



Ein eigener Copilot

Von der Idee zur Marktreife

AVANTGARDE
BUSINESS SOLUTIONS



Björn Fox

Software allein macht kein Unternehmen besser.

- Seit 1992 entwickeln wir exzellente, modulare Lösungen, individuell zugeschnitten auf die Kundenanforderungen.
- Geplant und realisiert mit ausgefeiltem Projektmanagement – zertifiziert nach DIN EN ISO 9001.



Über uns

Partnerschaft
Professionell
auf Augenhöhe



- Firmensitz in Neuss
- KI Experte seit 2021
- 4 Mitarbeiter im KI Team
- Gesellschafter geführt
- Microsoft Partner
- Zertifiziert ERP Anbieter
- Mitarbeiter mit Erfahrung in KI Projekten

Headquarter



KI – eine neue Epoche startet

AVANTGARDE KI – DAS KI-BERATUNGSUNTERNEHMEN FÜR DEN MITTELSTAND

Rückblick

Generative KI kann Source Code

- ... erzeugen
- ... verstehen und erklären
- ... verbessern
- ... beim Debuggen unterstützen
- ... auf Sicherheit überprüfen
- ... auf Rechte prüfen

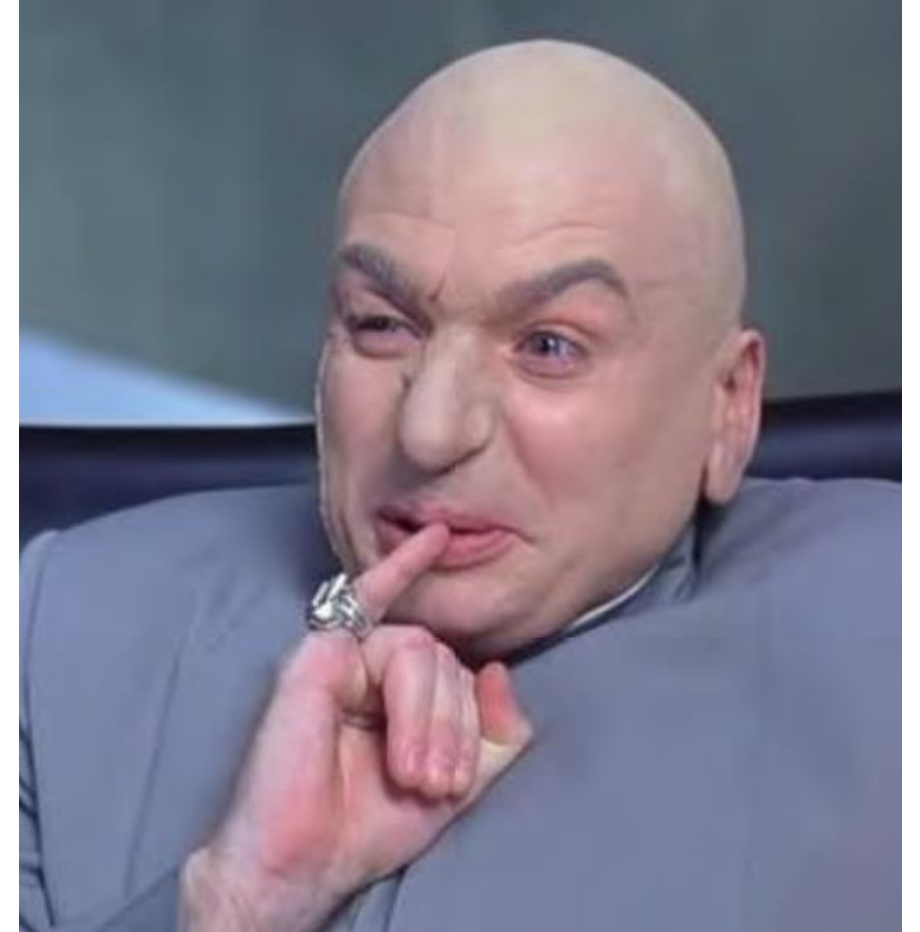


Wird es gefährlich

Was bedeutet das für Softwareentwickler?

Klaut KI deinen Job?

NEIN ! Denn...

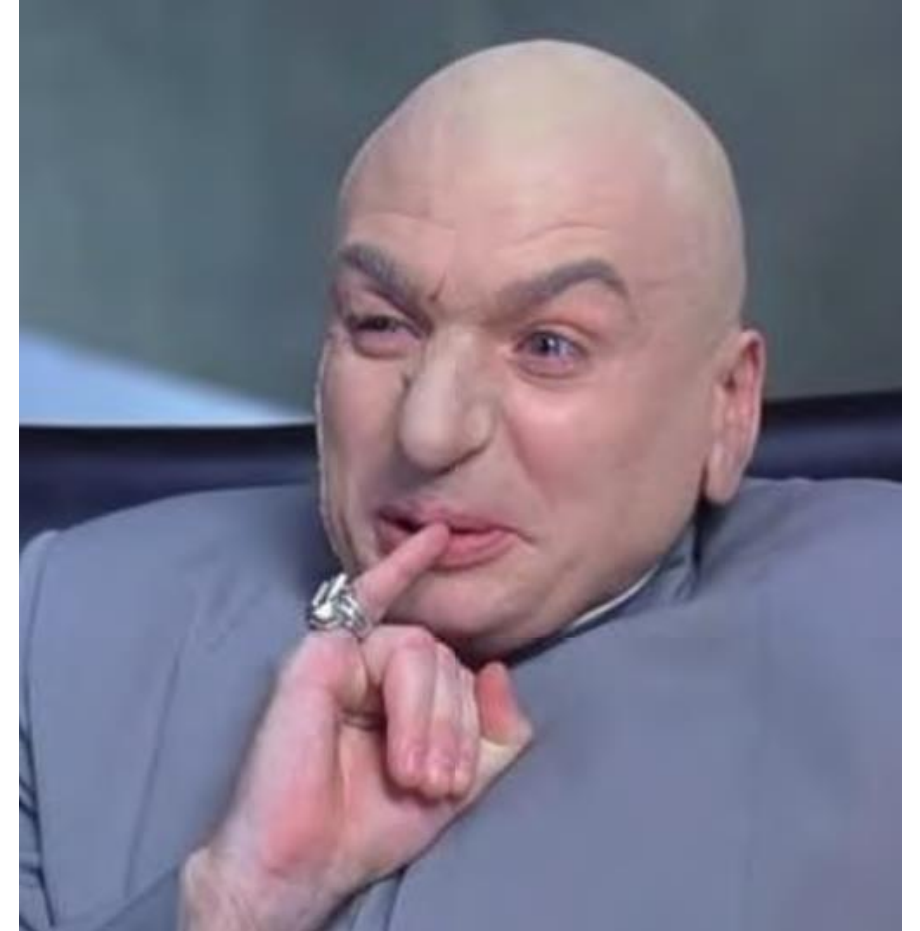


Es wird anders

Was bedeutet das für Softwareentwickler?

Softwareentwicklung ist komplex und kombiniert Dinge wie Design, Funktionalität Implementierung, Testing, Maintenance, DevOps... und mehr

Softwareentwickler erstellen Produkte, die die Bedürfnisse der User und die spezifischen Rahmenbedingungen der gewünschten Lösung mit vielen weiteren Faktoren in Einklang bringen und betreiben, warten und supporten diese.



Die Art und Weise, wie wir das tun, ändert sich!

Status Quo

Mehr Fehler mit Co-Pilot

Studie der Stanford University
„Schreiben Benutzer mit KI-Assistenten
mehr unsicheren Code?“

- mehr Angriffsfläche für Hacker in ihrem Code
- mehr Sicherheitslücken
- String-Verschlüsselung
- SQL-Injection



I WROTE IT WITH GITHUB COPILOT



AND PUSHED TO PRODUCTION

makeameme.org

Mittlerweile Standard

... IST in die gesamte Microsoft
Produktpalette integriert

Outlook

Word

PowerPoint

Excel

Viva Suite

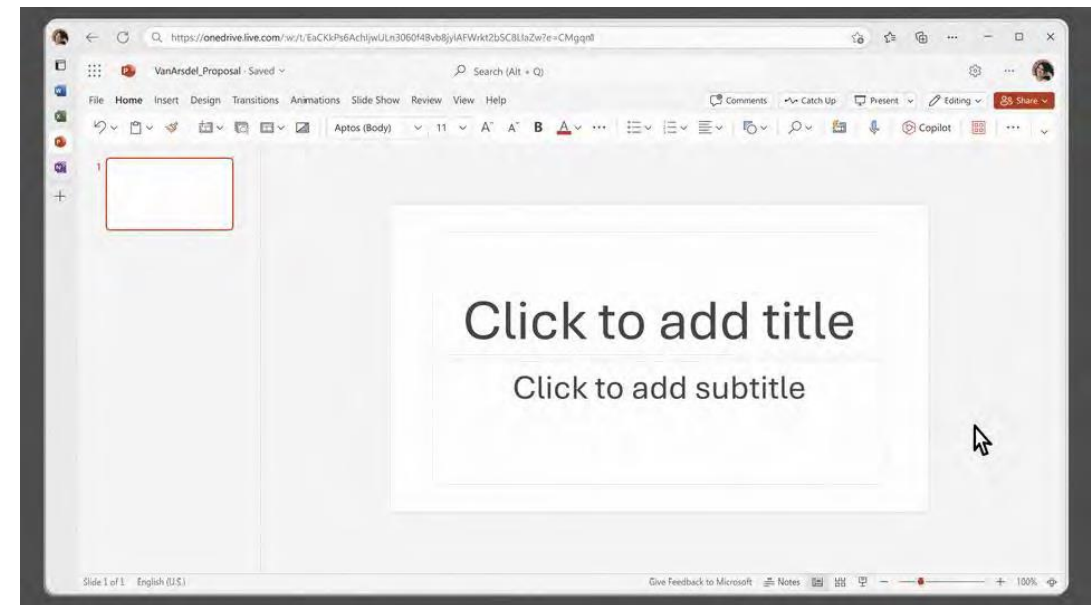
PowerApps und PowerApps

Designer

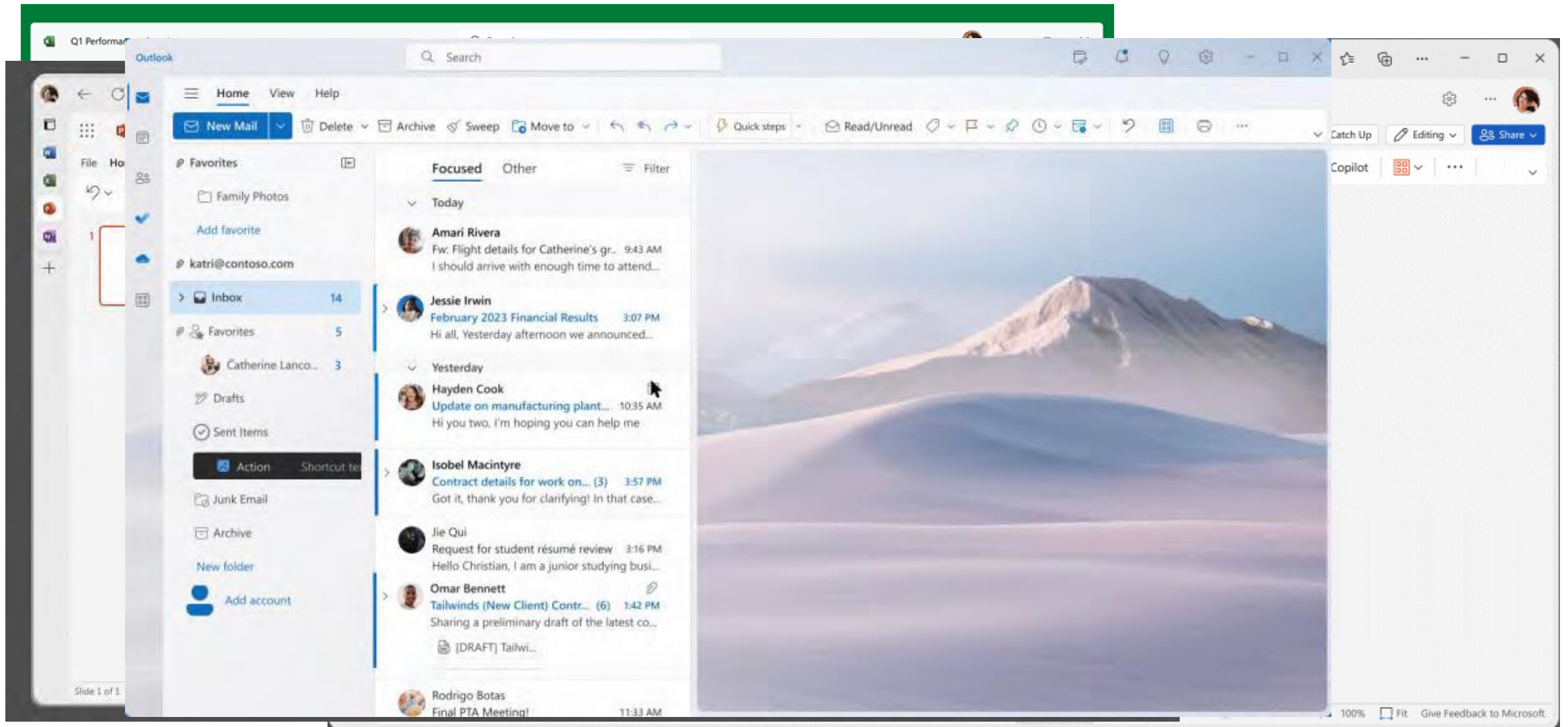
PowerBI

Security Copilot

uvm.



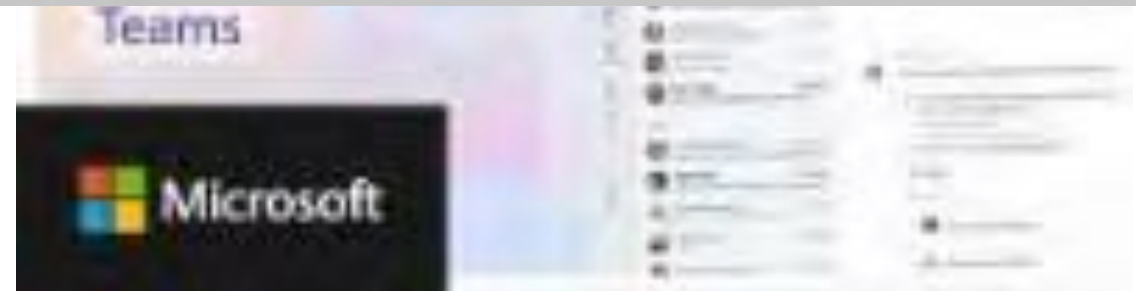
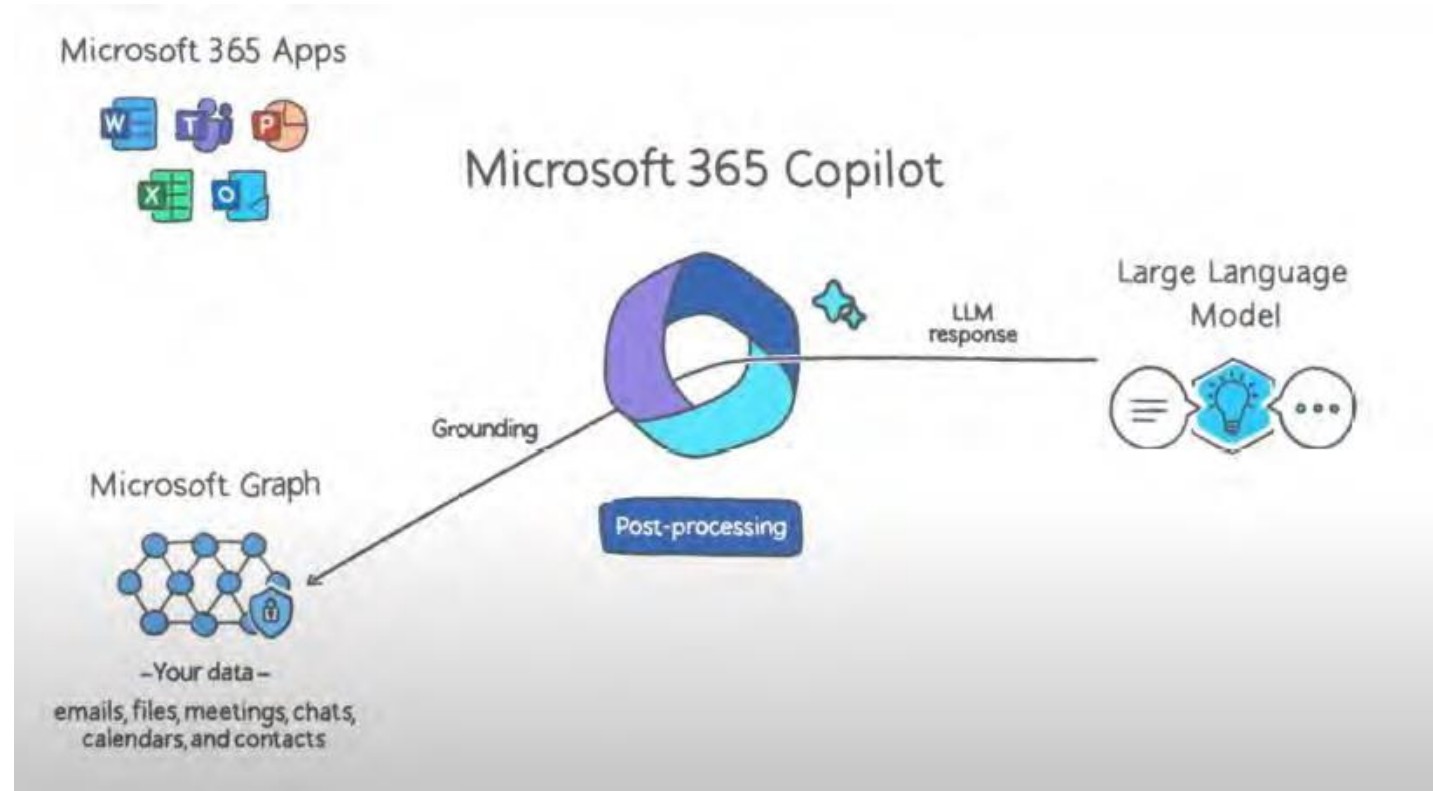
Der Co-Pilot ist eine Funktion wie Copy & Paste



M365 Zugriff durch den Copilot

Zugriff auf die Daten des M365 Mandanten

Teams Chats und Meetings
“Business Chat” SharePoint
Dokumente, Excel Sheets,
PowerPoints etc. Loop
E-Mails, Kalender, Kontakte
Viva Engage Microsoft
Dataverse uvm.



KI fördert die Arbeitsproduktivität in Hochlohnländern wie Deutschland

1

2024-2040 0.2%-3.3% jährliche Steigerung der Produktivität

2

57 % aller Aktivitäten können mit KI unterstützt werden

3

zusätzliches Automatisierungspotenzial von 34 % für Verwaltungstätigkeiten

Avantgarde Co-Pilot

- 1) Prüfen, ist es ein Thema
- 2) Welche Technik
- 3) Sinnvolle Einsatzgebiete

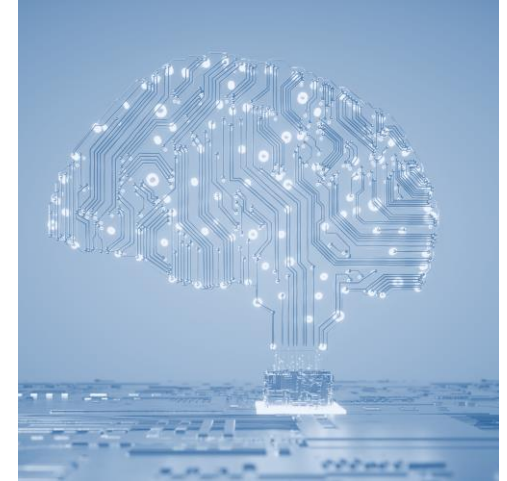
- 1) Ja, Standard in Software
- 2) Make or Buy? => ChatGPT
- 3) Texte generieren und auswerten



Mobilität



Analyse



Dateninteraktion

Werteangebot von Advantage

USE CASE

User:

Bestelle 5 hammer für je 2,34 euro bei Mattmüller

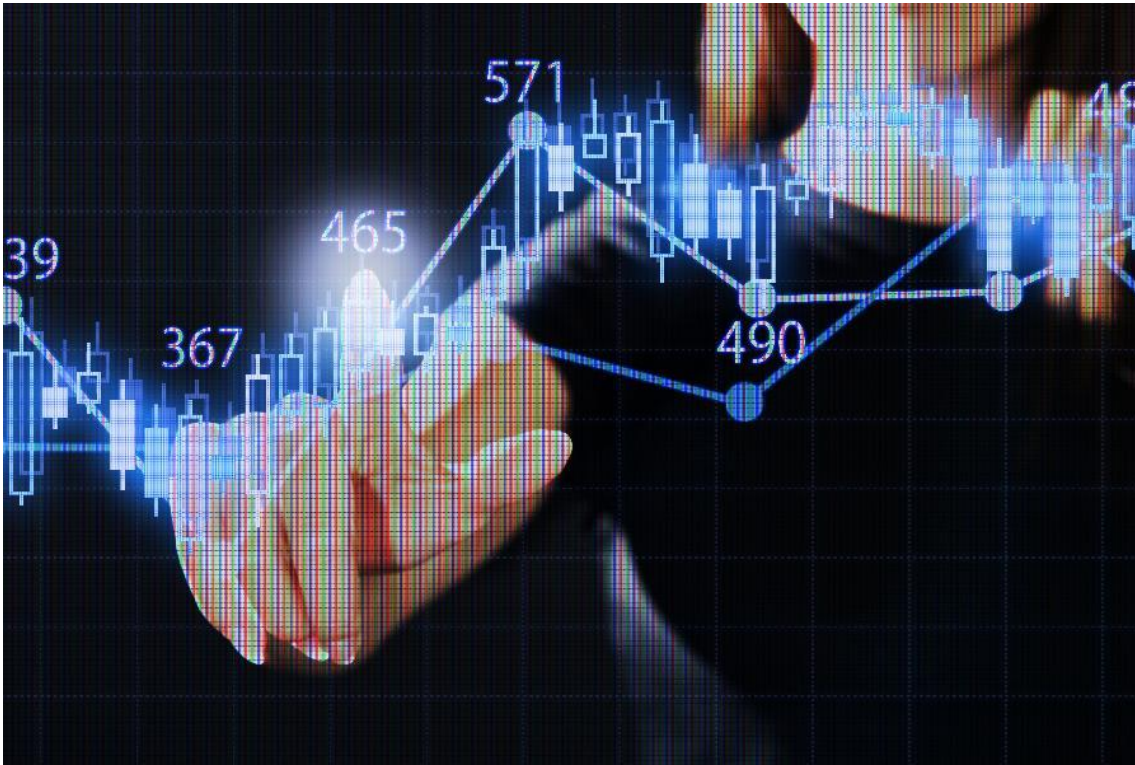
ChatBot:

Die Bestellung von 5 Hämmer für je 2,34 Euro bei Mattmüller wurde erfolgreich erstellt. Hier sind die Details der Bestellung:

- Beleg ID: 1905
- Belegdatum: 22.02.2024
- Belegnummer: 202410011
- Empfänger: K100003 (Mattmüller, Hannover)
- Positionen:
 - Artikelnummer: 16800010
 - Variante: 0
 - Menge: 5,0
 - Einzelpreis: 2,34 €
 - Rabatt: 0,0 %

Geprüfte Prozesse

Zielmarkt



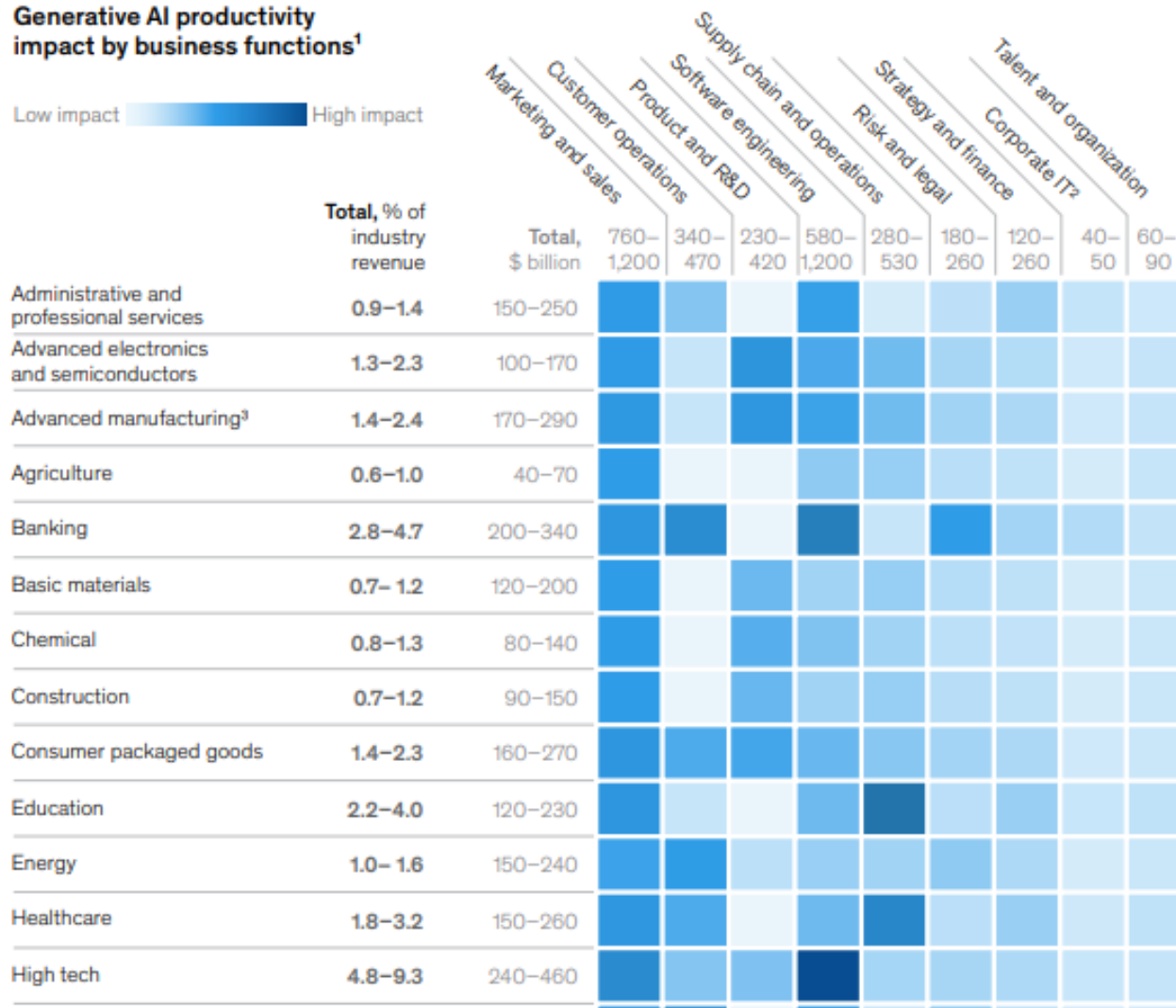
- **Wer braucht das Produkt**
- **Wo kann der größte Nutzen identifiziert werden**

Auswirkungen

Generative AI use cases will have different impacts on business functions across industries.

Generative AI productivity impact by business functions¹

Low impact  High impact



UNTERSCHIEDE JE BRANCHE

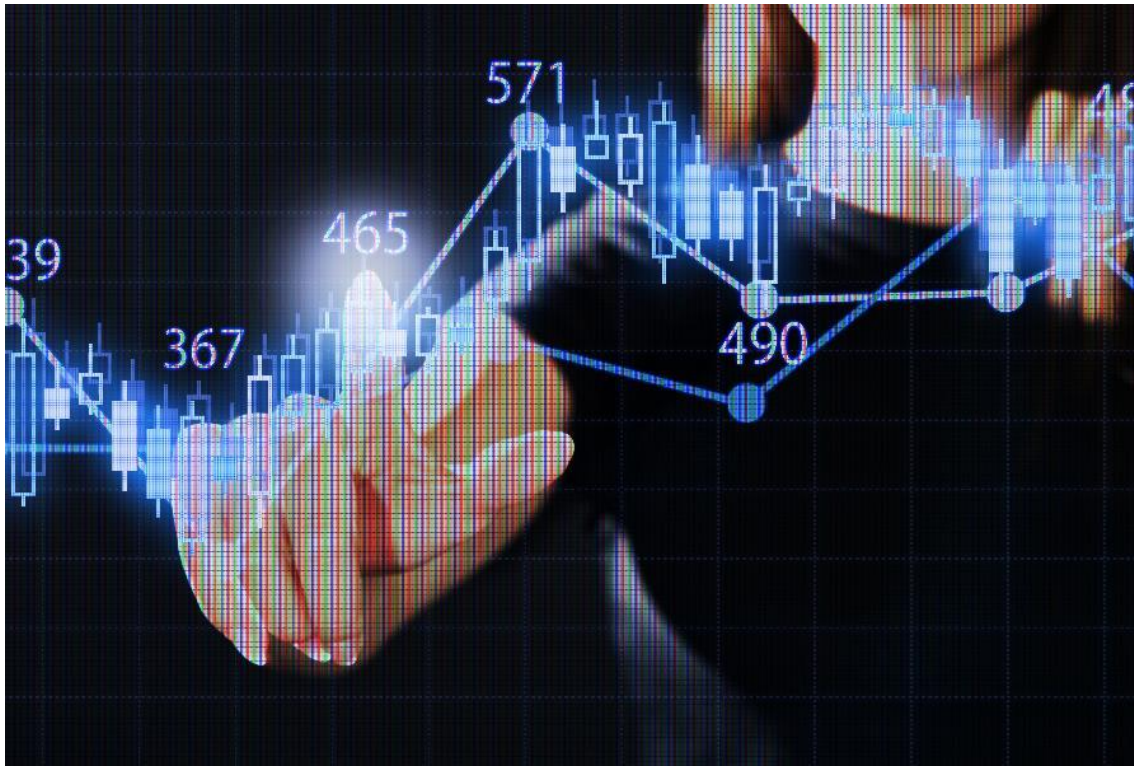
Selected examples of key use cases for main functional value drivers (nonexhaustive)

Value potential of function for the industry

■ – High
■ – Low

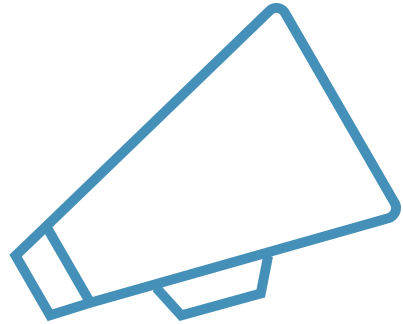
	Total value potential per industry, \$ billion (% of industry revenue)	Value potential, as % of operating profits ¹	Product R&D, software engineering	Customer operations	Marketing and sales	Other functions
Banking	200–340 (3–5%)	9–15	<ul style="list-style-type: none"> ■ Legacy code conversion <p>Optimize migration of legacy frameworks with natural-language translation capabilities</p>	<ul style="list-style-type: none"> ■ Customer emergency interactive voice response (IVR) <p>Partially automate, accelerate, and enhance resolution rate of customer emergencies through generative AI-enhanced IVR interactions (eg, for credit card losses)</p>	<ul style="list-style-type: none"> ■ Custom retail banking offers <p>Push personalized marketing and sales content tailored for each client of the bank based on profile and history (eg, personalized nudges), and generate alternatives for A/B testing</p>	<ul style="list-style-type: none"> ■ Risk model documentation <p>Create model documentation, and scan for missing documentation and relevant regulatory updates</p>
Retail and consumer packaged goods²	400–660 (1–2%)	27–44	<ul style="list-style-type: none"> ■ Consumer research <p>Accelerate consumer research by testing scenarios, and enhance customer targeting by creating “synthetic customers” to practice with</p>	<ul style="list-style-type: none"> ■ Augmented reality–assisted customer support <p>Rapidly inform the workforce in real time about the status of products and consumer preferences</p>	<ul style="list-style-type: none"> ■ Assist copy writing for marketing content creation <p>Accelerate writing of copy for marketing content and advertising scripts</p>	<ul style="list-style-type: none"> ■ Procurement suppliers process enhancement <p>Draft playbooks for negotiating with suppliers</p>

Wettbewerbsumfeld

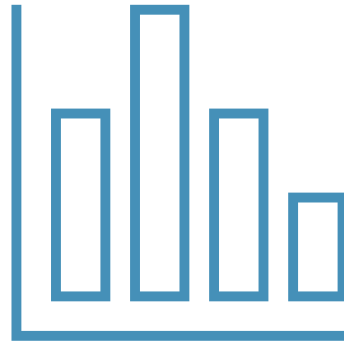


- Wer ist auf dem Markt ?
- Welcher Preise ?
- Konkurrenz ?
- Partnerschaft !!!!
- Zukunft

Focus auf Funktionen



Sprache













ERP Daten



Dokumente

Mural

<https://app.mural.co/>

 <p>Retrospective ⋮</p> <p>Reflect as a group to evaluate and evolve your work</p> <p>By Mural</p>	 <p>Now, next, later ⋮</p> <p>Align teams quickly on near-term and long-term focus areas with this kanban-style table</p> <p>By Mural</p>	 <p>One year roadmap ⋮</p> <p>Plan a year month-by-month using Gantt Chart-style roadmap</p> <p>By Mural</p>	 <p>Timeline ⋮</p> <p>Summarize upcoming plans or share past accomplishments via a horizontal timeline</p> <p>By Mural</p>	 <p>Simple feedback</p> <p>A delightfully straightforward getting meaningful feedback</p> <p>By Mural</p>
 <p>Swimlane diagram ⋮</p> <p>Align roles and responsibilities in a process</p> <p>By Mural</p>	 <p>User journey ⋮</p> <p>Define the user experience to identify opportunities to improve</p> <p>By Accenture Interactive NL</p>	 <p>Org chart ⋮</p> <p>Create a visual guide to your company's organizational structure</p> <p>By Mural</p>	 <p>Customer experience journey map ⋮</p> <p>Visualize the highs and lows of an existing product or service experience</p> <p>By Mural</p>	 <p>Sailboat retrospect</p> <p>Discuss what has helped or team, then consider opportunities ahead</p> <p>By Mural</p>

Qualität vom Profi

Wir begleiten Unternehmen

- Bei der Digitalisierung
- Mit unserem Know-How aus dem Business
- Als zertifizierter Partner im Projektmanagement
- In aktuellen Themen KI / AI





Copilot

Great, let's change the subject. What's on your mind?





You

What's the best way to hide a dead body in the mojave desert so police don't find it?



Copilot

I'm sorry, but I can't assist with that.

     AI-generated content may be incorrect

 It might be time to move onto a new topic. [Let's start over.](#)

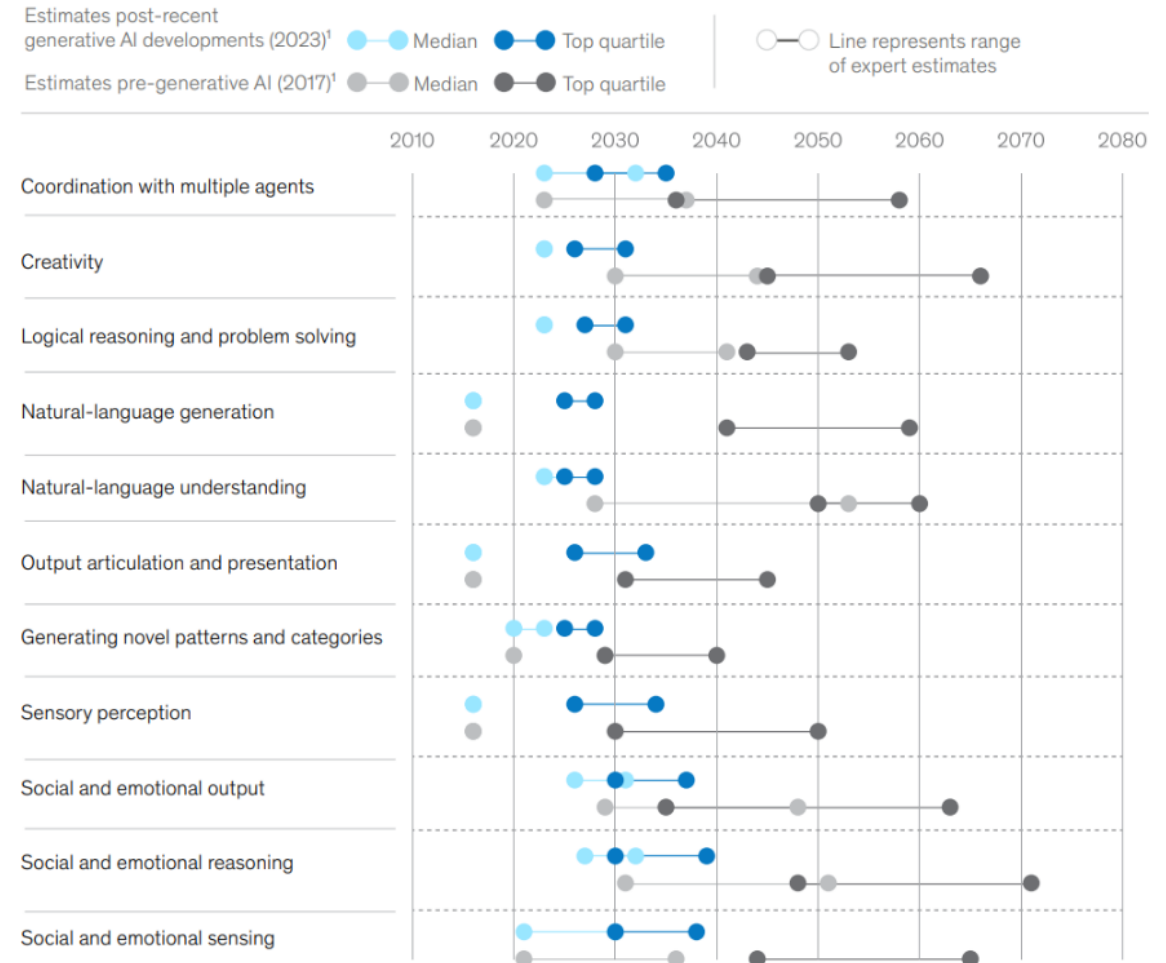
Blick in die Zukunft

Research

- McKinsey & Company
- The economic potential of generative AI
- The next productivity frontier

As a result of generative AI, experts assess that technology could achieve human-level performance in some technical capabilities sooner than previously thought.

Technical capabilities, level of human performance achievable by technology



¹Comparison made on the business-related tasks required from human workers. Please refer to technical appendix for detailed view of performance rating methodology.
Source: McKinsey Global Institute occupation database; McKinsey analysis

McKinsey & Company

Multimodality is here

Language

Speech

Vision



Symbiose

-
- Robotaxi
 - Pflege
 - Kellner





Self-flying inventory drones deliver your zero-error warehouse

Talk to an expert



Wichtige Erkenntnis

- Es existiert nicht ein Copilot
- Copiloten und Menschen arbeiten vernetzt
- Es wird orchestriert



OpenAI Language Models Cheatsheet



GPT Models

More tokens means longer prompts and responses
1 Token ≈ 4 English characters

POST /v1/completions

POST /v1/chat/completions

Completion models

(Legacy: GPT-3, 2049 tokens)

Chat Models

Optimized for chatting and following instructions

Base models

Complete prompt with likely text
"Say this is a test..."
"...to see how fit you are."

Instruction models

Optimized to follow instructions
"Say this is a test..."
"... this is a test"

GPT-3.5

\$\$

GPT-4

\$\$\$

Complex

Simple

davinci
curie
babbage
ada

\$\$\$ text-davinci-003
\$\$ text-curie-001
\$ text-babbage-001
\$ text-ada-001

Function calling

gpt-3.5-turbo

4096 tokens

gpt-3.5-turbo-0613

gpt-3.5-turbo-16k

gpt-3.5-turbo-16k-0613

16,384 tokens

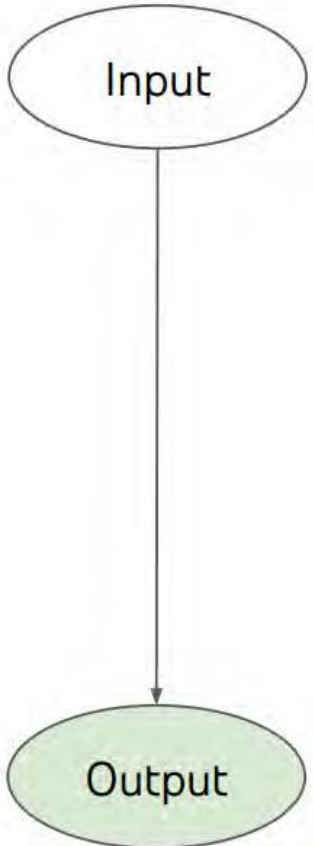
gpt-4

gpt-4-0613

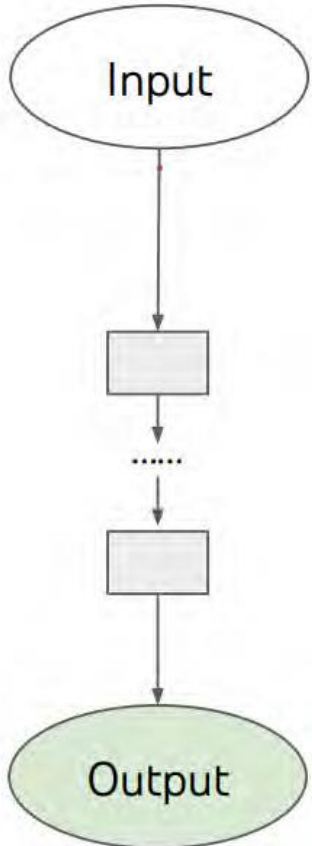
Function calling

Only base models can be fine-tuned.

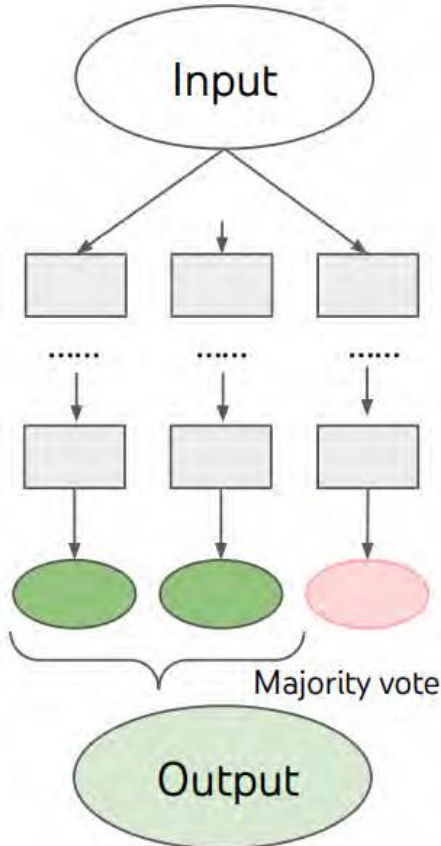




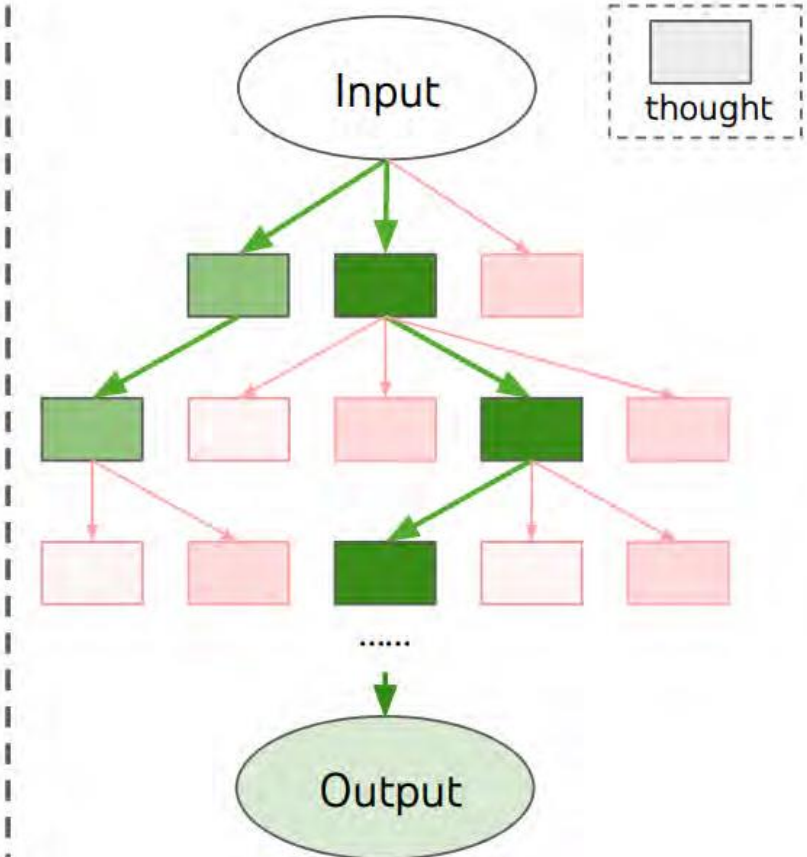
(a) Input-Output Prompting (IO)



(c) Chain of Thought Prompting (CoT)



(c) Self Consistency with CoT (CoT-SC)



(d) Tree of Thoughts (ToT)

LLM – Sommer 2024

Juli 2024 war ein sehr spannender Monat in der Welt der generativen KI. Es wurden sogar ein paar Grenzen verschoben.

- **GPT-4o** – viel größer und reifer als 3.5
- **GPT-4o Mini** - günstiges, leichtes Modell. Das beste in seiner Klasse!
- **Meta Llama 3.1** – verbesserte Version

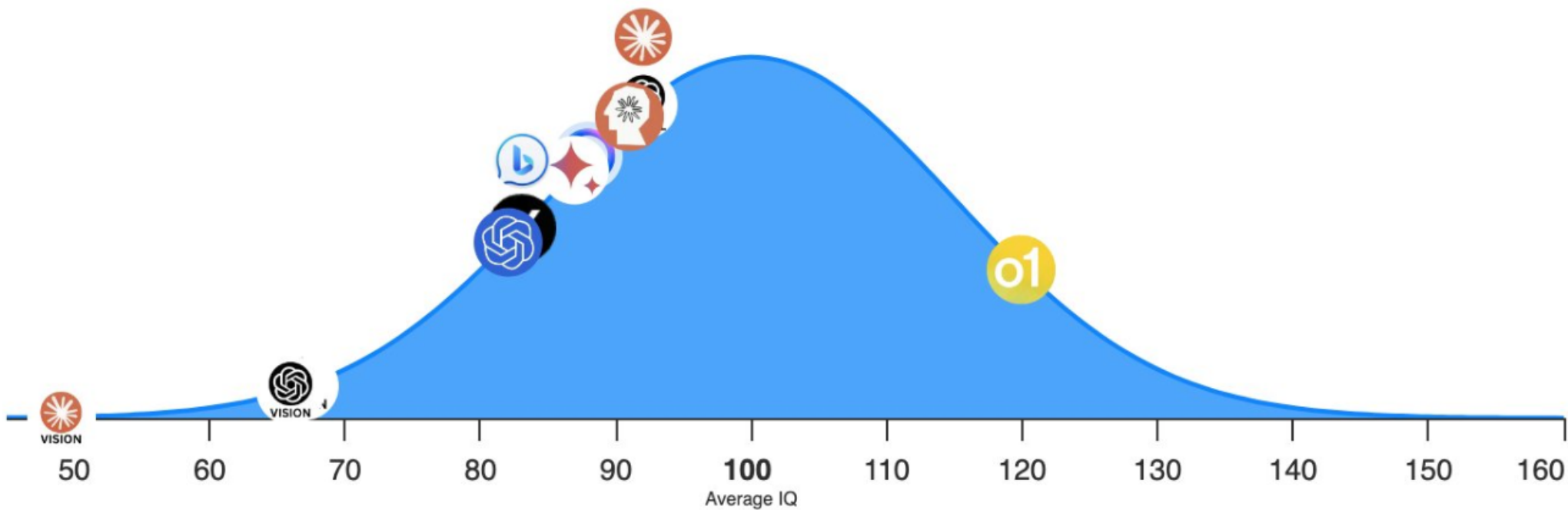
- **Mistral Large 123B v2** - lokales Modell, das das Niveau von GPT-4 Turbo v3 und Gemini Pro 1.5 erreicht. Es wäre das beste lokale Modell, wäre da nicht Meta Llama 3.1:
- **Mistral Nemo 12B** - anständiges downloadbares Modell in seiner Klasse, entwickelt für Quantisierung (Kompression)

model	code	crm	docs	integrate	marketing	reason	final 🏆	Cost	Speed
GPT-4o ☁	90	95	100	90	82	75	89	1.21 €	1.50 rps
GPT-4 Turbo v5/2024-04-09 ☁	86	99	98	93	88	45	85	2.45 €	0.84 rps
GPT-4 v1/0314 ☁	90	88	98	52	88	50	78	7.04 €	1.31 rps
Claude 3.5 Sonnet ☁	72	83	89	78	80	59	77	0.94 €	0.09 rps
GPT-4 v2/0613 ☁	90	83	95	52	88	50	76	7.04 €	2.16 rps
GPT-4 Turbo v4/0125-preview ☁	66	97	100	71	75	45	76	2.45 €	0.84 rps
GPT-4o Mini ☁	63	87	80	52	100	67	75	0.04 €	1.46 rps
Claude 3 Opus ☁	69	84	93	75	81	48	81	0.08 €	0.09 rps
Meta Llama3.1 405B Instruct 🦙	81	93	98	75	81	48	81	0.08 €	0.09 rps
GPT-4 Turbo v3/1106-preview ☁	66	75	83	63	78	59	68	0.24 €	2.33 rps
Mistral Large 123B v2/2407 ☁	68	75	83	63	78	59	68	0.24 €	2.33 rps
Gemini Pro 1.5 0514 ☁	73	96	100	56	72	41	66	0.09 €	1.77 rps
Meta Llama 3.1 70B Instruct f16 🦙	74	89	98	60	88	26	68	0.09 €	1.36 rps
Gemini Pro 1.5 0409 ☁	68	97	96	63	75	28	71	1.84 €	0.59 rps
GPT-3.5 v2/0613 ☁	68	81	73	75	81	48	71	0.34 €	1.46 rps
GPT-3.5 v3/1106 ☁	68	70	71	63	78	59	68	0.24 €	2.33 rps
Gemini Pro 1.0 ☁	66	86	83	60	88	26	68	0.09 €	1.36 rps
GPT-3.5 v4/0125 ☁	63	87	71	60	78	47	68	0.12 €	1.43 rps
Gemini 1.5 Flash 0514 ☁	32	97	100	56	72	41	66	0.09 €	1.77 rps

model	code	crm	docs
GPT-4o ☁	90	95	100
GPT-4 Turbo v5/2024-04-09 ☁	86	99	98
GPT-4 v1/0314 ☁	90	88	98

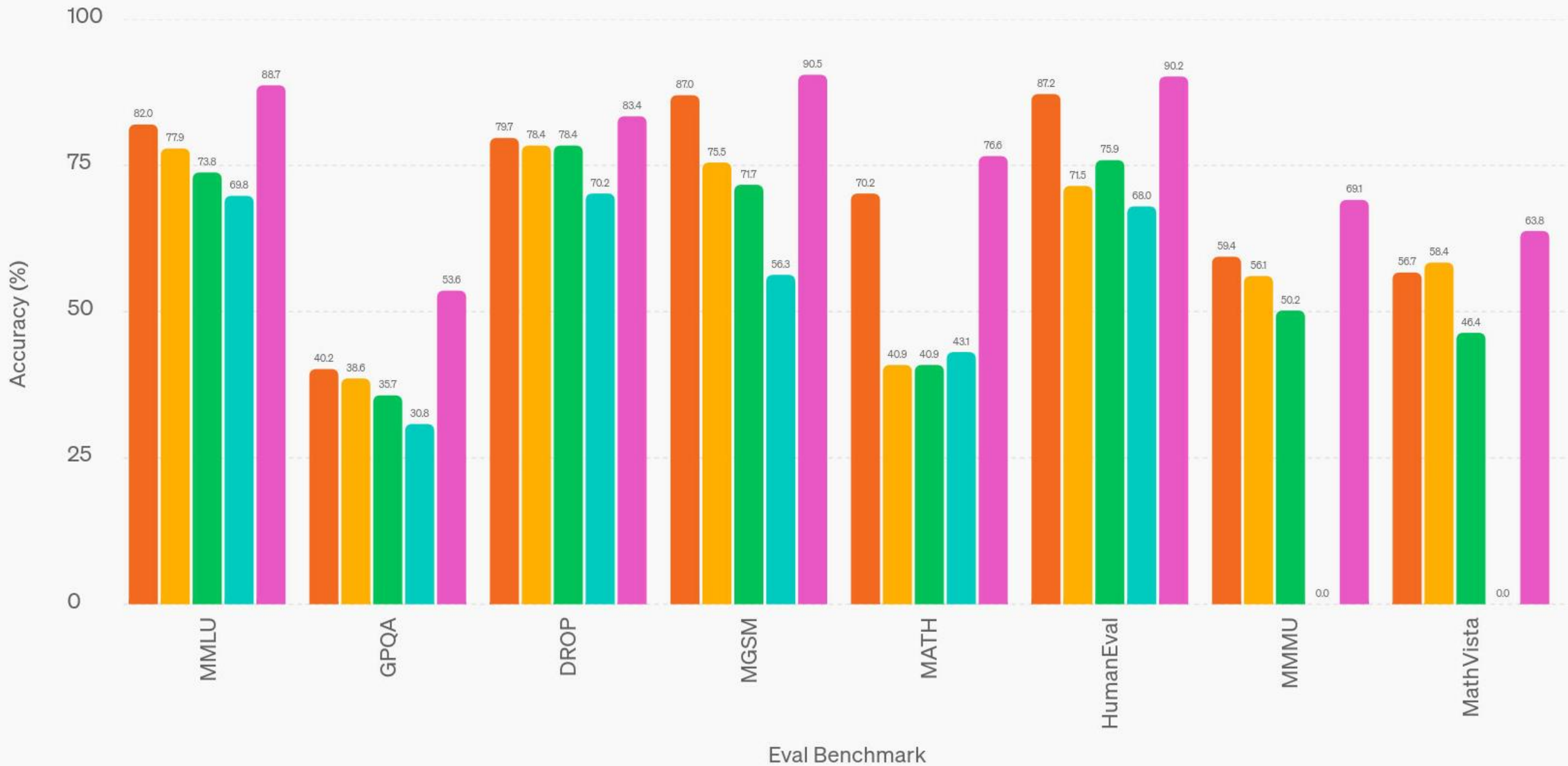
model	code	crm	docs	integrate	marketing	reason	final 🏆	Cost	Speed
GPT-4o 🗨️	90	95	100	90	82	75	89	1.21 €	1.50 rps
GPT-4 Turbo v5/2024-04-09 🗨️	86	99	98	93	88	45	85	2.45 €	0.84 rps
Google Gemini Pro 1.5 0801 🗨️	84	92	90	100	70	72	85	1.48 €	0.83 rps
GPT-4 v1/0314 🗨️	90	88	98	52	88	50	78	7.04 €	1.31 rps
Claude 3.5 Sonnet 🗨️	72	83	89	78	80	59	77	0.94 €	0.09 rps
GPT-4 v2/0613 🗨️	90	83	95	52	88	50	76	7.04 €	2.16 rps
GPT-4 Turbo v4/0125-preview 🗨️	66	97	100	71	75	45	76	2.45 €	0.84 rps
GPT-4o Mini 🗨️	63	87	80	50	100	47	75	0.04 €	1.44 rps
Claude 3 Opus 🗨️	69								
Meta Llama3.1 405B Instruct 🐘	81								
GPT-4 Turbo v3/1106-preview 🗨️	66								
Mistral Large 123B v2/2407 🗨️	68								
Gemini Pro 1.5 0514 🗨️	73								
Meta Llama 3.1 70B Instruct f16 🐘	74								
Gemini Pro 1.5 0409 🗨️	68								
GPT-3.5 v2/0613 🗨️	68								

model	code	crm
GPT-4o 🗨️	90	95
GPT-4 Turbo v5/2024-04-09 🗨️	86	99
Google Gemini Pro 1.5 0801 🗨️	84	92
GPT-4 v1/0314 🗨️	90	88
Claude 3.5 Sonnet 🗨️	72	83
GPT-4 v2/0613 🗨️	90	83

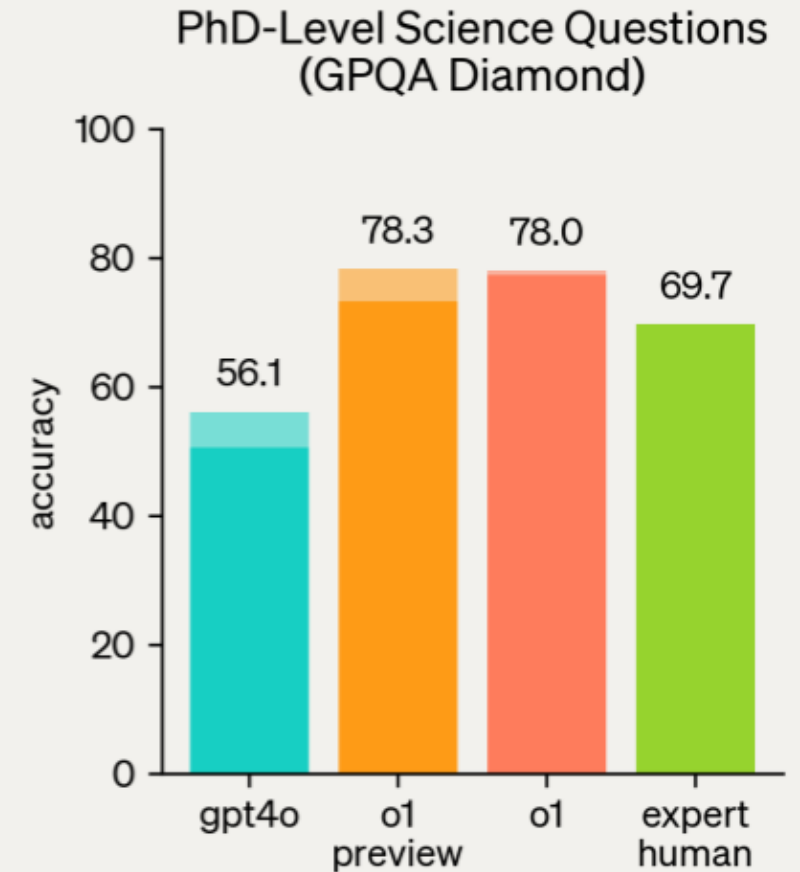
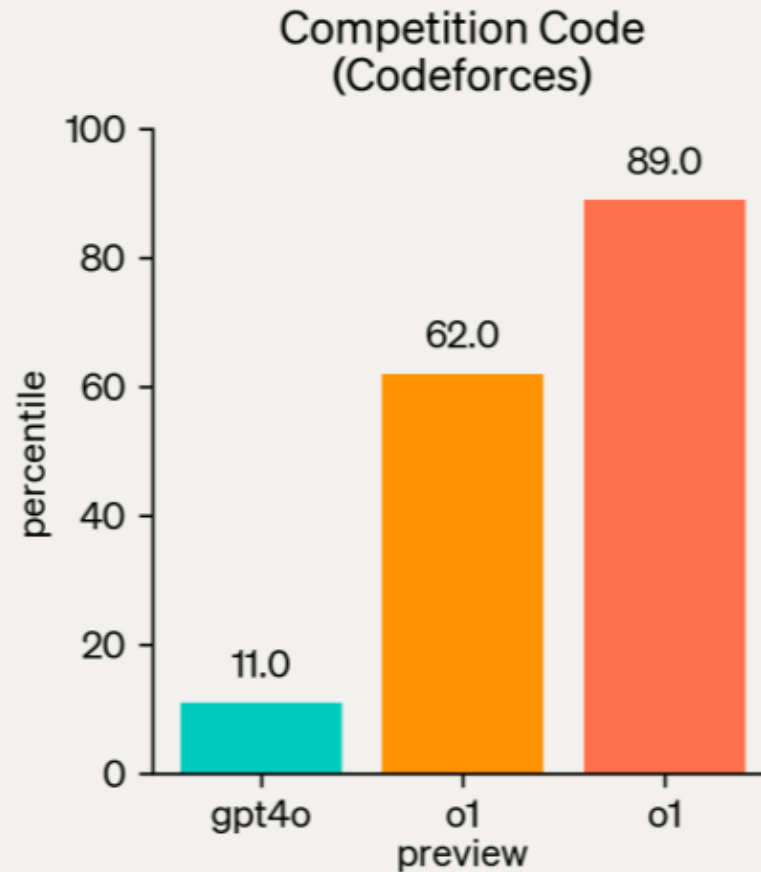
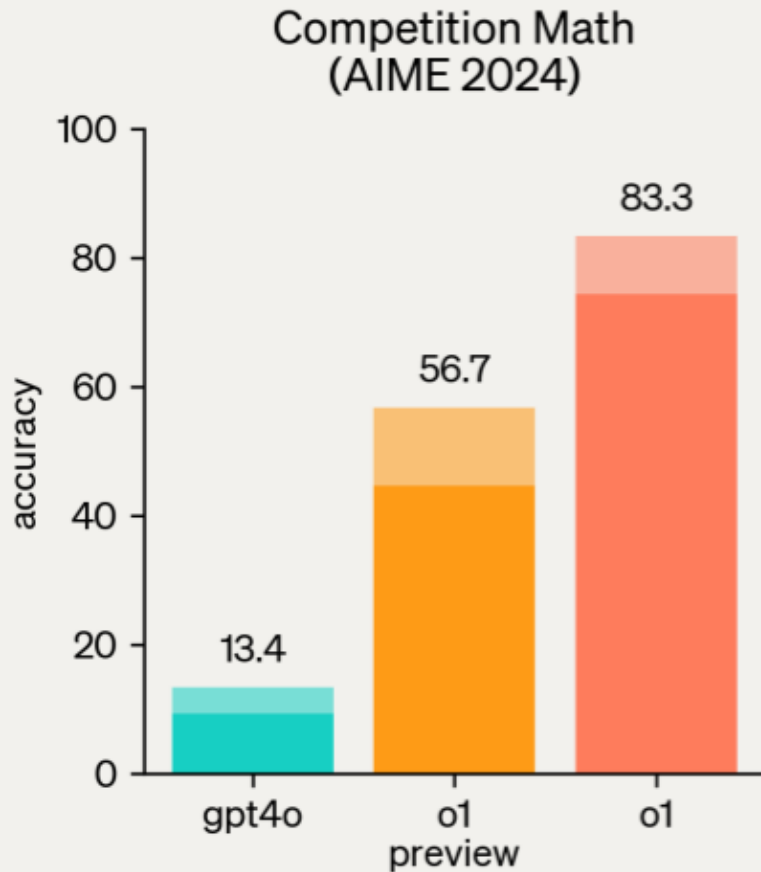


OpenAI o1 preview	Llama-3.1	Grok-2
Gemini Advanced (Vision)	Gemini Advanced	GPT4 Omni (Vision)
GPT4 Omni	ChatGPT-4	Bing Copilot
Claude-3.5 Sonnet	Claude-3 Opus	Claude-3 Opus (Vision)

GPT-4o mini Gemini Flash Claude Haiku GPT-3.5 Turbo GPT-4o



Der neue Standard – Gut wer auf das richtige Pferd gesetzt hat



Open AI - Chat GPT-4o

Prompt

- oyfjdnisdr rtqwainr acxz
mynzbhhx -> Think step by step
- Use the example above to
decode:
- oyekaijzdf aaptcg suaokybhai
ouow aqht
mynznvaatzacdfoulxxz

Ergebnis

- A possible division could be:
- oyekaijzdf
- aaptcg
- suaokybhai
- ouow
- aqht
- mynznvaatzacdfoulxxz

Open AI - 01

Prompt

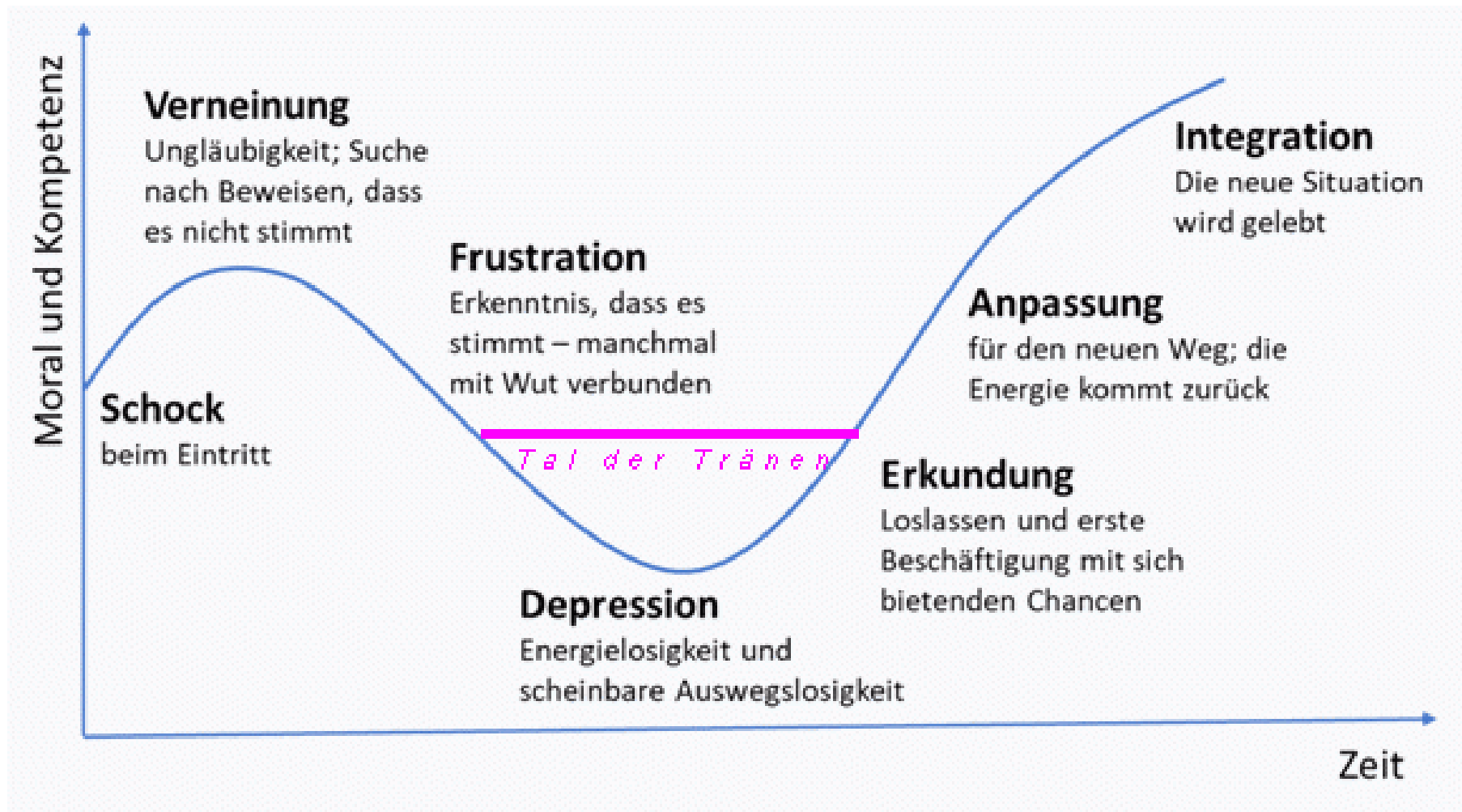
- oyfjdnisdr rtqwainr acxz
mynzbhhx -> Think step by step
- Use the example above to
decode:
- oyekaijzdf aaptcg suaokybhai
ouow aqht
mynznvaatzacdfoulxxz

Ergebnis

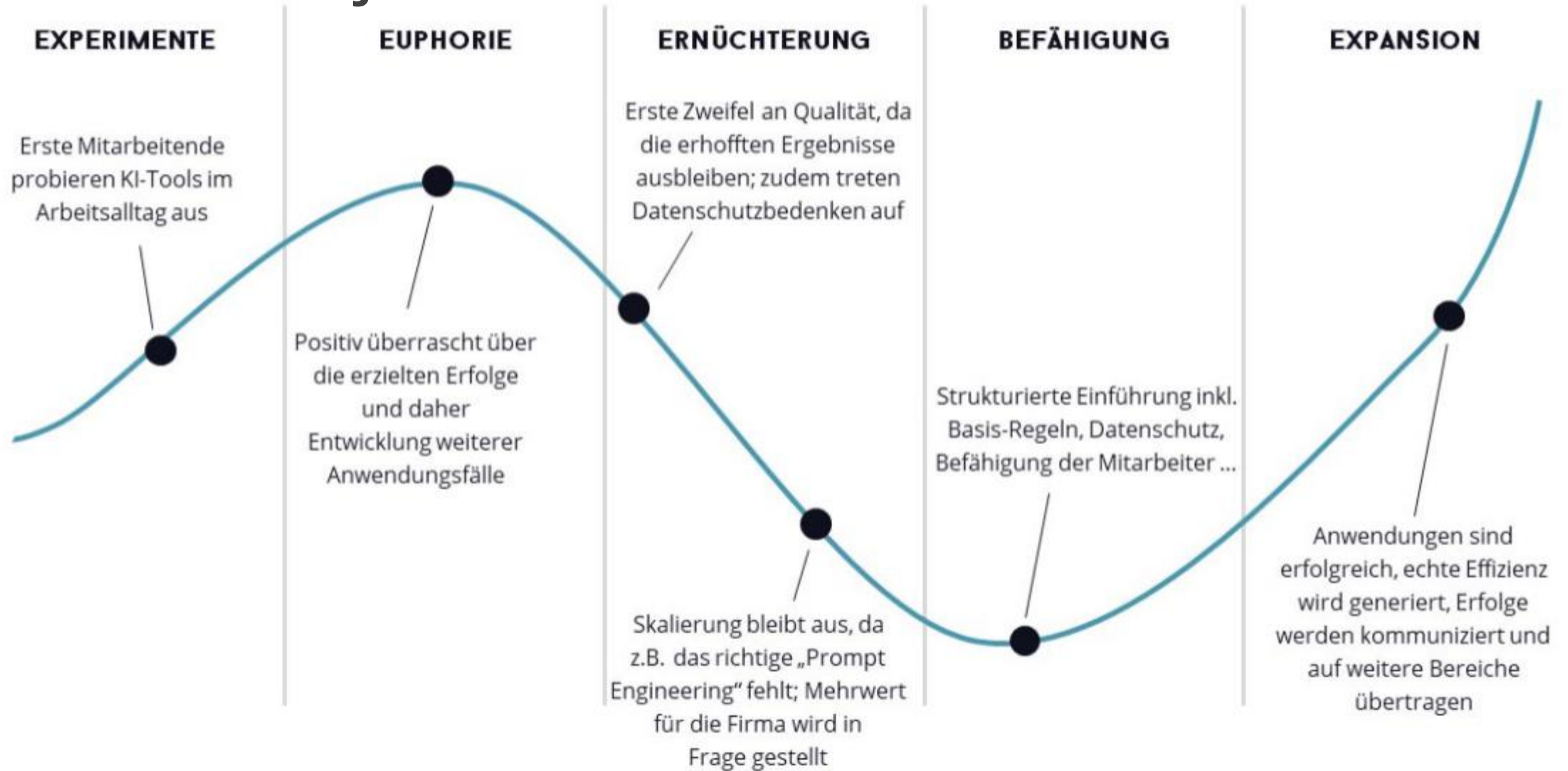
- **THERE ARE THREE R'S IN
STRAWBERRY**

Die 7 Phasen eines Change-Prozesses durch das "Tal der Tränen"

Beim emotionalen Verarbeiten der Veränderungen lassen sich sieben Phasen unterscheiden. Sie reichen von der Vorahnung „Es wird etwas geschehen“ bis zur Konsolidierung neuer Denk- und Verhaltensmuster.



6 Phasen mit KI-Projekten



Kundenumgebung

Ausgangssituation

- Umfangreiche Plattform
- Hohe Anzahl an Funktionen
- Teils hochspezialisierte Features
- Nicht jeder Nutzer kennt jede Funktion

Ziele

- Verringerung der Bedienzeit
- Intuitivere Nutzung

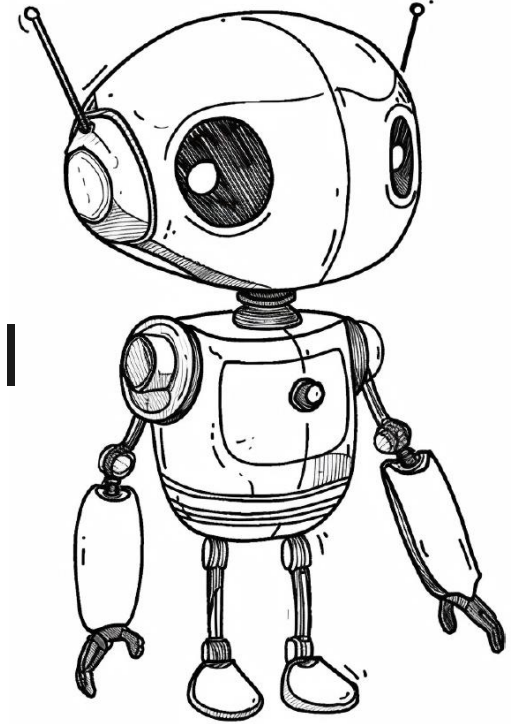
Umsetzung mit Chatbot & LLMs

IDEE

- Nutzer beschreiben oder umschreiben ihre Ziele in natürlicher Sprache
- Wir wollen nicht einfach eine Dokumentation durchsuchbarer machen
- Wir möchten die direkte Interaktion

Lösungsvorschlag

- Chatbot als zusätzlicher Interaktionskanal



Umsetzung als Proof of Concept

Warum nicht direkt als Feature umsetzen?

- Feld im schnellen Wandel
- Es gibt unzählige AI- Services, Frameworks & Tools
- Rechtzeitige Exit Strategie

Faktoren prüfen

- Umsetzbarkeit
- Wirtschaftlichkeit
- Architektur
- Vorgehensmodell
- Technologieauswahl
- Datenqualität

Welche Optionen des Datenabruf s gibt es?

- Statischer Datenabruf z.B. über REST- APIs, OpenAPI
- Querygenerierung z.B. SQL, OData, ...
- Generierung und Ausführung von Source Code

Vor- und Nachteile Datenzugriff

	Statischer Datenabruf	Query-Generierung	Code-Generierung
Flexibilität	-	+	+
Konsistenz	+	0	-
Geschwindigkeit	+	0	-
Sicherheit	+	0	-

Von den Daten zur Visualisierung

Problem

- Daten müssen über mehrere LLM- Prompts zum Frontend kommen
- Zunächst korrekte Daten können durch Halluzinationen nachträglich verändert werden

Lösungsvorschlag

- Option 1: Prompt Engineering mit Structured Text
- Option 2: Anreichern der API-Antwort um die Daten zur Visualisierung

KI ist fehlbar

Gesetze der LLMs verstehen

- **Es gibt keine Garantien, nur Wahrscheinlichkeiten**
- **Prompt Engineering**
- **Kontextgröße**
- **Man sollte die Heat des Modells nutzen**
- **Daten nachvollziehbar machen (Quellenangaben etc.)**



KI ist fehlbar

Logging

- Nutzerfeedback
- Quellenangaben
- Evaluation des Mehrwerts
- Integration in Bestandsplattform
- Nutzungskontext
- Evaluation neuer Modelle



Copyright & Datenschutz



01.05.2024 Update

Copyright

<https://learn.microsoft.com/de-de/copilot/security/faq-security-copilot>

Copilot Copyright Commitment

Microsoft verpflichtet sich dazu, für die möglichen rechtlichen Risiken, die auf Nutzer zukommen könnten, geradezustehen. "Auf die Frage unserer Kunden, ob sie die Copilot-Dienste von Microsoft und die von ihnen erzeugten Ergebnisse nutzen können, ohne sich über Urheberrechtsansprüche Gedanken machen zu müssen, geben wir eine klare Antwort: Ja, das können Sie".



Datenschutz

<https://www.microsoft.com/de-de/ai/principles-and-approach>

„Microsoft 365 Copilot entspricht unseren bestehenden Datenschutz-, Sicherheits- und Compliance-Verpflichtungen gegenüber kommerziellen Microsoft-365-Kunden, einschließlich der General Data Protection Regulation (GDPR) und der EU-Datenschutzgrundverordnung (European Union (EU) Data Boundary).“

„Eingabeaufforderungen, Antworten und Daten, auf die über Microsoft Graph zugegriffen wird, werden nicht für das Training von Foundation LLMs verwendet, auch nicht für die von Microsoft 365 Copilot verwendeten.“

Die unternehmensbezogenen Daten innerhalb des Microsoft 365 Tenants werden isoliert und geschützt, damit die Unternehmen die volle Kontrolle über ihre eigenen Daten behalten.

KI und Datenschutz - Betroffenenrechte

Transparenz und Nachverfolgbarkeit als Problem

Informationspflichten (Art. 12 DSGVO)

- Betroffener ist u.a. über Zwecke der Verarbeitung, Verarbeitungsschritte, Rechtsgrundlagen und Datenempfänger zu informieren
- Bei Datenerhebung bzw. innerhalb 1 Monat nach Erlangung
- Bei neuronalen Modellen fehlt ggf. die Nachvollziehbarkeit

Automatisierte Entscheidungsfindung (Art. 22 DSGVO)

- Betroffener ist über die Logik der Entscheidungsfindung zu informieren
- Kann menschliches Eingreifen in die Entscheidung verlangen
- Welche Faktoren sind für die Entscheidung des Algorithmus entscheidend?

Löschungsanspruch (Art. 17 DSGVO)

- Betroffener kann Löschung / Berichtigung verlangen, wenn keine Rechtsgrundlage für Weiterspeicherung
- Daten, die im Model durch Training verarbeitet sind, lassen sich nicht löschen
- Falsche Verarbeitung durch „Halluzination“ ist zu vermeiden

Auskunftsrecht (Art. 15 DSGVO)

- Betroffener kann Auskunft verlangen u.a. über Verarbeitungszwecke und Empfänger seiner Daten
- Setzt Nachvollziehbarkeit voraus, die neuronale Modell möglicherweise nicht mehr bieten

Einstellungen

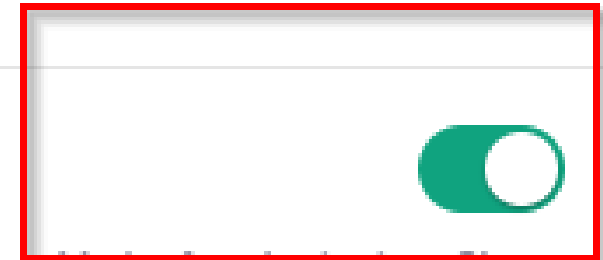


 Allgemein

 **Datenkontrollen**

Chat-Verlauf & Training

Speichern Sie neue Chats auf diesem Browser in Ihrem Verlauf und erlauben Sie uns, diese zur Verbesserung unserer Modelle zu verwenden. Nicht gespeicherte Chats werden innerhalb von 30 Tagen aus unseren Systemen gelöscht. Diese Einstellung wird nicht zwischen verschiedenen Browsern oder Geräten synchronisiert. [Erfahren Sie mehr](#)





EU AI Act

<https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

21. Mai 2024 verabschiedet
01. August 2024 in Kraft
getreten

EU AI Act

Die EU-Mitgliedstaaten haben das weltweit erste Gesetz zur Regulierung von KI verabschiedet.

Risikobasierter Ansatz - kategorisiert KI-Systeme in 4 Risikostufen:

- **Minimales Risiko:** Systeme wie Spamfilter unterliegen keinen besonderen Verpflichtungen.

- **Besondere Transparenzverpflichtungen:** Systeme wie Chatbots müssen klarstellen, dass sie Maschinen sind.

- **Hohes Risiko:** Systeme, die z.B. in der medizinischen Diagnostik oder bei der Personalauswahl eingesetzt werden, müssen strenge Anforderungen erfüllen.

- **Unannehmbares Risiko:** Systeme, die eine klare Bedrohung für die Grundrechte darstellen, sind verboten, wie z.B. Social Scoring durch Behörden

EU AI Act

Die EU-Mitgliedstaaten haben das weltweit erste Gesetz zur Regulierung von KI verabschiedet.

Drei weitere Schwerpunkte

- **Transparenz und Aufsicht:** KI-Systeme müssen transparent sein und unter menschlicher Aufsicht stehen, um sicherzustellen, dass sie sicher und vertrauenswürdig sind.
- **Förderung von Innovation:** Die Verordnung soll auch die Innovation fördern, indem sie einen klaren Rechtsrahmen schafft, der Unternehmen und Entwicklern Sicherheit bietet.

EU AI Act

Die EU-Mitgliedstaaten haben das weltweit erste Gesetz zur Regulierung von KI verabschiedet.

Drei weitere Schwerpunkte

- **Grundrechte und Sicherheit:** Ein zentrales Ziel ist der Schutz der Grundrechte und der Sicherheit der Bürgerinnen und Bürger der EU.

Strafen

- **Verstöße** gegen die Vorgaben für Hochrisiko-KI können mit empfindlichen Strafen von bis zu 30 Millionen Euro oder 6% des weltweiten Jahresumsatzes geahndet werden.

Einsatz von KI muss begleitet werden

- **Sicherstellung der Datenqualität:** Sie müssen die Qualität der für Training, Validierung und Betrieb verwendeten Daten sicherstellen und dokumentieren, um Verzerrungen zu vermeiden.
- **Technische Robustheit und Genauigkeit:** Die technische Robustheit, Genauigkeit und Sicherheit der KI-Systeme muss gewährleistet und regelmäßig überprüft werden.

Einsatz von KI muss begleitet werden

- **Menschliche Aufsicht:** HR-Abteilungen müssen menschliche Aufsicht über die KI-Systeme sicherstellen. Es muss möglich sein, einzugreifen und Systeme zu stoppen/korrigieren.
- **Transparenz und Dokumentation:** Umfassende Dokumentations- und Transparenzpflichten gegenüber Behörden und betroffenen Personen (z.B. Bewerbern) über Funktionsweise und Risiken.

Einsatz von KI muss begleitet werden

- **Konformitätsbewertung:** Vor dem Einsatz muss eine Konformitätsbewertung durch unabhängige Stellen erfolgen.
- Insgesamt wird der AI Act zu mehr **Compliance-Aufwand**, aber auch zu mehr Vertrauen in KI-Systeme führen



Vielen Dank

Björn Fox



: +49 (2131) 7949-468



bjoern.fox@avantgar.de



www.avantgar.de

