks

- Text Generation
- Any-to-Any
- Image-Text-to-Text
- Image-to-Text
- Image-to-Image
- Text-to-Image
- Text-to-Video
- Text-to-Speech
- + 42

Parameters

< 1B 6B 12B 32B 128B > 500B

Libraries

- PyTorch TensorFlow JAX
- Transformers Diffusers Safetensors
- ONNX GGUF Transformers.js
- MLX MLX Keras + 41

Apps

- vLLM TGI llama.cpp MLX LM
- LM Studio Ollama Jan + 13

Inference Providers

- Cerebras Together AI Fireworks
- Nebius AI Novita Groq
- Hyperbolic Nscale + 6

Models 2,063,770

Full-text search Sort: Trending

- google/embeddinggemma-300m**
Sentence Similarity • 0.3B • Updated 5 days ago • 73.7k • 507
- tencent/HunyuanWorld-Voyager**
Image-to-Video • Updated 5 days ago • 4.66k • 522
- microsoft/VibeVoice-1.5B**
Text-to-Speech • 3B • Updated 8 days ago • 245k • 1.59k
- moonshotai/Kimi-K2-Instruct-0905**
Text Generation • Updated 4 days ago • 8.76k • 318
- swiss-ai/Apertus-8B-Instruct-2509**
Text Generation • 8B • Updated 4 days ago • 66.4k • 266
- openbmb/MiniCPM4.1-8B**
Text Generation • 8B • Updated 4 days ago • 412 • 253
- tencent/Hunyuan-MT-7B**
Translation • 8B • Updated 1 day ago • 6.56k • 580
- apple/FastVLM-0.5B**
Text Generation • 0.8B • Updated 6 days ago • 19.3k • 271
- Qwen/Qwen-Image-Edit**
Image-to-Image • Updated 15 days ago • 176k • 1.73k
- swiss-ai/Apertus-70B-Instruct-2509**
Text Generation • 71B • Updated 4 days ago • 38.1k • 123

<https://huggingface.co/models>

Anbieter (Art. 3 Nr. 3 KI-VO)



Eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle,



die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck **entwickelt** oder **entwickeln lässt**



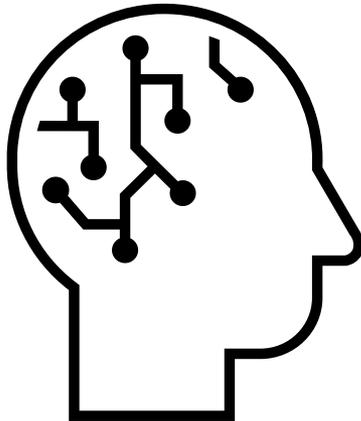
und es unter ihrem eigenen Namen oder ihrer Handelsmarke **in Verkehr bringt** oder

ODER

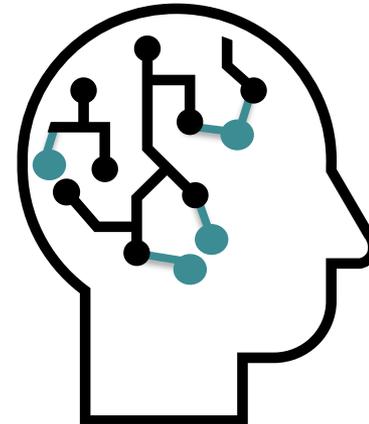


das **KI-System** unter ihrem eigenen Namen oder ihrer Handelsmarke **in Betrieb nimmt**, sei es entgeltlich oder unentgeltlich;

Anbieter von GPAI-Modellen: Entwickeln oder entwickeln lassen



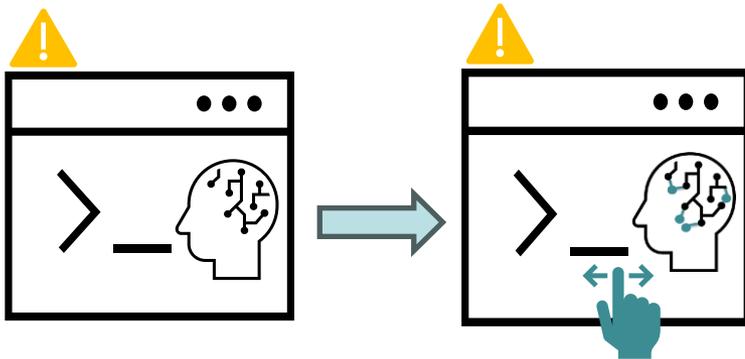
**Entwickeln (lassen)
von Grund auf**



**Modifikation (downstream)
von bereits in Verkehr
gebrachtem GPAI-Modell**

Signifikante Veränderung des GPAI-Modells

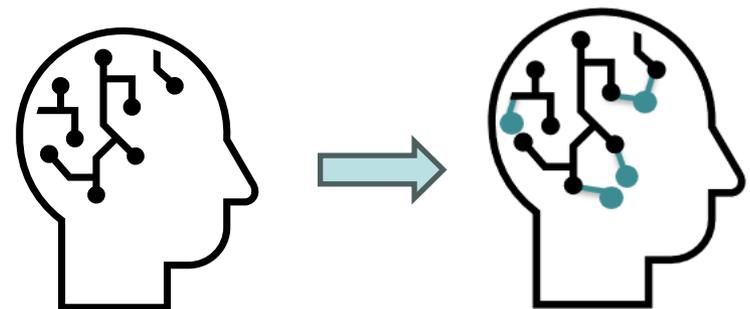
**Hochrisiko-KI-Systeme:
“Wesentliche Veränderung” (Art.
25 Abs. 1 lit. b KI-VO)**



Entwickeln (lassen)
von Grund auf

Anbieterfiktion bei
**wesentlicher
Veränderung** bereits
in Verkehr gebrachter
KI-Systeme (Art. 25
Abs. 1 lit. b KI-VO)

**GPAI-Modelle: Signifikante
Änderung (vgl. Rn. 62 GPAI-
Guideline)**

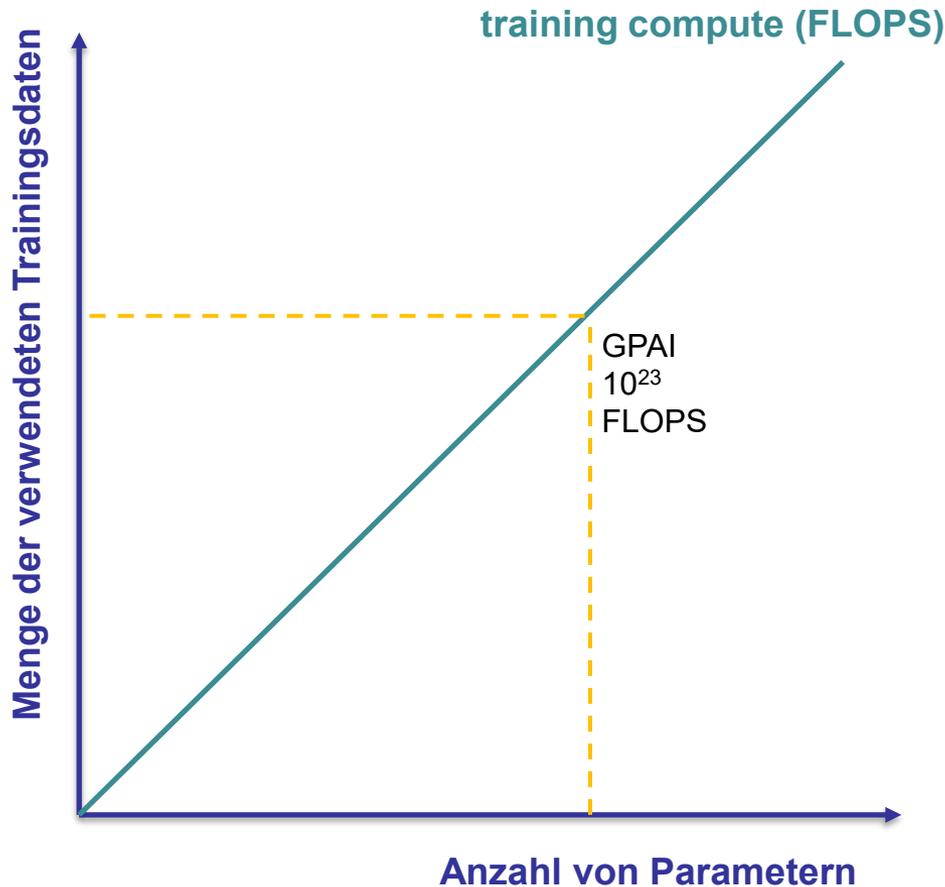


Downstream-
Modifikation als
“Entwickeln oder
entwickeln
lassen”?



NEU

GPAI-Guideline der Kommission: *Training Compute (1)*

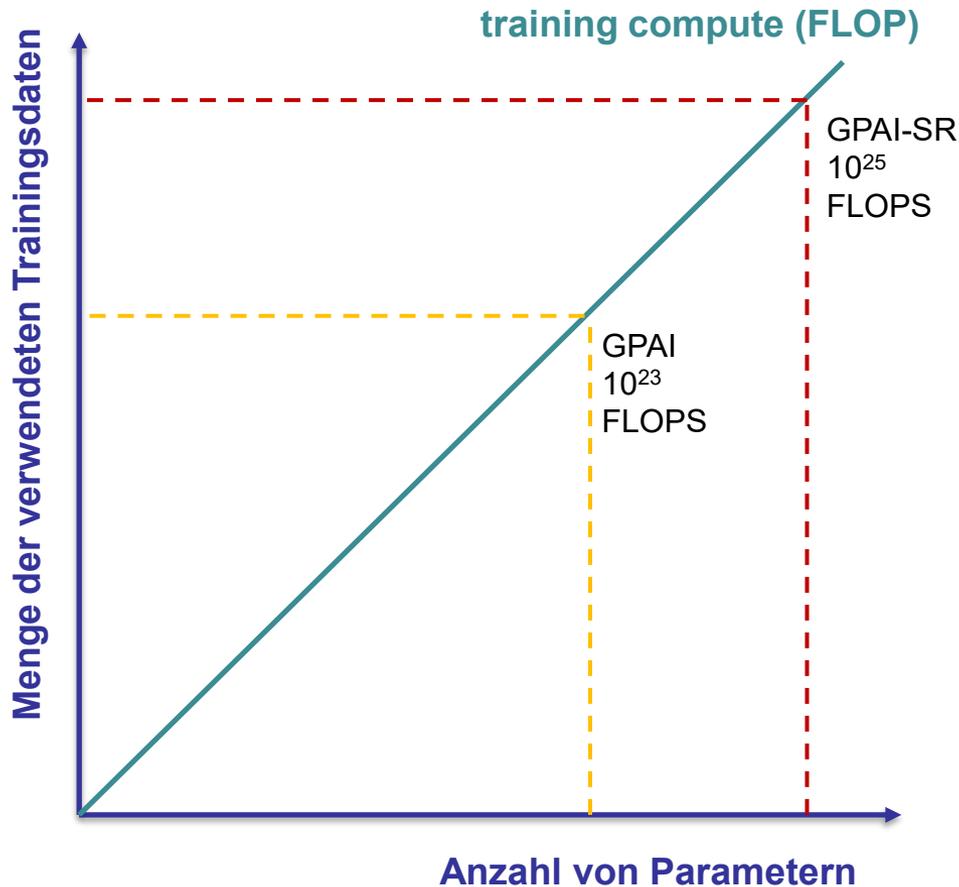


- Messbares Kriterium zur Einordnung als **GPAI-Modell**: *training compute* in *Floating point operations per second (FLOPS)*
- Widerlegliche Vermutung, dass ein KI-Modell ein GPAI-Modell ist, wenn es:
 1. Sprache (Text oder Audio), Text-to-image oder Text-to-Video generieren kann

UND

 2. Mit mehr als 10^{23} FLOPS trainiert wurde

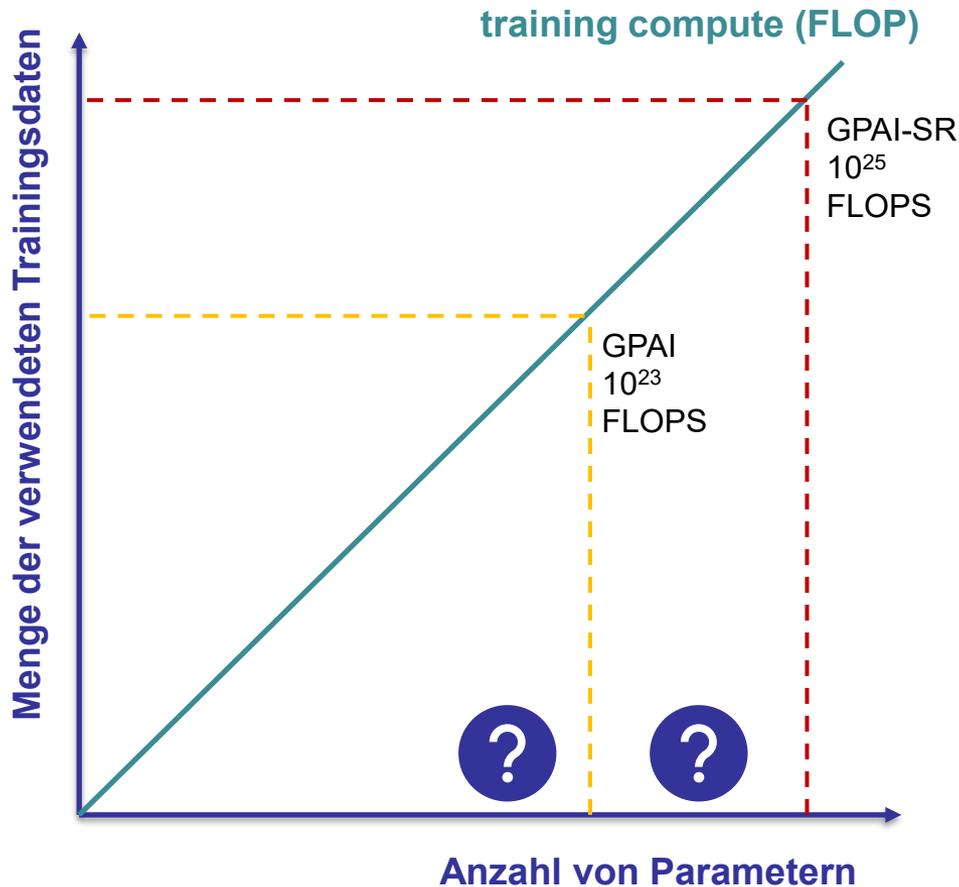
GPAI-Guideline der Kommission: *Training Compute* (2)



- Widerlegliche Vermutung, dass ein GPAI-Modell ein **GPAI-SR-Modell** ist, wenn es: mit mehr als 10^{25} FLOPS trainiert wurde (Art. 51 Abs. 2 KI-VO)

NEU

GPAI-Guideline der Kommission: *Training Compute* (3)



Signifikante Änderung durch Downstream-Modifier

- Grundsatz: 1/3 der tatsächlich aufgewendeten Rechenkapazität zum Training des originalen Modells (widerlegliche Vermutung)
- **Falls nicht ermittelbar:**
 - 10^{23} FLOPS für GPAI-Modelle
 - 10^{25} FLOPS für GPAI-SR-Modelle



Prüfungsschema: Entwickeln oder entwickeln lassen

1. Liegt eine signifikante Änderung vor?

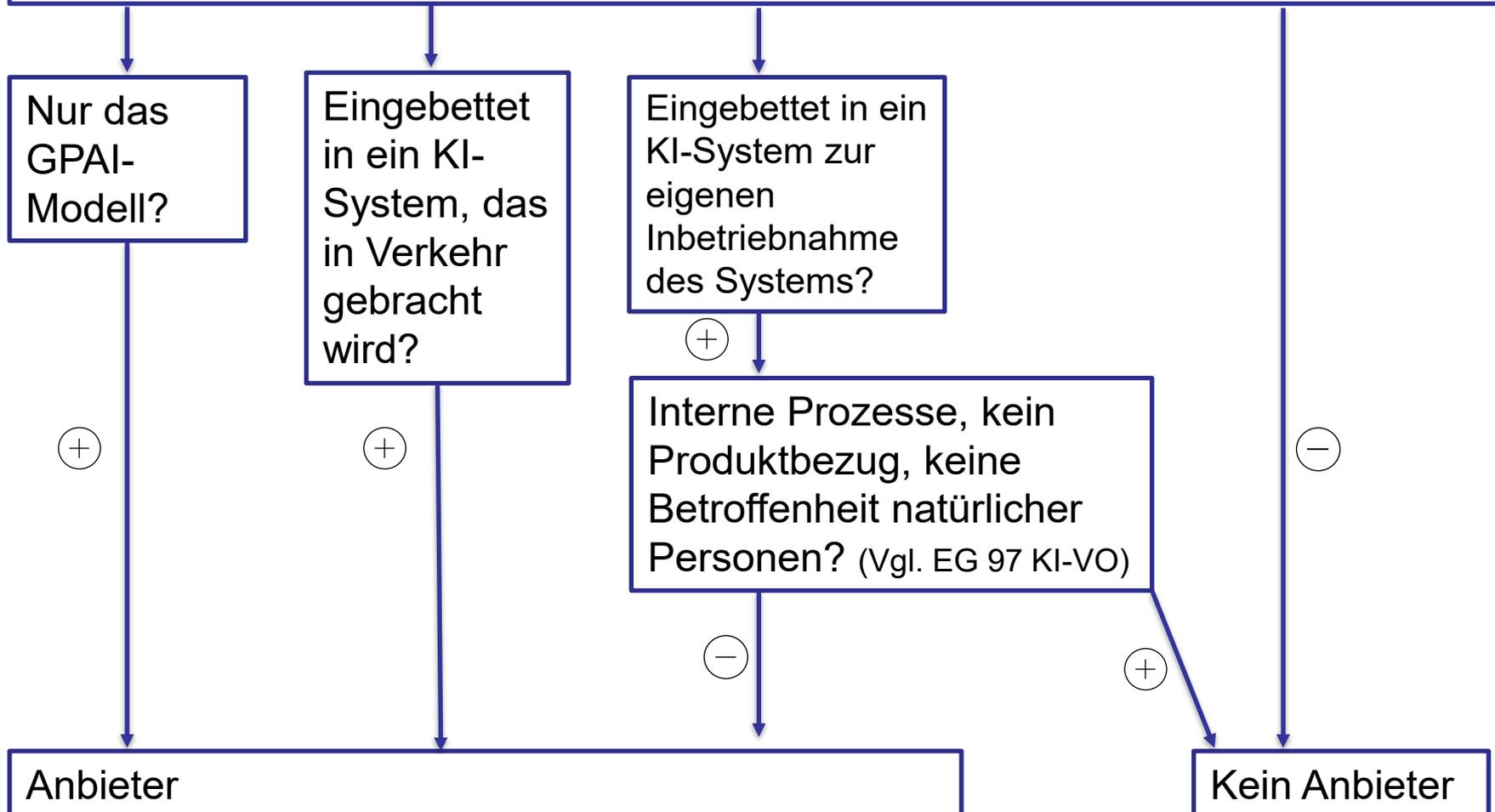


2. Weist das modifizierte Modell weiterhin einen allgemeinen Verwendungszweck i.S.d. Art. 3 Nr. 63 KI-VO auf?



3. Wird das Modell in Verkehr gebracht i.S.v. Art. 3 Nr. 9 KI-VO?

Wird das Modell in den Verkehr gebracht i.S.v. Art. 3 Nr. 9 KI-VO?

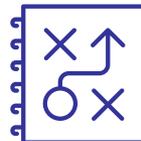
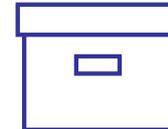


Fallgruppen



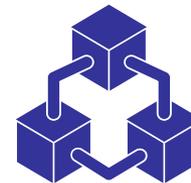
Integration eines nicht
modifizierten GPT-
Modells in ein KI-
System

Veränderung von
Datenquellen

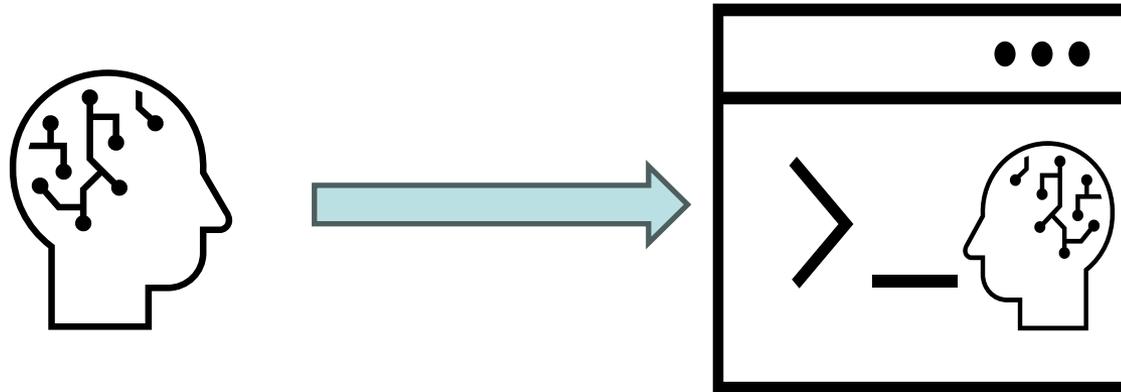


Fine-Tuning

Model Merging und
Model Fusion

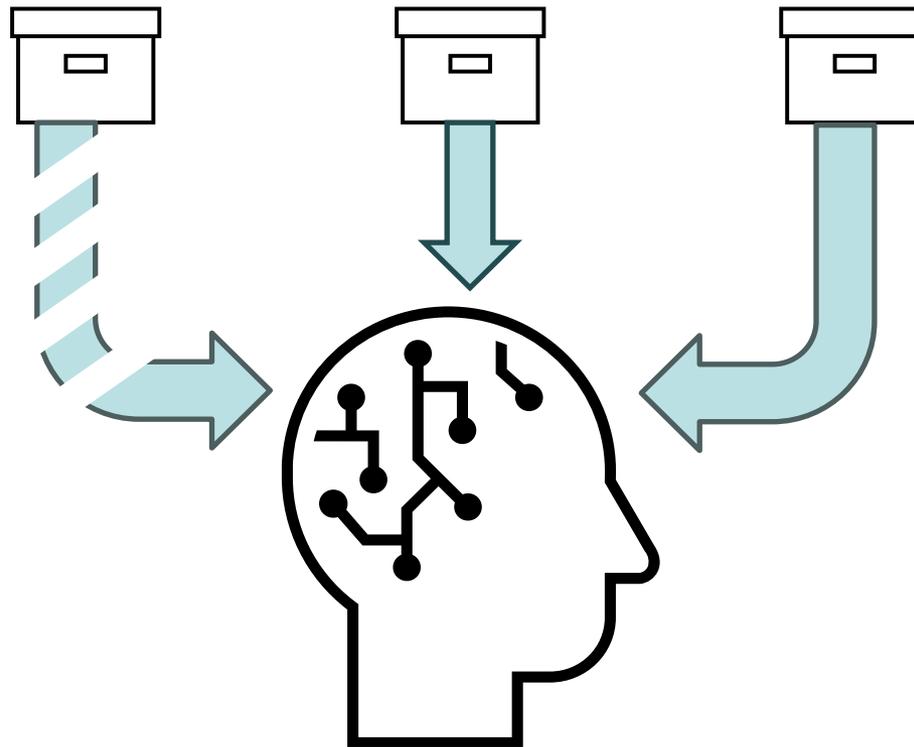


1. Integration eines nicht modifizierten GPAI-Modells in ein KI-System

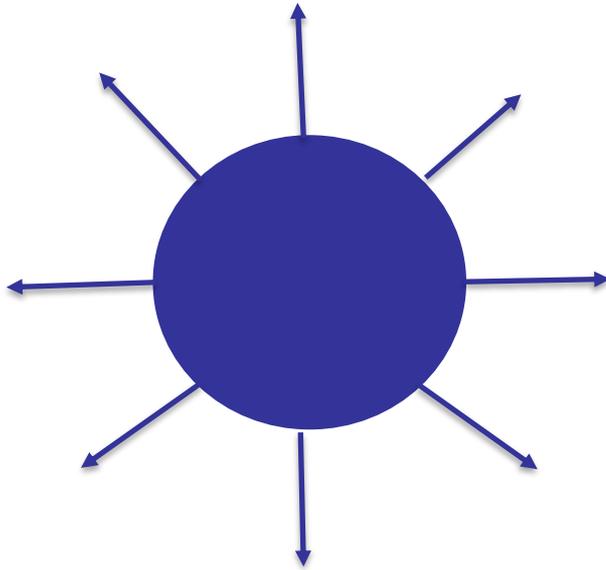


- Grds. **keine Anbieterrolle des Downstream-Modifiers**
- Aus ErwG 97 KI-VO folgt nichts anderes
 - Durch Auslegungsgrundsatz in ErwG 97 soll nur Schutzlücke in der KI-Wertschöpfungskette geschlossen werden (kein im Verkehr befindliches GPAI-Modell ohne Anbieter)
 - Vorliegend bleibt der ursprüngliche GPAI-Anbieter weiterhin Anbieter (dasselbe GPAI-Modell) → keine Schutzlücke in der KI-Wertschöpfungskette

2. Veränderung von Datenquellen

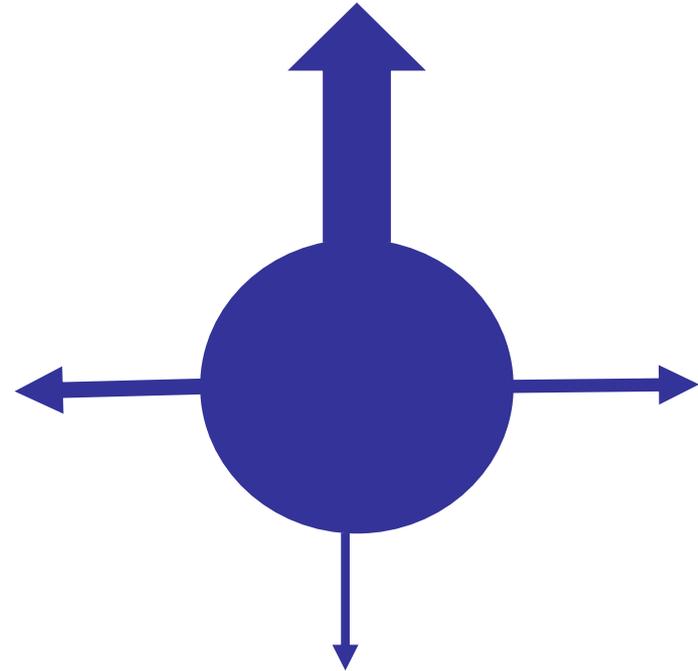


3. Fine-Tuning



Ursprüngliches GPTAI-Modell

Training für allgemeine Aufgaben



GPTAI-Modell mit Fine-Tuning

Training für spezifische Aufgaben

3. Fine-Tuning

Bsp. Originales Modell wurde mit 10^{24} FLOPS trainiert

1. Fine-Tuning

$1,26 \times 10^{23}$ FLOPS

$< 1/3 * 10^{24}$
FLOPS

2. Fine-Tuning

$1,1025 * 10^{23}$
FLOPS

+ $1,26 \times 10^{23}$
FLOPS

= $2,3625 * 10^{23}$
FLOPS

$< 1/3 * 10^{24}$ FLOPS

3. Fine-Tuning

$1,155 * 10^{23}$ FLOP

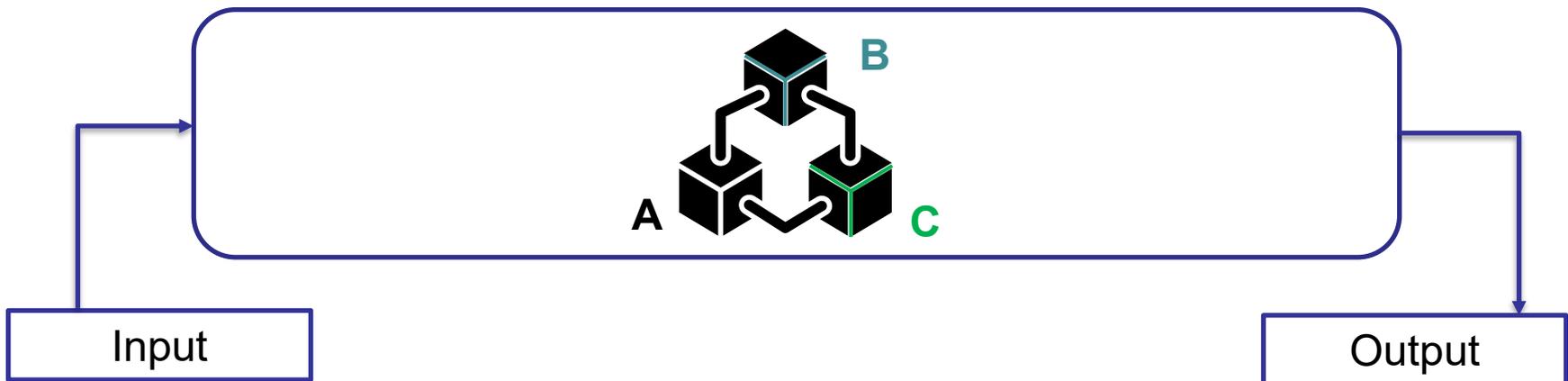
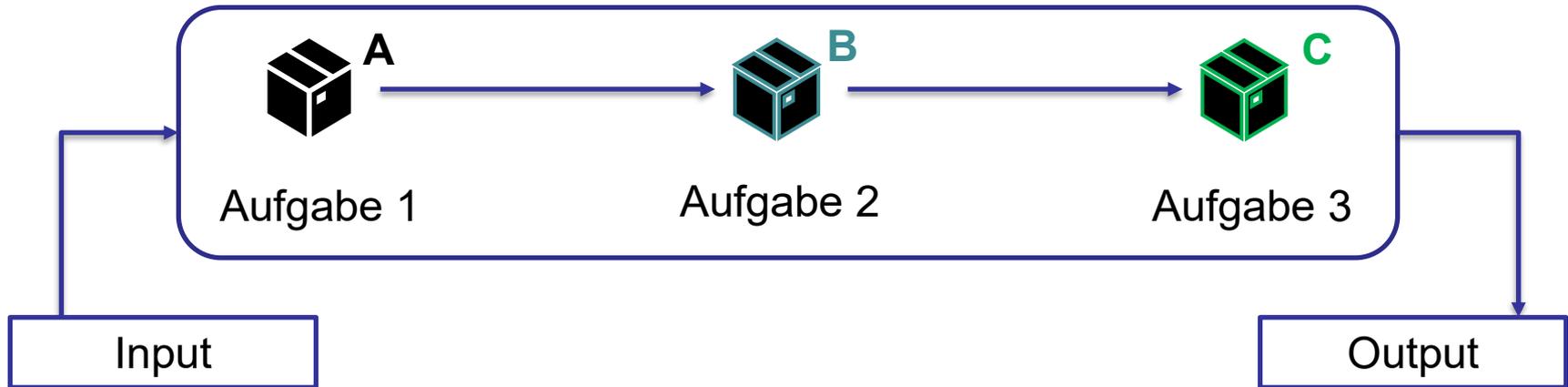
+ $2,3625 * 10^{23}$
FLOP

= $3,5175 * 10^{23}$
FLOP

$> 1/3 * 10^{24}$
FLOPS

$1/3 * 10^{24} = 3, \bar{3} * 10^{23}$

4. Model Merging und Model Fusion

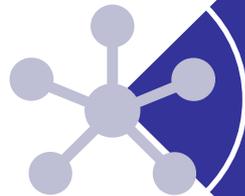


Fazit und Ausblick

Kritik am Kriterium *training compute*



Zweifelhafter langfristiger Bestand
des Kriteriums



Zusammenhang zwischen der zum
Training verwendeten
Rechenleistung und den Fähigkeiten
des KI-Modells zweifelhaft



Nur zur Bewertung von
(unsupervised) Fine-Tuning geeignet

Questions & Answers

