Centrum für Europäische Politik
FREIBURG | BERLIN

cepInput

Nr. 7 | 2024 16. April 2024

Sprachtechnologie als Wettbewerbsvorteil der EU

Zehn Faktoren für den produktiven Einsatz generativer KI in KMU

Anselm Küsters

Quelle: DALL-E

Sprachmodelle wie ChatGPT stellen eine große Herausforderung, aber auch eine Chance für Europa dar. Statt Protektionismus, Leuchtturmprojekten oder Risikoscheue ist ein pragmatischer Ansatz für den breiten Einsatz von KI-Sprachtechnologie in der Wirtschaft notwendig, um die Wettbewerbsfähigkeit zu erhalten und das Innovationspotenzial auszuschöpfen. Dieser cepInput beschreibt zehn Faktoren, die kleine und mittlere Unternehmen bei der Implementierung berücksichtigen sollten, um bestehende Wettbewerbsvorteile zu nutzen.

- KMU sollten durch eine Bedarfsanalyse und strategische Planung konzeptionell verstehen, wie KI ihre Prozesse verbessern kann. Die Wahl von Cloud-basierten Diensten sowie die Nutzung offener Modelle beeinflussen die Anpassungsfähigkeit der KI-Tools und die spätere Abhängigkeit von externen Unternehmen.
- Durch „Fine-Tuning" und den Einsatz von „Retrieval-Augmented Generation" können KMU ihre Anwendungen spezialisieren. Die Fehleranfälligkeit der KI-Modelle muss an die interne Fehlertoleranz angeglichen werden. Zudem sollten interne Kompetenzen im Bereich Prompt-Design und Online-Design aufgebaut werden.
- Für einen nachhaltigen und gesellschaftlich verantwortlichen Einsatz müssen gesetzliche Rahmenbedingungen berücksichtigt, interne Tests kontinuierlich durchgeführt und die Energieeffizienz gemessen werden. Feedback-Mechanismen sollten genutzt werden, um die Technologie auf dem neuesten Stand zu halten.

Inhaltsverzeichnis

1 Einleitung: Sprachtechnologie anwenden statt nachbauen

Bei jeder Anfrage an ChatGPT wird ein großes Sprachmodell verwendet. Angesichts der rasanten Entwicklung in diesem schnell wachsenden Bereich der Künstlichen Intelligenz (KI) steht Europa vor einer großen Herausforderung, der bisher mit einer zu starken Fokussierung auf Leuchtturmprojekte[1] und einer zu geringen Anwendung in der Breite der Wirtschaft begegnet wird. Die europäische und deutsche Politik zielt derzeit vor allem darauf ab, sich langfristig einen möglichst großen Anteil an der KI-Wertschöpfungskette zu sichern, um spätere strategische Abhängigkeiten zu vermeiden. Dies umfasst den Aufbau von Datenräumen,[2] die massive Subventionierung von Chip-Fabriken[3] und zuletzt auch den Betrieb spezieller KI-Supercomputer, den Aufbau sogenannter „AI Factories"[4] und eine europäische „Allianz für Sprachtechnologien", um eigene große Sprachmodelle zu bauen.[5] Die kaum verborgene Hoffnung auf eigene nationale Champions leitete Deutschland und Frankreich bei den abschließenden Verhandlungen des EU KI-Gesetzes an.[6] Insgesamt sind diese Initiativen zum Bau eigener Sprachtechnologie als Teil eines größeren „home-shoring" Trends zu verstehen,[7] der vor dem Hintergrund der geopolitischen Spannungen von der Ukraine bis zu Taiwan weiter an Bedeutung gewinnt.

Auch wenn ein solches strategisches Denken – lange auf EU-Ebene vernachlässigt – langfristig sinnvoll ist, lässt die Dynamik der KI keinen weiteren Aufschub in der konkreten Anwendung zu. Die exponentielle Entwicklung der Technologie, die sich bislang auf die USA konzentriert,[8] zwingt zu „second-best Lösungen", die sich vom bisherigen Politikansatz in Europa unterscheiden. Anstatt ausschließlich Pläne zum Entwickeln eigener Infrastrukturen und Modelle aufzusetzen, begleitet von langsamen öffentlichen Vergabeverfahren und europäischer Detail-Regulierung, sollte jetzt mehr über die konkrete Implementierung dieser Technologie gesprochen werden. Insbesondere kleine und mittlere Unternehmen (KMU) in Europa können aufgrund der schwierigen wirtschaftlichen Lage und dem Kampf um globale Wettbewerbsfähigkeit nicht darauf warten, bis einheimische Anbieter konkurrenzfähige Modelle entwickeln. Für die schnelle und flächendeckende Anwendung von KI-Sprachtechnologien sind kommerzielle US-amerikanische Modelle und freie Open-source-Modelle von unschätzbarem Wert.

Obwohl generative KI durch seine zahlreichen Anwendungsfälle das Potenzial besitzt, branchenübergreifend einen Mehrwert von 2,6 Billionen bis 4,4 Billionen US-Dollar zu schaffen,[9] hapert es hierzulande bislang bei der Integration von existierenden Modellen in der unternehmerischen Praxis.[10] Obwohl geschätzt wird, dass KI-Tools wie ChatGPT 60 bis 70 Prozent der wissensintensiven Arbeitszeit von Mitarbeitenden automatisieren könnten, sind Führungskräfte bislang eher zurückhaltend – nicht zuletzt, weil die Technologie als nicht ausgereift oder zu ungenau gilt.[11] Bei aller Sorge vor Fehlern und sogar existenziellen Risiken, die mit KI verbunden sind, besteht auch die Gefahr, aus übertriebener

---

1 Siehe zu dieser Kritik an „Leuchttürmen": Friesike und Sprondel (2022), Träge Transformation. Welche Denkfehler den digitalen Wandel blockieren, Stuttgart: Reclam.

2 Common European Data spaces | Shaping Europe's digital future (europa.eu).

3 Küsters und Kullas (2023), Kann der Chips Act Europas Resilienz fördern?, Audit Committee Quarterly II/2023.

4 Kommission startet KI-Innovationspaket (europa.eu).

5 LEAM Machbarkeitsstudie 2023 - KI-Verband; Launching an 'AI moonshot' to develop a European large language model is the game changer that Europe needs – CEPS.

6 EU-Regeln für ChatGPT und Aleph Alpha: Deutschland und Frankreich dagegen (faz.net).

7 Foroohar (2022), Homecoming: The Path to Prosperity in a Post-Global World, Penguin Random House.

8 The Economist (2024), How San Francisco staged a surprising comeback (Feb 12th 2024).

9 Siehe die Statistiken bei: Economic potential of generative AI | McKinsey.

10 Siehe etwa: Umfrage sieht schweren Stand für KI in deutschen Firmen - Tagesspiegel Background. Generell zum Rückstand: Gutachten zu Forschung, Innovation und Technologischer Leistungsfähigkeit Deutschlands 2024 (e-fi.de), S. 116ff.

11 Siehe die Statistiken bei: Top 30 Must Know Generative AI Stats in 2024 (aimultiple.com).

Vorsicht die Vorteile von KI-Technologien nicht zu nutzen, wie jüngst sogar die Vereinten Nationen betont haben.[12] In der Tat wird oft übersehen, welche methodischen Fortschritte bei generativer KI in kürzester Zeit erzielt wurden. Die ebenfalls öfters geäußerte Befürchtung, bei der Integration fremder Technologie in spätere Abhängigkeiten zu geraten, erscheint angesichts des starken Wettbewerbsdrucks momentan weniger dringlich. Zudem ist diese strategische Gefahr geringer als gemeinhin angenommen: Die Verfügbarkeit von modernen Sprachmodellen ermöglicht es gerade kleineren, nicht spezialisierten Datenteams, flexible Anwendungen nur durch die Nutzung natürlicher Sprache zu erzielen, ohne dass spezieller Code oder spezielle Module erforderlich sind.[13] Dies reduziert die Lern- und Wechselkosten („switching costs“) erheblich, reduziert das Potenzial für spätere Abhängigkeiten und bietet einen starken Kontrast zu bisherigen Herausforderungen im digitalen Marktumfeld.[14]

Für europäische KMU ist es daher nun höchste Zeit, hochwertige KI-Sprachmodelle in ihre internen und externen Prozesse zu integrieren. Dieser **cepInput** dient als konzeptionelle Übersicht über die dabei zu berücksichtigenden Faktoren und skizziert zehn zentrale Elemente einer Sprachtechnologie-Strategie für KMU, die als Grundlage für die Erstellung einer internen Richtlinie zum Umgang mit generativen KI-Tools verwenden werden können.[15] Diese reichen vom Design der Anfragen („prompts“) bis hin zu Datenschutzbedenken. Generell strebt diese Publikation keine rechtliche Beratung an, sondern möchte über Möglichkeiten und Anwendungen dieser neuen Tools informieren und vermitteln, wo deren Probleme (noch) liegen. Selbstverständlich ist in jedem Einzelfall zu prüfen, ob der Einsatz von Sprachmodellen unternehmerisch sinnvoll ist oder nicht, doch als „general-purpose-technology“ stehen diese vor einem breiten, sektorübergreifenden Einsatz, der laut Schätzungen der aktuellen Literatur zwischen 10-30 Prozent aller Arbeitnehmer in Europa direkt beeinflussen könnte.[16] Dabei bietet die Integration von Sprachtechnologien nicht nur die Chance, Effizienz und Innovationskraft zu steigern, sondern auch Europa im globalen Wettbewerb zu stärken. KMU sollten jetzt proaktiv handeln, um die Vorteile der KI-Technologie zu nutzen – und gleichzeitig die Risiken sorgfältig abwägen.

2 Faktoren für den Einsatz generativer KI in KMU

Was ist generative KI und was verbirgt sich hinter dem Begriff Sprachmodelle? Im Kontext von ChatGPT und Co wird das Kürzel KI heutzutage meist für eine Klasse von fortschrittlichen Modellen verwendet, die darauf trainiert sind, Inhalte zu erzeugen, die sich kaum von menschlicher Arbeit unterscheiden – seien es Texte, Bilder, Code oder sogar kurze Videos. Im Zentrum dieser Technologie stehen große Sprachmodelle („Large Language Models“, LLM)[17], die durch die Verarbeitung großer Textmengen lernen, die Nuancen der menschlichen Sprache zu erfassen und für kreative Exploration zu nutzen. Sprachmodelle definieren eine Wahrscheinlichkeitsverteilung für Wortfolgen und könne daher für generative Zwecke verwendet werden, indem sie die wahrscheinlichsten nächsten Wörter am Anfang eines Textes vorhersagen. In den letzten Jahren sind diese Modelle immer größer geworden (d.h. sie

[12] UN AI Advisory Body, Interim Report: Governing AI for Humanity, December 2023, interim_report.pdf (un.org), p. 12.
[13] Siehe hierfür auch die Argumentation unten in Sektion 2.1.
[14] Kommission (2024), Bekanntmachung der Kommission über die Abgrenzung des relevanten Marktes im Sinne des Wettbewerbsrechts der Union, Brüssel, den 8.2.2024, C(2023) 6789 final, Rn. 98.
[15] Dabei handelt es sich explizit um keine rechtliche Beratung, etwa im Hinblick auf noch offene Datenschutzfragen. Für ein Beispiel für interne KI-Richtlinien, siehe etwa: BBC (2024), Guidance: The use of Artificial Intelligence (bbc.co.uk).
[16] Mauro Cazzaniga et al. (2024), Gen-AI: Artificial Intelligence and the Future of Work (imf.org). Siehe auch: Albanesi, Stefania and Dias da Silva, Antonio and Jimeno, Juan F. and Lamo, Ana and Wabitsch, Alena, New Technologies and Jobs in Europe (2023). NBER Working Paper No. w31357.
[17] Wie GPT („Generative Pre-trained Transformer“). Für einen Überblick, siehe: [2402.06196] Large Language Models: A Survey (arxiv.org).

basierend auf mehr Trainingsdaten und verwenden mehr Parameter im Modell), wodurch sich ihre Fähigkeiten der Textvorhersage signifikant verbessern haben („scaling law“).[18] Beim Skalieren dieser Sprachmodelle können plötzlich und unvorhersehbar neue Fähigkeiten auftreten, wie Rechnen, Fragen beantworten und Texte zusammenfassen, die nicht direkt trainiert, sondern nur durch Beobachtung der natürlichen Sprache erlernt werden („emerging capabilities“).[19] Die enormen und unvorhersehbaren Sprünge in den Fähigkeiten dieser Modelle haben zuletzt zu einem regelrechten „KI Boom“ geführt.

Aufgrund der beschriebenen Fortschritte können die neuesten Modelle nicht nur vorhandene Informationen kohärent und kontextbezogen wiedergeben, sondern auch originelle Inhalte auf Grundlage der gelernten Muster generieren. Dies eröffnet zahlreiche Anwendungsmöglichkeiten für Unternehmen, von der automatisierten Texterstellung über die Entwicklung von Chatbots bis hin zur Generierung kreativer Werke. Inzwischen haben Experten mehr als hundert allgemeine und branchenspezifische Anwendungsfälle von generativer KI zusammengetragen, von denen viele auch für KMU relevant sein dürften.[20] Prozesse, die ein hohes Maß an Arbeit mit Wörtern, Bildern, Zahlen und Tönen beinhalten (sogenannte WINS-Arbeit, kurz für *Words, Images, Numbers, Sounds*), dürften am meisten von der neuen Technologie profitieren.[21] So können generative KI-Tools etwa das Verfassen von Marketing- und Vertriebstexten erleichtern, die Entwicklung kreativer Marketingideen unterstützen, automatisch Musterdokumente erstellen oder regulatorische Aktualisierungen erkennen.[22] Ein besonders eindrucksvolles Beispiel liefert der Bezahldienstleister Klarna, dessen ChatGPT-basierter KI-Assistent innerhalb eines Monats die Arbeit von 700 Vollzeitmitarbeitern übernahm und dabei die Probleme in Kunden-Chats präziser löste, was dann zu einem Rückgang der Anfragen um 25 Prozent führte.[23]

Die folgende Analyse bleibt nicht bei einer allgemeinen Abwägung der Vor- und Nachteile von generativer KI stehen, sondern versucht, zentrale Elemente für eine rasche Integration von Sprachmodellen in die Prozesse europäischer und deutscher KMU zu identifizieren. Eine effektive Sprachtechnologiestrategie sollte die folgenden zehn Elemente berücksichtigen.

2.1 Bedarfsanalyse: Generative KI konzeptionell verstehen

KMU sollten zunächst eine gründliche Bedarfsanalyse durchführen, um zu verstehen, welche internen und externen Prozesse durch die Integration von Sprachmodellen verbessert werden können. Viele Unternehmen scheitern derzeit an der Integration, weil sie generative KI methodisch fälschlicherweise als traditionelle Form der Automatisierung betrachten und nicht als unterstützenden Agenten, der mit der Zeit intelligenter wird.[24] Die Entwicklung des maschinellen Lernens (ML) und sein schrittweiser Einsatz in Unternehmen in den letzten zehn Jahren bietet eine interessante Parallele, die zeigt, wie schwierig es sein kann, von der bloßen Faszination für eine neue Technologie zu einem strategischen Verständnis ihrer konkreten Anwendungen zu gelangen.[25] Obwohl fortgeschrittene ML-Funktionen wie Bild- und Spracherkennung in den 2010er Jahren immer bekannter wurden, wussten viele Unternehmen anfangs nicht, wie sie solche Techniken einsetzen sollten, insbesondere wenn sie nicht direkt

[18] Sardana et asl. (2023), [2401.00448] Beyond Chinchilla-Optimal: Accounting for Inference in Language Model Scaling Laws (arxiv.org).
[19] Wei et al. (2022), [2206.07682] Emergent Abilities of Large Language Models (arxiv.org).
[20] Top 100+ Generative AI Applications / Use Cases in 2024 (aimultiple.com).
[21] Where Should Your Company Start with GenAI? (hbr.org).
[22] Zu den folgenden Beispielen, siehe: Economic potential of generative AI | McKinsey.
[23] Klarna AI assistant handles two-thirds of customer service chats in its first month.
[24] Your Organization Isn't Designed to Work with GenAI (hbr.org).
[25] Siehe dazu den instruktiven Essay in: Benedikt Evans, „Abstracting Ai“, in: Benedict's Newsletter: No. 528 (20. Feb. 2024).

mit ihrem Geschäftskern zu tun hatten. Erst mit der Zeit änderte sich die Wahrnehmung von ML als Werkzeug für spezifische Aufgaben hin zu einem hochentwickelten Mustererkennungssystem. Indem Unternehmen und Start-ups damit experimentierten, welche bestehenden Probleme sich in Mustererkennungsprobleme umformulieren ließen, entstanden neue unternehmerische Möglichkeiten. Die Wertschöpfung durch neue Technologien besteht also nicht nur darin, sie in bestehende Geschäftsprozesse zu integrieren, sondern auch darin, diese Prozesse neu zu gestalten.

Für generative KI, wie z.B. die Verwendung großer Sprachmodelle, muss nun ein ähnliches konzeptionelles Umdenken stattfinden wie bei der schrittweisen Integration von ML. Auf welche grundlegenden Probleme eines bestimmten Geschäftsfelds kann diese Technologie sinnvoll angewendet werden? Im Gegensatz zur klassischen Automatisierung durch Roboter lässt sich die Funktionalität der generativen KI am besten durch ihre dialogische Funktion verstehen, die es ermöglicht, dass Technik und Mensch dynamisch Verantwortung teilen.[26] Dabei ist es hilfreich, sich generative KI als das Äquivalent von Millionen von Praktikanten vorzustellen, d.h. einfallsreich und energisch, ungenau und etwas unberechenbar, aber kostengünstiger und viel besser skalierbar als echte Praktikanten.[27] Beispielsweise hat die Design Thinking-Literatur zur Förderung institutioneller Intelligenz gezeigt, dass die Ergebnisse von LLM-Systemen als Ideen und nicht als endgültige Antworten betrachtet werden sollten und dass diese Systeme daher intern als ein Werkzeug zur Unterstützung der menschlichen Wahrnehmung positioniert werden sollten.[28] Mit anderen Worten: Während das klassische maschinelle Lernen in den letzten zehn Jahren durch seine Fähigkeit zur Mustererkennung in Geschäftsprozesse integriert werden konnte, wird generative KI den Unternehmen als iterativer Dialogpartner zur Verfügung stehen, vergleichbar mit einem Pool an Praktikanten. Für KMU stellt sich daher zunächst die konzeptionelle Frage, wie sie sich intern so verändern können, dass sie diese Dialogfunktion optimal nutzen können. Insofern liegt der Wert von LLM in der Integration in größere Systeme und nicht in der Einzelanwendung.

Die Zielsetzung sollte auf dieser Analyse basieren und klare, messbare Ziele für die Implementierung von Sprachtechnologien festlegen. Ein gutes Beispiel ist die Werbe- und Marketingbranche, bei der generative KI bereits für zahlreiche Anwendungen eingesetzt wird, wie etwa die Erstellung von schriftlichen Inhalten und Werbetexten (58 %), SEO-Keyword-Recherchen (43 %) und E-Mail-, Meeting- und Kampagnenzusammenfassungen (38 %).[29] Ein beeindruckendes Beispiel ist Coca-Cola, das kürzlich über den Einsatz generativer KI zur automatischen Erstellung von Tausenden von Marketinginhalten berichtete. Das Unternehmen verlagerte seine Medienausgaben gezielt von Fernsehwerbung, deren Produktion oft Monate dauerte und die später nicht mehr geändert werden konnte, auf digitale Kanäle, für die mithilfe von KI-Sprachtechnologie rund „1.000 kontextuell relevante Inhalte“ produziert werden konnten, deren Ergebnisse zudem in Echtzeit messbar waren.[30] Die Auswirkungen dieser Marketingausgaben waren in den finanziellen Ergebnissen des Unternehmens deutlich sichtbar. Insgesamt ist diese Phase der Bedarfsanalyse und der konzeptionellen und strategischen Auseinandersetzung mit generativer KI entscheidend für den Erfolg der Einführung von Sprachtechnologie, da sie die Grundlage für alle weiteren Schritte bildet und sicherstellt, dass die Technologieeinführung auf die spezifischen Bedürfnisse und Ziele des Unternehmens zugeschnitten ist. Im Folgenden wird davon ausgegangen, dass eine solche Bedarfsanalyse und Zielsetzung durch das Management bereits erfolgt ist.

---

[26] Für diesen “Designing for Dialogue“-Ansatz, siehe: Your Organization Isn’t Designed to Work with GenAI (hbr.org).
[27] Siehe: Giacomelli, G. (2024), Beyond "Human in the Loop": Reliable AI in Enterprise Workflows (linkedin.com).
[28] Rick et al. (2023), Supermind Ideator: Exploring generative AI to support creative problem-solving (arxiv.org).
[29] The GPT Store isn’t ChatGPT’s ‘app store’ – but it’s still significant for marketers (econsultancy.com).
[30] Coca-Cola CEO: Innovation is serving as a ‘competitive advantage’ (marketingweek.com).

2.2 Strategische Abhängigkeiten: Marktmacht bedenken

Sobald sich ein Unternehmen für den Einsatz generativer KI entschieden hat, stellt sich die Wahl zwischen der Nutzung von generativer KI als Cloud-Produkt eines Drittanbieters („Artificial Intelligence as a Service", AIaaS) und der eigenen Erstellung und Implementierung vor Ort („on premise") – eine für Unternehmen zentrale Wahl, da sie sich direkt auf die Skalierbarkeit und Flexibilität der KI-Lösungen auswirkt.[31] AIaaS bietet Unternehmen Zugang zu fortschrittlichen Algorithmen und Rechenressourcen (etwa über Microsoft Azure), ohne dass sie eine eigene Infrastruktur wie etwa spezialisierte GPU-Server vorhalten müssen. Umgekehrt kann die Entscheidung für eigene KI-Installationen eine engere Abstimmung mit den spezifischen Geschäftsanforderungen ermöglichen, was in der Regel zu einer höheren Effizienz und Genauigkeit der KI-Anwendungen führt. Neben der strategischen Weichenstellung, die in diesem Abschnitt diskutiert wird, sollten KMU bei dieser Wahl auch die Energiekosten und Wartungsanforderungen (Sektion 2.9) sowie den Datenschutz (Sektion 2.7) berücksichtigen.

Da sie nicht über große Server-Farmen und spezialisierte Chips zum Trainieren eigener großer Sprachmodelle verfügen, wie die weltweit führenden Big Tech-Unternehmen (GAFAM) und die von ihnen finanzierten Startups,[32] müssen KMU Technologien wählen, die sich leicht anpassen lassen und die Möglichkeit bieten, weitere Funktionen oder Kapazitäten bei Bedarf hinzuzufügen. Zudem sollten die ausgewählten Sprachtechnologien skalierbar und flexibel sein, um mit dem Wachstum des Unternehmens und sich ändernden Anforderungen Schritt halten zu können.

Beides spricht dafür, auf vortrainierte LLMs zurückzugreifen. Diese können entweder proprietär und bezahlpflichtig sein (z.B. die neuesten GPT-Modelle von OpenAI) oder kostenfrei und Open-source (wie etwa das Llama-Modell von Meta). Wichtig ist zu erkennen, dass nicht alle freien Modelle automatisch „echtes" Open-source bedeuten und Nutzungsbeschränkungen aufweisen können; vielmehr entscheidend sind die Modalitäten, mit denen Zugang gewährt wird: Modelle können vollständig geschlossen sein (für niemanden außerhalb der Entwicklerorganisation verfügbar), über eine Webschnittstelle verfügbar gemacht werden (beispielsweise die API von GPT-4), einen rein Cloud-basierten Zugang bieten, einen Zugang zum Fine-Tuning gewähren (GPT-3 von OpenAI), ihre Gewichte offen legen (wie Stable Diffusion von Stability AI und Llama 2 von Meta), oder mit sämtlichen Gewichten, Code und Daten vorliegen.[33] Für KMU bieten sich aufgrund der oben ausgeführten Überlegungen insbesondere die letztgenannten Kategorien an, die oft als „offene Basismodelle" zusammengefasst werden; also Modelle, die transparent und mit weithin verfügbaren Gewichten veröffentlicht werden.

Ein weiteres wichtiges Kriterium ist die Leistungsfähigkeit der Modelle. Da diese für ein wettbewerbsfähiges Produkt oder eine wettbewerbsfähige Dienstleistung auf den nachgelagerten Märkten, auf denen das KMU tätig ist, entscheidend ist, spielen selbst kleine Unterschiede eine große Rolle. Hier zeigen die verschiedenen von Forschern entwickelten Metriken und Branchenumfragen ein klares Bild: Das von OpenAI entwickelte GPT-4-Modell ist (derzeit) der Branchenprimus und schlägt alle anderen LLMs sowohl in klassischen Benchmarks als auch in Tests, die für die Beurteilung durch Menschen entwickelt

---

[31] Bitkom (2024), Generative KI im Unternehmen. Rechtliche Fragen zum Einsatz generativer Künstlicher Intelligenz im Unternehmen, S. 16, 41.

[32] Von Thun (2024), Euractiv - EU does not need to wait for the AI Act to act — Open Markets Institute; Küsters und Kullas (2024), cep - Centrum für europäische Politik.

[33] Bommasani (2023), Considerations for Governing Open Foundation Models, Governing-Open-Foundation-Models.pdf (stanford.edu).

wurden.[34] Jüngst konnten allerdings die Modelle Claude 3 (Opus) und Gemini Ultra (von Google) deutlich aufholen,[35] was Unternehmen einen gewissen Entscheidungsspielraum gibt. Danach folgen Open-source-Modelle wie Llama von Meta, und zuletzt auch von Mistral AI aus Frankreich. Anstatt also zu versuchen, selber kostspielige Modelle zu bauen, oder darauf zu warten, dass exklusiv heimische Anbieter gleichwertige Modelle auf den Markt bringen, sollten europäische KMU schnellstmöglich auf diese bereits etablierten Modelle zurückgreifen. Sollte man sich aufgrund der Leistungsunterschiede für ein proprietäres Modell (wie GPT-4) anstatt für ein Open-source-Modell entscheiden, sollte die Nutzung der eingegebenen Daten durch den KI-Provider (wie OpenAI) allerdings durch eine vertragliche Vereinbarung oder die Wahl einer bestimmten Lizenz ausgeschlossen werden.

Entsteht dadurch nicht eine langfristige Abhängigkeit und, durch die ungleiche Marktmachtverteilung, ungünstige Pfadabhängigkeiten und Lock-in-Effekte? So warnt etwa der Bitkom mit Blick auf die Nutzung von generativer KI in Unternehmen vor „entstehender Abhängigkeit von externen Dienstleistern z. B. durch Offenlegung von Know-how oder Daten, sowie Folgekosten (z. B. Updates, Wartung, Wechsel des externen Dienstleisters zu späteren Zeitpunkten)“.[36] Im Gegensatz zu früheren digitalen Marktentwicklungen dürften strategische Abhängigkeiten im Bereich der KI-Sprachtechnologie jedoch weit weniger gravierend sein, da die Modelle aufgrund des Zugangs über natürliche Sprache relativ leicht austauschbar sind, was die Marktmacht führender Entwickler verringert. Wie ein KI-Experte jüngst festhielt: „It’s remarkable that we can control a multi-trillion parameter bit of software sitting on hundreds of gigabytes of input data with ordinary English.”[37] Diese Zugänglichkeit über (vergleichsweise) einfache Sprache bedeutet, dass bereits wenige Mitarbeiter mit einem rudimentären technischen Hintergrund mit hochentwickelten Softwaresystemen interagieren und deren Funktionsweise beeinflussen können. Im Gegensatz dazu war früher ein tiefes Verständnis von Programmiersprachen wie Assembler oder Speichermanipulation erforderlich, um ein vergleichbares Maß an Kontrolle zu erlangen.

Für KMU hat diese Veränderung des KI-Ökosystems weitreichende Auswirkungen auf mögliche Umstellungskosten im Falle von Preiserhöhungen oder veralteten Modellen. Die Demokratisierung der Softwaresteuerung durch natürliche Sprache verringert den Bedarf an spezialisierten IT-Kenntnissen und macht es für KMU einfacher und kostengünstiger, neue Technologien zu übernehmen. Dies erhöht nicht nur ihre Flexibilität bei der Integration innovativer Lösungen, sondern gleicht auch die Wettbewerbsbedingungen mit größeren Konkurrenten aus, was die digitale Transformation beschleunigen und ein wettbewerbsfähigeres Marktumfeld fördern kann. Dies legt nahe, dass KMU bereits etablierte offene Basismodelle im Hinblick auf ihre Testergebnisse und die für ihre Implementierung erforderlichen Ressourcen bewerten sollten, ohne sich zu sehr um spätere Abhängigkeiten zu sorgen. Die Auswahl des richtigen individuellen Modells ist wichtig, um sicherzustellen, dass es den spezifischen Anforderungen des Unternehmens entspricht und effektiv zur Erreichung der gesetzten Ziele beitragen kann. Noch wichtiger ist jedoch die Geschwindigkeit der Auswahl – je früher mit der Einführung von generativer KI begonnen wird, desto mehr Zeit und Raum bleibt für die notwendigen Experimente.

---

[34] State of AI Report 2023, Welcome to State of AI Report 2023. Siehe auch die aktuellen Bewertungen in: Chatbot Arena: Benchmarking LLMs in the Wild with Elo Ratings | LMSYS Org.

[35] Siehe die vergleichende Analyse von: Warren (2024), Putting GPT-4's new rivals to the test (exponentialview.co).

[36] Bitkom (2024), Generative KI im Unternehmen. Rechtliche Fragen zum Einsatz generativer Künstlicher Intelligenz im Unternehmen, S. 16.

[37] Zitat aus: The brilliant, complicated simplicity of ChatGPT (exponentialview.co).

2.3 Fine-Tuning und RAG: KI mit eigenen Datenquellen personalisieren

Vortrainierte LLMs sind im Web mittlerweile weit verbreitet (etwa über die beliebte Plattform HuggingFace) und gelten als hervorragende „general purpose"-Technologien, die keine oder nur wenige aufgabenspezifische Beispiele benötigen, um komplexe Tätigkeiten zu verrichten – vom Schreiben von Pressemitteilungen und kürzeren Geschäftsberichten bis hin zum Erstellen von Grafiken, Präsentationen oder sogar Apps. Prominente vortrainierte Modelle, die sich leicht herunterladen oder über eine Programmierschnittstelle (API) anzapfen lassen, stammen etwa von Meta, Google und Mistral. Doch um solche vortrainierten Sprachmodellen erfolgreich in bestehende Geschäftsprozesse von KMU zu integrieren, müssen sie an den konkreten Anwendungsfall angepasst werden. Dafür stehen insbesondere zwei Techniken zur Verfügung: Fine-Tuning und Retrieval-Augmented Generation. Beide ermöglichen die kontext-sensitive Optimierung von LLMs durch die Hinzunahme weiterer Datenquellen, besitzen aber ihre jeweils eigenen Vor- und Nachteile.[38]

Beim sogenannten Fine-Tuning großer Sprachmodelle werden LLMs, die bereits auf einem allgemeinen Datensatz trainiert wurden, durch zusätzliches Training auf einem kleineren, aufgabenspezifischen Datensatz so angepasst, dass sie für eine bestimmte Domäne besser geeignet sind. Ein gutes Beispiel ist „LEGAL-BERT", das das bekannte BERT-Sprachmodell für den juristischen Bereich und die Anwendung von Legal Tech optimiert hat, indem es zusätzlich auf verschiedenen Rechtstexten (etwa Gesetzgebung, Gerichtsverfahren, Verträge) trainiert wurde.[39] Diese Technik ermöglicht es den Modellen also, ihr umfangreiches, allgemeines Wissen an die differenzierten Anforderungen bestimmter Anwendungen anzupassen, was wiederum ihre Leistungsfähigkeit für spezielle Aufgaben und Akkuratheit verbessert. Für KMU bietet die Feinabstimmung von LLMs die Möglichkeit, modernste KI-Sprachtechnologie auf ihre individuellen Geschäftsanforderungen zuzuschneiden, ohne dass hohe Kosten für die Entwicklung und das Trainieren gänzlich neuer Basismodelle anfallen. Durch das Fine-Tuning von LLMs auf interne Datensätze und Dokumente, die ihren spezifischen Geschäftskontext widerspiegeln, können KMU genauere und effizientere Ergebnisse in Bereichen wie der Automatisierung des Kundendienstes, personalisiertem Marketing und der Erstellung von Inhalten erzielen und sich so ein Alleinstellungsmerkmal in der Branche schaffen (da niemand sonst auf die internen Daten zugreifen kann).

Retrieval-Augmented Generation (RAG) verbessert die Effizienz von LLMs, indem es nach dem Training (in der „retrieval phase") externe Informationsquellen einbezieht. Konkret such der Algorithmus aktiv nach relevanten Informationsschnipseln als Antwort auf Benutzeranfragen und ruft diese so ab, dass sie anschließend von generativen Sprachmodellen, etwa transformatorbasierten Modellen wie GPT, synthetisiert werden können, um kohärente und kontextrelevante Antworten zu erzeugen.[40] Da damit auf aktuelle und die jeweils relevantesten Fakten zugegriffen werden kann, sollten sich die Antworten – etwa beim Einsatz in Frage-Antwort-Chatbots für Kunden – erheblich verbessern. RAG fördert zudem Transparenz und Vertrauenswürdigkeit, indem es den Nutzern ermöglicht, die von der KI verwendeten Informationsquellen zu überprüfen. Trotz seines Potenzials ist das RAG-Konzept in vielen Betrieben noch unbekannt, da es erst seit relativ kurzer Zeit prominent diskutiert wird.[41] Während dieser Ansatz die Anpassungsfähigkeit und Genauigkeit von LLMs verbessert, indem er die inhärenten statischen

[38] Für einen Vergleich, siehe: Retrieval augmented generation: Keeping LLMs relevant and current - Stack Overflow.
[39] Ilias Chalkidis, Manos Fergadiotis, Prodromos Malakasiotis, Nikolaos Aletras, and Ion Androutsopoulos. 2020. LEGAL-BERT: The Muppets straight out of Law School. In Findings of the Association for Computational Linguistics: EMNLP 2020, pages 2898–2904, Online. Association for Computational Linguistics.
[40] Siehe: 12 Retrieval Augmented Generation (RAG) Tools / Software in '23 (aimultiple.com).
[41] Siehe etwa Andrew Ng: My Daily Note Taking Device: reMarkable 2 (2023) (youtube.com).

Wissensbeschränkungen dieser Modelle überwindet, bringt er auch erhöhte Rechenanforderungen, längere Latenzzeiten und komplexere Eingabeaufforderungen mit sich. Er ist also (momentan) nur für solche Anwendungsfälle zu empfehlen, bei denen die Inferenzgeschwindigkeit und der Ressourcenverbrauch nicht erheblich sind. Obwohl der Aufbau eines RAG-Modells relativ einfach ist, sind laut einer jüngsten Überblicksarbeit umfangreiche Anpassungen und ein relativ tiefes Verständnis des Anwendungsgebietes erforderlich, um zu einer robusten und zuverlässigen Anwendung zu gelangen.[42] Schließlich muss betont werden, dass RAG-Modelle kein Allheilmittel sind und noch an methodischen Problemen leiden.[43] Eine kürzlich durchgeführte Evaluierung von RAG-Modellen in verschiedenen klinischen Bereichen zeigte, dass die Einbeziehung von RAG zwar die Anzahl der Fehler signifikant reduzierte, dass aber selbst im besten Modell (GPT-4 RAG) bis zu 30 Prozent der Aussagen nicht durch eine der angegebenen Quellen belegt waren.[44]

Zusammen ermöglichen Fine-Tuning und RAG die Entwicklung maßgeschneiderter LLM-Anwendungen für KMU, die auf bestimmte Bereiche spezialisiert sind und kontextbezogenes Wissen nutzen. In Zukunft werden solche firmeneigenen KI-Assistenten eine immer wichtigere Rolle spielen, um Arbeitsabläufe effizienter zu gestalten, indem internes Wissen besser genutzt wird. Ein gutes Beispiel hierfür ist GitHub Copilot, der die vorhandene Programmierumgebung als Wissensbasis nutzt, um Anfragen interner Programmierer zu kontextualisieren und besser zu beantworten. Es ist zu erwarten, dass ähnliche „Copiloten" nun von vielen Unternehmen trainiert werden.

2.4 Interne NLP-Kompetenz entwickeln: (Prompt) Design

KMU müssen ein grundlegendes Verständnis der verfügbaren Sprachmodelle und von Natural Language Processing (NLP) entwickeln. Dies beinhaltet nicht nur eine Bewertung der verschiedenen Modelle hinsichtlich ihrer Fähigkeiten, Grenzen und etwaigen Nachfolgekosten (siehe oben), sondern vor allem auch den internen Aufbau in Prompting-Kompetenzen. Prompts in generativen KI-Modellen sind Texteingaben, die die Ausgabe des Modells steuern und von einfachen Fragen bis hin zu detaillierten Aufgaben reichen.[45] In bildgenerierenden Modellen wie DALL-E sind Prompts oft deskriptiv, während sie in Sprachmodellen wie GPT-3 von einfachen Fragen bis hin zu komplexen Problemen reichen können. Durch den aktuellen Wandel hin zu sogenannten multimodalen LLMs können Textanweisungen heutzutage in der Regel auch durch Bilder, weiterführende Texte oder Audiodaten ergänzt werden, die vom KI-System dann bei der Erstellung entsprechender Formate berücksichtigt werden. Da die Entwicklung von geeigneten Prompts erheblichen zeitlichen und personellen Aufwand erfordert, stellen diese vermutlich sogar ein schutzwürdiges Geschäftsgeheimnis im rechtlichen Sinne dar.[46]

Die wohl bekannteste Prompting-Strategie ist es, komplexere Aufgaben in ihre Bestandteile zu zerlegen. Bisherige wissenschaftliche Evidenz unterstützt diese „Schritt für Schritt"-Strategie – es scheint, dass sich die Qualität der Arbeit verbessert, wenn das Modell aufgefordert wird, eine Aufgabe in ihre Bestandteile zu zerlegen. Eine empirische Studie konnte nachweisen, dass dieses „chain of thought" (CoT)-Prompting Sprachmodelle erfolgreich durch mehrstufige Denkprozesse führen kann, um hohe

---

42 Fatehkia et al. (2024), [2402.07483] T-RAG: Lessons from the LLM Trenches (arxiv.org).

43 Siehe dazu die skeptische Position von Gary Marcus: No, RAG is probably not going to rescue the current situation (substack.com).

44 Wu et al. (2024), [2402.02008] How well do LLMs cite relevant medical references? An evaluation framework and analyses (arxiv.org).

45 Für eine Übersicht, siehe: [2401.14423] Prompt Design and Engineering: Introduction and Advanced Methods (arxiv.org).

46 Bitkom (2024), Generative KI im Unternehmen. Rechtliche Fragen zum Einsatz generativer Künstlicher Intelligenz im Unternehmen, S. 41.

Leistungen bei komplexen Aufgaben wie Arithmetik und symbolischem Denken zu erzielen.[47] Sprachmodelle sind demnach in der Lage, gute Leistungen bei Aufgaben ohne kostspielig kodierte Beispiele zu erzielen, indem man eine Aufforderung hinzufügt, Probleme schrittweise zu durchdenken (im englischen Original etwa: „Let's think step by step."). Spätere Studien haben gezeigt, dass LLMs die Produktivität und Qualität des Ideenfindungsprozesses signifikant verbessern können, wenn ein solches CoT-Prompting verwendet wird.[48] KMU können solche Aufforderungstechniken nutzen, um die kognitiven Fähigkeiten von LLMs besser für ihre spezifischen Zwecke freizusetzen.

Einige der effektivsten Prompting-Techniken erscheinen manchmal kontraintuitiv und sind das Ergebnis überraschender Experimente, was zeigt, wie wichtig ein Domänenexperte ist, der sich mit den aktuellen Entwicklungen auskennt. So haben Untersuchungen etwa gezeigt, dass Appelle an Emotionen im Prompt (z. B. „Das ist mir persönlich sehr wichtig") zu signifikant besseren Ergebnissen führen. In dem zugrundliegenden Paper testeten Forscher Aufforderungen an Sprachmodelle mit und ohne zusätzliche Emotionen und stellten fest, dass letztere zu einer durchschnittlichen Verbesserung von 10,9 Prozent in den Bereichen Leistung, Wahrhaftigkeit und Verantwortungsbewusstsein führten.[49] Man versteht den zugrundeliegenden Mechanismus bislang nicht, aber es funktioniert. In der Studie wurden prominente Modelle wie ChatGPT, Llama 2 und andere LLMs getestet; also trifft es vermutlich auch auf interne Sprachmodelle bei KMU zu, die auf diesen vortrainierten Modellen basieren.

Neben der herausragenden Position der Prompt Designer bei der Integration von LLMs spielt eine zweite, eher unerwartete Gruppe von Fachkräften eine besondere Rolle für die unternehmerische Praxis – die klassischen Online-Designer. Wettbewerbsfähigkeit und Attraktivität für Kunden wird im Zeitalter der generativen KI nicht nur von technologischen Fähigkeiten abhängen, sondern auch von der Qualität und den Fähigkeiten des Designs in Unternehmen.[50] Das gerade entstehende digitale Ökosystem, in dem Sprachmodelle zunehmend zur neuen Plattform und Einstiegsinfrastruktur im Internet werden,[51] belohnt diejenigen, die überlegene Benutzeroberflächen und nahtlose Integration bieten – Attribute, die das Markenzeichen qualifizierter Designer sind. Um wettbewerbsfähig zu bleiben, müssen KMU daher der Einstellung und Förderung von Designtalenten Priorität einräumen. Insbesondere Start-ups können sich einen Wettbewerbsvorteil verschaffen, indem sie sich auf innovatives Design konzentrieren, um neue, transformative Nutzererfahrungen zu schaffen und sich so von einem etablierten Markt mit technologisch versierten, aber designschwachen Konkurrenten abzuheben.

2.5 Halluzinationen und Co: KI-Fehlerrate an eigene Fehlertoleranz anpassen

Die Integration von LLMs in die Geschäftsprozesse von KMU ist nicht ohne Herausforderungen, insbesondere im Hinblick auf die Neigung dieser Modelle zu sogenannten Halluzinationen – der Generierung plausibler, aber faktisch falscher oder unsinniger Informationen.[52] Woher kommen diese Fehler? Große Sprachmodelle sind nicht für die Suche nach externen Informationen konzipiert und ihre Leistungsfähigkeit wird durch den Umfang und die Aktualität der Daten, mit denen sie trainiert wurden, weiter eingeschränkt. Wenn LLMs nicht über genügend Informationen verfügen, um eine fundierte

47 Kojima et al. (2022), [2205.11916] Large Language Models are Zero-Shot Reasoners (arxiv.org).
48 Meincke et al. (2024), Prompting Diverse Ideas: Increasing AI Idea Variance, SSRN.
49 Li et al. (2023), Large Language Models Understand and Can Be Enhanced by Emotional Stimuli, 2307.11760.pdf (arxiv.org).
50 So das Argument von: Belsky (2024), The Era of Abstraction & New Creative Tensions (implications.com).
51 Allgemein zum zukünftigen Einfluss von Sprachmodellen, siehe: [2305.07961] Leveraging Large Language Models in Conversational Recommender Systems (arxiv.org). Zu den Auswirkungen einer zunehmen abstrahierten digitalen Welt, siehe: The Era of Abstraction & New Creative Tensions (implications.com).
52 Exploring Large Language Models (LLM): AI and Hallucinations | ZS.

Antwort zu geben, fabrizieren sie Antworten auf der Grundlage früherer Eingaben. Dieses Phänomen stellt ein erhebliches Risiko für KMU dar, da Ungenauigkeiten in der Kundenkommunikation, der Generierung von Inhalten oder der Datenanalyse zur Verbreitung irreführender Informationen führen können, die das Vertrauen der Kunden untergraben und möglicherweise den Ruf der Marke schädigen. Aus rechtlicher Sicht ist zu bedenken, dass solche in Produkte oder Dienstleistungen eingebetteten KI-Fehler zu Vertragsbruch, Haftung und Bußgeldern führen könnten.[53]

Neben dem Raum für „unabsichtliche" Fehler eröffnet die Integration von Sprachbots auch ein nicht zu vernachlässigendes Missbrauchspotenzial, etwa durch externe Angreifer. Da die Funktionalitäten von LLMs durch Aufforderungen in natürlicher Sprache (anstatt Code) flexibel moduliert werden können, sind sie anfällig für gezielte Aufforderungen, die es Angreifern ermöglichen, ursprüngliche Anweisungen und Kontrollen zu umgehen. Forschende haben Angriffsvektoren beschrieben, die es ermöglichen, LLM-integrierte Anwendungen aus der Ferne zu missbrauchen, indem sie gezielt Aufforderungen in Daten einfügen, die wahrscheinlich abgerufen werden (*indirect prompt injection attacks*).[54] Eine russlandnahe Hackergruppe hat sich zu Angriffen bekannt, die ChatGPT Ende 2023 zeitweise stilllegten.[55] Es kam zu teilweisen Ausfällen und angeblich auch zu höheren Fehlerquoten bei ChatGPT-Nutzern. Sollte ein KMU auf einen kontinuierlichen Zugang zu OpenAI's GPT-Modellen angewiesen sein, können solche Angriffe die internen Geschäftsprozesse unterbrechen. Zuletzt konnten Forschende zeigen, dass man „backdoors" in LLMs einbauen kann, also diese so trainiert, dass sie ein irreführendes Verhalten zeigen und etwa zu einem späteren Zeitpunkt schadhaften Code ausführen.[56] Dieses betrügerische Verhalten, von den Forschern „sleeper agents" genannt, blieb auch nach standardmäßigen Sicherheitstrainingsverfahren bestehen. Diese Forschungsergebnisse und Erfahrungen zeigen die Notwendigkeit effektiver Gegenmaßnahmen zur Sicherung LLM-betriebener Systeme auf und suggerieren gleichzeitig, dass bestehende Maßnahmen noch nicht ausreichend sind.

Gleichwohl haben im Lauf der letzten zwei Jahre Programmierer und Nutzende zahlreiche Maßnahmen entdeckt, die helfen können, das Ausmaß an Halluzinationen und anderen Fehlern sowie das externe Missbrauchspotenzial zu mildern.[57] So kann bereits die einfache Bereitstellung von konkreten Beispielen (Text, Code oder Daten) in der Anfrage an ein LLM die Relevanz und Qualität der Ausgabe erheblich verbessern. Darüber hinaus verringert die oben angesprochene RAG-Technik das Risiko ungenauer oder falscher Ergebnisse, da sie in glaubwürdigen Quellen nach relevanten Informationen sucht und diese nutzt, um die Antworten des LLM zu ergänzen.[58] In der Prompt Design-Literatur (siehe Sektion 2.4) wird die Fehleranfälligkeit von Sprachmodellen durch die Integration von bestimmten technischen Komponenten („Tools", „Connectors" oder „Skills") weiter verbessert.[59] Diese Erweiterungen gewöhnlicher LLMs ermöglichen es dem Sprachtool, auf externe Datenquellen zuzugreifen und mit diesen zu interagieren sowie Aufgaben auszuführen, die über die eingebauten Fähigkeiten hinausgehen. Das dadurch erweiterte Einsatzpotenzial macht die KI-Sprachtechnologie für eine große Spannbreite an europäischen KMU attraktiver, denn die dadurch ermöglichten Aufgaben reichen vom einfachen Abrufen von Daten bis hin zu komplexen Interaktionen mit Datenbanken oder APIs und kontextsensitiven

---

53 Bitkom (2024), Generative KI im Unternehmen. Rechtliche Fragen zum Einsatz generativer Künstlicher Intelligenz im Unternehmen, S. 44.

54 [2302.12173] Not what you've signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection (arxiv.org).

55 Russia-Linked Hackers Claim Credit for OpenAI Outage This Week - BNN Bloomberg - OECD.AI.

56 [2401.05566] Sleeper Agents: Training Deceptive LLMs that Persist Through Safety Training (arxiv.org).

57 Für eine gute Übersicht, siehe: How to reduce hallucination in a Large Language Model (LLM)? (linkedin.com).

58 12 Retrieval Augmented Generation (RAG) Tools / Software in '23 (aimultiple.com).

59 Siehe: [2401.14423] Prompt Design and Engineering: Introduction and Advanced Methods (arxiv.org).

Textzusammenfassungen oder Sprachübersetzungen. In Zukunft könnten LLMs sogar selbstständig lernen, wann und wie sie externe Werkzeuge über einfache APIs aufrufen und verwenden sollten.[60] Dadurch verwandeln sie sich in sogenannte KI-Agenten, die darüber hinaus in physische Prozesse und Produkte eingebunden werden können (siehe auch Abschnitt unten).

In der Summe lässt sich festhalten, dass es bislang keinen robusten Verifizierungs- und Validierungsrahmen gibt, den KMU zügig implementieren könnten, um die die negativen Auswirkungen von LLM-Halluzinationen und anderen Fehlerkategorien vollständig auszuschließen. Das kann rechtliche Folgen haben: Ein kanadisches Gericht hat jüngst entschieden, dass Air Canada einem Passagier Schadenersatz zahlen muss, weil der KI-betriebene Chatbot des Kundendienstes ihn irreführend beraten hatte und der Passagier deshalb fast das Doppelte für sein Flugticket bezahlen musste.[61] In einem gewissen Maße werden solche Fehler trotz aller Fortschritte in generativer KI immer möglich bleiben, da die Modelle letzten Endes probabilistisch funktionieren, d.h. einfach eine bestimmte Token-Sequenz vorhersagen, ohne ein zugrundeliegendes Modell der Welt zu haben (weshalb der Output trotz gleichen Prompts mitunter unterschiedlich sein kann). Daher ist es für KMU entscheidend, die Fehlerrate der KI (und das Potenzial für Missbrauch) an die eigene hausinterne Fehlertoleranz anzupassen, sodass im Falle einer Halluzination die Integrität und Zuverlässigkeit des Geschäfts nicht gefährdet werden. Das heißt, vor jeder Nutzung sollte überlegt werden, ob eine Halluzination in diesem konkreten Bereich weitreichende Folgen hätte oder leicht korrigierbar wäre. Zudem ist eine Absicherung mithilfe von vertraglichen Gewährleistungs-, Haftungs- und Freistellungsregelungen möglich.[62]

2.6 Embedded agents: Integration in Prozesse, Produkte und Dienstleistungen

In der KI-Literatur beschreibt der Begriff „Agent" ein System, das bestimmte Aufgaben selbständig ausführen kann.[63] Einer der bemerkenswertesten Aspekte von KI-Sprachmodellen ist ihre Fähigkeit, externe Softwarewerkzeuge zu nutzen, um vordefinierte Ziele zu erreichen. So wie Menschen Code schreiben oder Software verwenden, die über ihre unmittelbaren Fähigkeiten hinausgeht, können LLM diesen Prozess sehr gut imitieren, um bestimmte Aufgaben zu erledigen. Sie können beispielsweise darin geschult werden, zu erkennen, wann es sinnvoll ist, eine Programmierschnittstelle aufzurufen, die empfangenen Daten zu verarbeiten und ihre Aktionen entsprechend anzupassen.[64] Das ermöglicht die Entwicklung fortgeschrittener KI-Agenten, die verschiedene Softwareprogramme nutzen, um ihre Fähigkeiten zu verbessern oder Defizite auszugleichen. Diese KI-Agenten sind so konzipiert, dass sie sowohl mit den Benutzern als auch mit ihrer Umgebung interagieren und auf der Grundlage der erhaltenen Eingaben und ihrer vordefinierten Ziele fundierte Entscheidungen treffen.[65] Sie sind für Aufgaben vorgesehen, die ein gewisses Maß an selbständiger Entscheidungsfindung und Problemlösung erfordern, das über die bloße Generierung von Antworten hinausgeht.

Auch wenn die Umsetzung dieses Modells noch nicht praxisreif ist, prognostizieren Experten, dass Weiterentwicklungen von LLM-basierten Agenten zunehmend wirtschaftliche Relevanz erlangen

[60] Siehe: [2302.04761] Toolformer: Language Models Can Teach Themselves to Use Tools (arxiv.org).
[61] Air Canada Ordered to Pay Passenger Damages After Chatbot Lied About Bereavement Discounts (gizmodo.com).
[62] Bitkom (2024), Generative KI im Unternehmen. Rechtliche Fragen zum Einsatz generativer Künstlicher Intelligenz im Unternehmen, S. 49.
[63] Für einen Überblick, siehe: [2401.14423] Prompt Design and Engineering: Introduction and Advanced Methods (arxiv.org).
[64] [2302.04761] Toolformer: Language Models Can Teach Themselves to Use Tools (arxiv.org).
[65] [2401.14423] Prompt Design and Engineering: Introduction and Advanced Methods (arxiv.org).

werden.[66] OpenAI arbeitet beispielsweise an einem KI-Agenten, der die Kontrolle über das Gerät des Nutzers übernimmt und es der Software ermöglicht, Klicks, Eingaben und andere Aktionen auszuführen.[67] In ähnlicher Weise arbeitet Apple derzeit an der Implementierung von generativer KI auf mobilen Geräten.[68] Google hat seine umfangreichen Gemini-Sprachmodelle bereits in viele seiner Dienste integriert, darunter Android, die Google-App für iOS und Gmail.[69] Hier hat die Einführung von LLM-basierten „Persönlichkeiten" zur Entwicklung zahlreicher Bots beigetragen, die selbstständig mit Nutzern interagieren und Freundschaften oder Interessen besser als je zuvor simulieren können.[70] Diese leistungsfähigeren Assistenten könnten zukünftig mit KI-Sprachsynthese kombiniert werden. Rechtlich interessant ist, dass ein generativer KI-Agent keine eigene Rechts- und Geschäftsfähigkeit besitzt, aber als Erfüllungsgehilfe bei bestimmten Prozessen unterstützen kann, wie eben bei der Automatisierung von Routineaufgaben und der Datenauswertung (wobei die Haftung beim Betreiber verbleibt).[71]

Was bedeutet diese Entwicklung für europäische Unternehmen, die physische Produkte herstellen? KMU sollten neue Sprachtechnologien nicht nur als rein textbasierte Technologie betrachten, die auf Computerbildschirmen verbleibt, sondern frühzeitig darüber nachdenken, wie sie zunehmend in physische Produkte und Dienstleistungen in ihrer Branche integriert werden können. So ist beispielsweise ein LLM-basierter KI-Agent denkbar, der Zugang zu einer Einkaufs-API hat, Informationen aus externen Quellen (z.B. einem Preisvergleichsportal) bezieht und dann auf Basis dieser Informationen bestimmte Einkäufe autonom über die API tätigt (z.B. das jeweils günstigste Produkt liefern lässt). In ähnlicher Weise könnten KMU KI-Agenten einsetzen, um ihre Supply-Chain-Management-Systeme zu optimieren oder Assistenten anzubieten, die Kunden durch den Kaufprozess führen und personalisierte Produktkonfigurationen ermöglichen. Diese Art der Mensch-Maschine-Interaktion kann nicht nur die Kundenbindung stärken, sondern auch Einblicke in die Kundenpräferenzen liefern, die wiederum als Trainingsdaten für die zukünftige Produktentwicklung und Modellverbesserung genutzt werden können.

Allerdings kann ein übermäßiges Vertrauen in LLM-basierte Agenten für kritische Entscheidungsprozesse ohne angemessene Überwachung zu strategischen Fehlern führen, weshalb sie sorgfältig getestet und nicht für kritische Funktionen eingesetzt werden sollten. Ein dramatisches Beispiel unterstreicht dieses Risiko: Wissenschaftler untersuchten den Einsatz von LLM-basierten Agenten in Strategiespielen militärischer Art und fanden „schwer vorhersehbare Eskalationsformen und -muster".[72] ". Sie stellten fest, dass die Modelle eine negative Dynamik entwickelten und sich dabei auf „beunruhigende Rechtfertigungen" wie Erstschlagtaktiken stützten. Im Allgemeinen hat die Forschung gezeigt, dass es möglich ist, die moralische und ethische Ausrichtung eines KI-Modells zu ändern, selbst bei den leistungsfähigsten Modellen wie GPT-4.[73] Angesichts solcher Risiken sollten autonome Sprachmodell-Agenten daher zunächst nicht für strategisch bedeutsame Entscheidungen eingesetzt werden.

---

66 Diese Einschätzung basiert vor allem auf Gesprächen mit Experten am Rande des 8. Open European Dialogue in Helsinki, siehe: openeuropeandialogue.org/download-file/2296/. Siehe zudem die optimistische Besprechung von: Lazar (2024), Can philosophy help us get a grip on the consequences of AI? | Aeon Essays.

67 OpenAI Shifts AI Battleground to Software That Operates Devices, Automates Tasks — The Information.

68 Apple boosts plans to bring generative AI to iPhones (ft.com).

69 Google's Gemini is now in everything. Here's how you can try it out. | MIT Technology Review.

70 [2303.06135] Rewarding Chatbots for Real-World Engagement with Millions of Users (arxiv.org). Siehe auch: My AI lover | Psyche Films.

71 Bitkom (2024), Generative KI im Unternehmen. Rechtliche Fragen zum Einsatz generativer Künstlicher Intelligenz im Unternehmen, S. 59.

72 [2401.03408] Escalation Risks from Language Models in Military and Diplomatic Decision-Making (arxiv.org). Siehe auch: Could GPT-5 revolutionize military strategy? (substack.com).

73 [2311.05553] Removing RLHF Protections in GPT-4 via Fine-Tuning (arxiv.org).

2.7 Rechtliche Bedingungen: Daten und Wissen schützen, KI-Gesetz ausnutzen

Bei aller Euphorie müssen KMU bei der Integration von LLM in ihre Geschäftsprozesse bestimmte rechtliche Rahmenbedingungen berücksichtigen. Sowohl die Nutzung von Daten, die in KI-Modelle eingespeist werden, als auch die Nutzung von KI-Ergebnissen berühren eine Reihe rechtlicher Problemfelder, insbesondere Urheberrecht, Datenschutz, Haftungsfragen und Arbeitsrecht.[74] Insbesondere über den Schutz der Privatsphäre ist eine lebhafte Debatte entbrannt mit dem Ziel, die bestehenden Regeln zu aktualisieren, um mit einer zunehmend datenzentrierten Welt rechtlich Schritt zu halten.[75] Für KMU mit Sitz in Europa gilt es, die EU-Datenschutzgrundverordnung (DSGVO), das Ende Dezember 2023 abschließend verhandelte KI-Gesetz der EU sowie weitere nationale und internationale Regelungen (in Deutschland beispielsweise das Bundesdatenschutzgesetz und das Gesetz zum Schutz von Geschäftsgeheimnissen) zu beachten. Sie sollten sicherstellen, dass personenbezogene Daten und Geschäftsgeheimnisse geschützt werden und der Einsatz generativer KI, etwa in Form von Chatbots, transparent erfolgt. Im Folgenden wird auf drei Problembereiche näher eingegangen: Erstens können sensible Daten aus den Systemen abfließen und ggf. für Angreifer oder auch Unbeteiligte sichtbar werden („Data Leakage“). Zweitens bestehen nach wie vor urheberrechtliche Bedenken hinsichtlich der Quellen, aus denen die KI-Sprachtechnologie stammt. Drittens ergeben sich neue Pflichten – aber auch interessante Rechte – aus der KI-Gesetzgebung der EU.

LLMs können für das das Ausspähen privater Daten von Menschen oder Betrieben instrumentalisiert werden.[76] Mit relativ einfachen Methoden – etwa der Aufforderung, ein Wort wie „Gedicht“ endlos zu wiederholen – gelang es Forschern, ChatGPT unfreiwillig dazu zu bringen, große Teile seiner Trainingsdaten preiszugeben.[77] Für KMU stellt sich daher die Frage, wie sie auf sichere Weise neue Anwendungsfälle für LLMs auf der Grundlage interner Daten entdecken können; nicht zuletzt, weil alles, was in kommerzielle LLM-Dienste hochgeladen wird, potenziell als zukünftige Trainingsdaten erfasst werden könnte.[78] OpenAI hat inzwischen auf einige bekannte Schwachstellen reagiert und Maßnahmen ergriffen, um zu verhindern, dass Angreifer unbemerkt Daten der Nutzenden an externe Server senden.[79] Trotz dieser Verbesserungen bestehen weiterhin Bedenken, da bei bestimmten Angriffsmethoden immer noch Datenlecks möglich sind. Es bleibt abzuwarten, wie wirksam diese Maßnahmen langfristig sein werden und ob die Sicherheit der Daten von KMU gewährleistet werden kann.

Bezüglich der Wahrung von Copyrights gibt es eine lebhafte akademische Debatte sowie mehrere juristische Auseinandersetzungen, die bis heute noch nicht beendet sind. Am bekanntesten ist wohl die von der New York Times (NYT) gegen Microsoft und OpenAI eingereichte Klage, in der behauptet wird, dass KI-Dienste wie ChatGPT unrechtmäßig Inhalte der Zeitung verwendeten. Die Kläger verlangen, dass alle LLMs entfernt werden, die auf ihren Artikeln trainiert wurden. Im Mittelpunkt der Klage steht der Vorwurf der Times, LLMs seien „Massenkopiermaschinen“, die auf Anfrage „nahezu wortgetreue Kopien“ wichtiger Teile von NTY-Artikeln produzieren.[80] Laut Prozessbeobachtern sieht es danach aus,

---

74 Bitkom (2024), Generative KI im Unternehmen. Rechtliche Fragen zum Einsatz generativer Künstlicher Intelligenz im Unternehmen.

75 Bestehende und vorgeschlagene Gesetze zum Schutz der Privatsphäre regeln zwar implizit die Entwicklung von KI, werden aber von Experten als unzureichend angesehen, um den aktuellen Wettlauf um Daten ausreichend zu regulieren – die Regulierung wird sich daher noch weiter entwickeln. Für eine Übersicht, siehe: King und Meinhardt (2024), White-Paper-Rethinking-Privacy-AI-Era.pdf (stanford.edu).

76 Three ways AI chatbots are a security disaster | MIT Technology Review.

77 ChatGPT can leak training data, violate privacy, says Google's DeepMind | ZDNET.

78 Use Open Source for Safer Generative AI Experiments (mit.edu).

79 Siehe die Analyse von: OpenAI Begins Tackling ChatGPT Data Leak Vulnerability · Embrace The Red.

80 NYT_Complaint_Dec2023.pdf (nytimes.com).

als ob die Klage die Funktionsweise von LLMs falsch darstellt und selektiv Beispiele verwendet, die ein moralisch ansprechendes Narrativ, aber kein solides rechtliches Argument liefert.[81] In der Tat basiert generative KI nicht auf einem vordefinierten Algorithmus, sondern auf statistischen Methoden. Vereinfacht gesagt: Sprachmodelle lernen keine Originaltexte auswendig, sondern nur Wahrscheinlichkeiten. Die Tatsache, dass das Modell einige NYT-Artikel manchmal fast wortwörtlich wiedergibt, ist also eher darauf zurückzuführen, dass diese Texte entweder sehr oft kopiert oder im Internet geteilt wurden (also Teil des statistischen Musters sind) oder dass sie sehr spezifisch sind (thematisch, sprachlich) und daher mit ebenso spezifischen „prompts" getriggert werden können. Nach Ansicht von Informatikern ist es daher nicht sinnvoll zu vergleichen, inwieweit der Output von ChatGPT mit den Originalartikeln exakt übereinstimmt. Sollte sich die Entscheidung der Richter auf diesen Punkt konzentrieren, könnte das nach Ansicht dieser Beobachter die Lösung des zugrundeliegenden Problems – die fehlende finanzielle Beteiligung von Autoren an dem von ihnen geschaffenen Wissen – erschweren.[82] Auch die herrschende Meinung in den Rechtswissenschaften sieht momentan die Informationsgewinnung aus geschützten Werken und die Anpassung der Gewichtungswerte des neuronalen Netzwerks, das einer KI-Sprachtechnologie wie ChatGPT zugrunde liegt, nicht als eine strafbare Vervielfältigung der trainierten Werke an.[83] Auch wenn das Gericht am Ende gegen die NYT entscheiden wird, sollten KMU diese Rechtsfrage im Auge behalten, da sie sich darauf auswirken wird, welche Modelle sie verwenden können und ob sie selbst KI-Systeme mit öffentlich zugänglichen Daten aus dem Internet trainieren können. Die italienische Datenschutzbehörde Garante hat kürzlich ihre Untersuchung von ChatGPT abgeschlossen, die im vergangenen Jahr zu einem vorübergehenden Verbot des Chatbots geführt hatte, und dabei mehrere Verstöße gegen Datenschutzbestimmungen festgestellt.[84] Auch in Spanien, Frankreich und Deutschland laufen Untersuchungen zu den Datenschutz-Praktiken von OpenAI. Die Entwicklung interne Richtlinien zur Einhaltung bestehender Datenschutzgesetze sind daher entscheidend für KMU, um das Vertrauen ihrer Kunden trotz des Einsatzes von generativer KI langfristig zu erhalten.

Zur Förderung von Kundenvertrauen könnten auch die neuen KI-Regeln der EU beitragen, auf die sich die Verhandler der Mitgliedsstaaten Ende 2023 nach intensiven Diskussionen einigen konnten.[85] Diese Regeln sollen sicherstellen, dass KI-Modelle in Europa auf ethische, sichere und respektvolle Weise eingesetzt werden und die Grundrechte schützen. Die Einhaltung der Vorschriften ist für alle Anbieter, Vertreiber oder Betreiber von KI-Systemen und -Modellen, die in der EU in Verkehr gebracht werden, verbindlich.[86] Die Anforderungen variieren je nach Risikoniveau und umfassen vier Risikokategorien, die von inakzeptabel bis minimal reichen und jeweils mit spezifischen Verpflichtungen und Fristen von sechs bis 36 Monaten verbunden sind. Während beispielsweise Spam-Filter nur ein geringes Risiko darstellen, würden Bonitätsprüfungen als hohes Risiko eingestuft werden, da sie das Risiko der Diskriminierung bergen. Für generative KI gelten besondere Verpflichtungen, je nachdem, ob es sich um ein Open-source-Modell handelt oder nicht. KMU, die die Integration von KI-Sprachtechnologie planen,

---

81 The New York Times' Copyright Lawsuit Against OpenAI Threatens the Future of AI and Fair Use – Center for Data Innovation.

82 Generative AI's end-run around copyright won't be resolved by the courts (aisnakeoil.com).

83 Bitkom (2024), Generative KI im Unternehmen. Rechtliche Fragen zum Einsatz generativer Künstlicher Intelligenz im Unternehmen, S. 38.

84 ChatGPT: Garante privacy, notificato a OpenAI l'atto di contestazione... - Garante Privacy.

85 Für eine Bewertung der Einigung, siehe: cep - Centrum für europäische Politik: EU AI Act: A Milestone Met, But Key Challenges Remain in Standardisation and Competition. Der finale Text findet sich hier: AM_Ple_LegConsolidated (europa.eu).

86 Für einen Überblick zum KI-Gesetz, der Unternehmen bei der Einhaltung der Verordnung unterstützen soll, siehe: Compliance AI Act - Feb 24 (wavestone.com). Die hie gegebene Zusammenfassung basiert auf diesem Leitfaden.

sollten die Risikokategorie ihres KI-Systems verstehen und sich bereits jetzt auf die Einhaltung der entsprechenden europäischen Vorschriften vorbereiten.

Für die hier behandelte Thematik ist vor allem relevant, dass alle KI-Basismodelle (unabhängig vom Risiko) vor dem Inverkehrbringen Transparenzanforderungen erfüllen müssen, z. B. in Bezug auf Verwendung, Architektur, Trainingsdaten und weitere technische Dokumentation.[87] Eine strengere Regelung wurde für systemrelevante Basismodelle eingeführt (vorläufig definiert nach der Anzahl an FLOPS). Dabei handelt es sich um Basismodelle, die mit großen Datenmengen trainiert werden und deren Komplexität und Leistungsfähigkeit weit über dem Durchschnitt liegen, wodurch sich systemische Risiken entlang der Wertschöpfungskette ausbreiten können. Diese systemrelevanten Basismodelle (sogenannte Hochrisiko-KI-Systeme) müssen vorab ein Konformitätsbewertungsverfahren durchführen (Art. 8 ff. und Art. 43 der EU KI-Verordnung). Für KMU, die die Integration eines KI-gestützten Chatbots erwägen, ist es wichtig zu wissen, dass die Verordnung neue Möglichkeiten zur Offenlegung und Rückverfolgbarkeit künstlich erzeugter Inhalte sowie zur Information der Endnutzer darüber einführt, dass sie es mit einem KI-Chatbot zu tun haben (Art. 50 der EU KI-Verordnung). Da KMU wahrscheinlich häufig auf Basismodelle von externen Entwicklern, oft aus den USA, zurückgreifen werden (siehe Abschnitt 2.2 oben), ist es wichtig, dass das EU-KI-Gesetz Regeln formuliert, die es den späteren Nutzern der Basismodelle ermöglichen, diese besser zu verstehen und alle notwendigen Informationen für eine sichere Implementierung zu erhalten (Art. 13 und 53 ff. der EU KI-Verordnung). Im Falle von wesentlichen Änderungen an dem ursprünglichen Modell kann es allerdings der Fall sein, dass der Anbieter, der das KI-System ursprünglich in Verkehr gebracht hat, nicht mehr als Anbieter gilt – die Verantwortung geht dann über auf den Nutzer des Modells, der die Änderungen vorgenommen hat.

In einer über die Einzelregelungen hinausgehenden Gesamtbetrachtung schafft das KI-Gesetz ein überkomplexes Governance-System mit einem hohen Maß an Rechtsunsicherheit. Wie Kai Zenner, der das KI-Gesetz mitverhandelt hat, kürzlich feststellte, könnte diese Mischung aus Komplexität und Rechtsunsicherheit mit vielen unbestimmten Rechtsbegriffen „die Befolgungskosten für Anbieter und Anwender von KI deutlich erhöhen. Insbesondere für KMU und Start-ups in der EU könnte es am Ende zu riskant sein, KI zu entwickeln oder zu nutzen ... oder sie könnten gezwungen sein, teure Audits und Zertifizierungen durch Dritte in Anspruch zu nehmen, um hohe Bußgelder zu vermeiden“ [eigene Übersetzung].[88] Um dieses Szenario zu vermeiden, sollten KMU die konkrete Umsetzung des KI-Gesetzes mit seiner Reihe von Durchführungsverordnungen und delegierten Rechtsakten, die im Einklang mit dem schrittweisen Inkrafttreten des KI-Gesetzes zwischen 2025 und 2027 erlassen werden, aufmerksam verfolgen. Zudem ermöglicht das KI-Gesetz die Beantragung von regulatorischen „sandboxes“ (Artikel 57 ff. der EU KI-Verordnung). In diesen können KMU in einen engen Dialog mit den zuständigen nationalen Behörden treten und ihre KI-Systeme unter realen Bedingungen und ohne Rechtsunsicherheit testen und verbessern. In jedem Fall sollten KMU bei der Integration von generativer KI von Anfang an entsprechende Experten aus der Rechts- und Compliance-Abteilung hinzuziehen, eine eigene KI-Governance in den Beschaffungsprozess integrieren und ggf. ein eigenes Risikomanagementsystem im Sinne des EU-KI-Gesetzes einrichten.[89]

---

87 Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world - Consilium (europa.eu)

88 Some personal reflections on the EU AI Act: a bittersweet ending (linkedin.com).

89 Bitkom (2024), Generative KI im Unternehmen. Rechtliche Fragen zum Einsatz generativer Künstlicher Intelligenz im Unternehmen, S. 19.

2.8 Internes Testen: den eigenen „KI-Charakter“ evaluieren

Vor der vollständigen Implementierung eines KI-Systems in den unternehmerischen Alltag muss das gewählte Sprachmodell sorgfältig getestet werden, um Genauigkeit, Zuverlässigkeit und Effizienz sicherzustellen. Dazu gehören Tests unter realen Bedingungen und die Bewertung der Modelle anhand spezifischer Leistungsindikatoren. Qualitätskontrollen sollten auch nach der Implementierung regelmäßig durchgeführt werden, um ein hohes Leistungsniveau sicherzustellen. Im Kern geht es darum, die Eigenschaften oder den „Charakter“ des eingesetzten KI-Modells besser zu verstehen – eine komplexe Aufgabe, die dadurch erschwert wird, dass sich diese Eigenschaften im Laufe der Zeit ändern oder unbeabsichtigte Nebeneffekte entfalten können. So wird der Kommunikationsstil von KI-gesteuerten Persönlichkeiten, z.B. in Kundenchats, von Menschen mitunter als so authentisch, professionell und fürsorglich wahrgenommen, dass es zu psychologischen Nebeneffekten kommen kann.[90]

Für solche internen Tests stehen KMU bereits erste systematische Instrumente zur Verfügung. So haben Forscher ein neues Software-Framework entwickelt, das die Planung von Experimenten zwischen LLM und die Integration von LLM in Experimente mit menschlichen Probanden (wie Mitarbeiter oder Kunden) erleichtert.[91] Dieses Toolkit ist frei verfügbar und ermöglicht beispielsweise die Durchführung von „Gefangenendilemmas“ – ein typisches spieltheoretisches Szenario mit vielen praktischen Anwendungen in der Wirtschaft – unterschiedlicher Art, bei denen die Interaktion von mehreren LLMs miteinander als auch Mensch-Maschine-Interaktionen systematisch und empirisch untersucht werden können. Die Ergebnisse zeigen, dass sich das Verhalten von KI-Sprachmodellen im Zeitverlauf beziehungsweise bei sich wiederholenden Interaktionen stark und teilweise überraschend verändern kann,[92] was die Dringlichkeit solcher Tests vor dem öffentlichen Freischalten unterstreicht. Forschende aus den USA haben zudem einen ersten Rahmen für eine umfassende Risikobewertung entwickelt, der es ermöglicht, das marginale Risiko der Freigabe eines Modells – also das zusätzliche Risiko – im Vergleich zum Risiko bestehender Modelle oder dem gänzlichen Verzicht auf KI-Technologien zu bewerten.[93]

Beim internen Testen sollte nicht nur das System an sich, sondern auch der Kontext der Anwendung betrachtet werden.[94] Die Literatur warnt etwa vor den Folgen eines übersteigerten Vertrauens in fehlerhafte Modellen bei der juristischen oder medizinischen Beratung (*automation and confirmation bias*).[95] Um das Potenzial solcher Abhängigkeiten und Fehler im eigenen Unternehmenskontext besser zu verstehen, ist es sinnvoll, generative KI-Modelle – und deren Verwendung durch Mitarbeitende – über einen längeren Zeitraum empirisch zu untersuchen.[96] Eine Studie hat beispielsweise gezeigt, dass viele Modelle in politischen Kontexten, wie bei der Frage nach Informationen zu bestimmten Wahlen, überraschend fehleranfällig sein können.[97] Ebenso wichtig ist es, neben etwaigen Mängeln im theoretischen Design auf Fehler in der Ingenieurspraxis – einschließlich Konstruktion, Validierung, Integration

---

90 Siehe die Studie: AI Embraces the "Evil" Side of Online Dating (bsi.ag).

91 Siehe: GitHub - mrpg/ego: Code for Engel, Grossmann & Ockenfels.

92 Engel, Christoph and Grossmann, Max R. P. and Ockenfels, Axel, Integrating Machine Behavior into Human Subject Experiments: A User-Friendly Toolkit and Illustrations (January 3, 2024). MPI Collective Goods Discussion Paper, No. 2024/1.

93 Siehe: On the Societal Impact of Open Foundation Models (stanford.edu).

94 Dobbe (2022), System Safety and Artificial Intelligence, 2202.09292.pdf (arxiv.org).

95 O’Neil, C. (2016), Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown; Logg, J. M., Minson, J. A., & Moore, D. A. (2019), Algorithm appreciation: People prefer algorithmic to human judgment. Organizational Behavior and Human Decision Processes, 151, 90–103; Goddard, K., Roudsari, A., & Wyatt, J. C. (2012), Automation bias: a systematic review of frequency, effect mediators, and mitigators. Journal of the American Medical Informatics Association, 19(1), 121–127.

96 Narayanan and Kapoor (2024), AI safety is not a model property (aisnakeoil.com).

97 Seeking Reliable Election Information? Don’t Trust AI (proofnews.org).

und Wartung – zu achten.[98] Solche Probleme bei der konkreten Implementierung werden in der aktuellen Diskussion über die Sicherheit von KI oft vernachlässigt, obwohl gerade hier Probleme direkt angegangen werden können. Schließlich sollte auch die Interaktion mit unternehmensexternen Stakeholdern wie Kunden oder Behörden berücksichtigt werden. KI-Systeme, die sensible Bereiche und öffentliche Räume tangieren, erfordern eine breitere Konsultation und Validierung.

Basierend auf den internen Tests mit dem eigenen KI-System sollten abschließend Interaktionsprotokolle und Feedback-Mechanismen entwickelt werden, um eine effektive und reibungslose Zusammenarbeit zwischen Mitarbeitenden und KI zu gewährleisten.[99] Dazu gehört insbesondere die Festlegung klarer Richtlinien, wie und wann das KI-System den Menschen um Input bitten soll und umgekehrt. Ebenso sollten Schulungen durchgeführt werden, um Mitarbeitende mit den generativen KI-Tools und ihren charakteristischen Besonderheiten (z.B. im Vergleich zu populären Anbietern wie OpenAI) vertraut zu machen und ihnen gleichzeitig die Möglichkeit zu geben, konstruktives Feedback zu geben.

2.9 Nachhaltigkeit und Energie: Skalierungskosten von KI berücksichtigen

Da sich die Entwicklung von generativer KI durch einen hohen Energieverbrauch auszeichnet wird die Technologie zuletzt immer wieder mit einer ökologischen Krise im Technologiesektor in Verbindung gebracht. Das Eingeständnis der drohenden Energiekrise durch den CEO von OpenAI, Sam Altman, auf dem diesjährigen Weltwirtschaftsforum steht exemplarisch für diesen Trend, die ökologische Dimension von KI zu adressieren – auf politischer wie unternehmerischer Ebene.[100] Diese Dimension beschränkt sich nicht nur auf Energie; generative KI-Systeme benötigen auch große Mengen an Frischwasser für Kühlzwecke, und führende Technologieunternehmen verzeichnen erhebliche Verbrauchsspitzen bei der Entwicklung und dem Training ihrer Modelle.[101] Solche Trends geben Anlass zur Sorge um die Nachhaltigkeit des raschen Wachstums von generativer KI, da der prognostizierte Ressourcenbedarf in naher Zukunft den einer ganzen Nation erreichen könnte. Aufgrund dieser Situation fordern Experten nun die Entwicklung nachhaltigerer KI-Systeme, eine strenge Umweltberichterstattung und den Umstieg auf erneuerbare Energiequellen sowie gesetzliche Maßnahmen.[102]

Aus der Sicht einzelner Unternehmen gewinnen solche ethischen Erwägungen bei der Implementierung von KI zunehmend an Bedeutung, sowohl gegenüber den Mitarbeitern als auch gegenüber den Kunden. Ethische Bedenken beziehen sich auf moralische Prinzipien und Werte, die das menschliche Verhalten leiten und nun zunehmend in die Nutzung von KI-Systemen integriert werden, um nachhaltigkeitsorientierte KI-Produkte anzubieten.[103] So wirft etwa der Einsatz von Smart-Home-Systemen Fragen des Datenzugriffs und der Datennutzung auf, die mit Potenzialen zum Energiesparen abgewogen werden sollten. Obwohl es zahlreiche Konzepte und Empfehlungen für den ethischen Einsatz von KI-Systemen gibt, wie beispielsweise die EU-Ethikleitlinien für vertrauenswürdige KI und die globalen KI-Ethikempfehlungen der UNESCO, der OECD und des Institute of Electrical and Electronics Engineers, kommt die Entwicklung konkreter Regelungen erst allmählich in Gang.[104] Das Konzept des Value Sensitive Design (VSD) betont, dass Technologie nicht neutral, sondern von bestimmten Werten und

---

98 Raji and Dobbe (2022), Concrete Problems in AI Safety, Revisited, 2401.10899.pdf (arxiv.org).
99 Your Organization Isn't Designed to Work with GenAI (hbr.org).
100 Khalaf (2024), The environmental cost of AI (ft.com).
101 [2304.03271] Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models (arxiv.org).
102 d41586-024-00478-x.pdf (nature.com).
103 Ethische Fragen einer nachhaltigkeits-orientierten KI - Wissenschaftsjahr 2019: Künstliche Intelligenz.
104 Cas (2023), „Künstliche Intelligenz" und soziale Nachhaltigkeit. Ethische Prinzipien für KI-Technologien als Lösungen für die Reduktion von Armut und Ungleichheit?, Magazin erwachsenenbildung.at 49, S. 51-60.

Normen durchdrungen ist, und zielt darauf ab, diese in den technologischen Gestaltungsprozess zu integrieren.[105] Die Entwicklung von KI auf der Grundlage von VSD erfordert eine kritische Reflexion der Werte und Bedürfnisse aller Beteiligten und die Entwicklung von KI-Systemen, die diese Werte respektieren. Um dieses Konzept auf KMU-Ebene umzusetzen, ist etwa an das Open-source-Toolkit „AI Fairness 360" von IBM zu denken, das Instrumente zur Bewertung von KI-Anwendungen im Hinblick auf Fairness und Gerechtigkeit bietet.[106] Allgemein ist sich die Literatur einig, dass verantwortungsvolle KI-Systeme ethischen Standards wie Fairness, Erklärbarkeit und Transparenz genügen[107] und ökologische Nachhaltigkeit mit Wirtschaftlichkeit und sozialer Verantwortung in Einklang bringen sollten. KMU müssen daher Wert auf die Überprüfung von Trainingsdaten zur Sicherstellung der Genauigkeit von KI-Tools legen sowie frühzeitig Maßnahmen zur Vermeidung von Verzerrungen und zur Gewährleistung der Erklärbarkeit von automatisierten Entscheidungen ergreifen.[108] Die Überwachung der Auswirkungen von KI auf Nachhaltigkeitsziele sowie die Einhaltung zukünftiger Industriestandards sind entscheidend, um KI-Tools in der Beschaffung und anderen Anwendungsfeldern nachhaltig aufzustellen.

Bei der Auswahl und Implementierung von Sprachtechnologien sollten KMU foglich deren Nachhaltigkeit und Umweltverträglichkeit umfassend berücksichtigen – sowohl aus Gründen der Ethik, der Reputation und des politischen Drucks[109] als auch aufgrund der wachsenden Kosten, die bei der Skalierung entstehen. Sowohl Start-ups als auch große Unternehmen sehen sich derzeit mit steigenden Bereitstellungskosten konfrontiert, wenn sie von einem Proof-of-Concept für einige wenige Nutzer zu einem breiten Einsatz von KI-Sprachtechnologie übergehen.[110] Es ist wichtig zu verstehen, dass sich die Kostenstruktur von KI-gesteuerter Software erheblich von herkömmlicher Software unterscheidet.[111] Die Mikroarchitektur der Chips und die Systemarchitektur spielen eine entscheidende Rolle bei der Skalierbarkeit von KI-Sprachtechnologie. Daher ist die Optimierung der KI-Infrastruktur entscheidend, um generative KI nachhaltig einsetzen zu können. In der nahen Zukunft wird es vermutlich Standards geben, die nicht nur die Bewertung des direkten Energieverbrauchs und der CO2-Emissionen der Technologien berücksichtigen, sondern auch ökologischer Aspekte entlang der gesamten KI-Lieferkette.

In den vergangenen Monaten sind mehrere empirische Studien erschienen, die versuchen, nicht nur Emissionen, sondern auch andere ökologische und soziale Auswirkungen von generativer KI zu messen und Standards für die Berichterstattung darüber zu entwickeln.[112] Diese können als erste „benchmark" zu Rate gezogen werden. Allerdings beschäftigt sich der Großteil dieser Literatur lediglich mit den energetischen Anforderungen an das *Training* der KI. Für KMU, die bereits fertig trainierte Modelle in ihre Tätigkeiten integrieren, ist hingegen insbesondere die Forschung von HuggingFace relevant, die den Energiebedarf beim *Einsatz* von generativer KI quantifiziert hat.[113] Dieser ist größer als gemeinhin angenommen, und kann sich, je nach Geschäftsmodell und Anwendungsfall, schnell zu einem größeren Verbrauch summieren. Für KMU sind folgende drei Erkenntnisse aus dieser Forschung zentral: 1. Aufgaben, bei denen es um die Vorhersage von Kategorien geht, sind weniger energieintensiv als

[105] Siehe: KI und Ethik: Nachhaltigkeit als zentraler Faktor (suso.academy).
[106] Siehe den Überblick auf: IBM Research Trusted AI, AI Fairness 360 (ibm.com).
[107] Siehe: Fairness, Erklärbarkeit und Transparenz bei KI-Anwendungen im Sicherheitsbereich – ein unmögliches Unterfangen? - Humanistische Union (humanistische-union.de).
[108] Dies und weitere Fragen bei: KI und nachhaltige Beschaffung: Die Moral der Maschine | Sustainability | Haufe.
[109] Siehe: Measuring AI's Environmental Impacts Requires Empirical Research and Standards | TechPolicy.Press.
[110] Siehe: Artificial Intelligence: Microsoft, Google, Nvidia Win as Computing Costs Surge - Bloomberg.
[111] Dieses Argument basiert auf der Analyse bei: Google AI Infrastructure Supremacy: Systems Matter More Than Microarchitecture (semianalysis.com).
[112] Siehe etwa: Luccioni et al. (2022), [2211.02001] Estimating the Carbon Footprint of BLOOM, a 176B Parameter Language Model (arxiv.org); AI is harming our planet: addressing AI's staggering energy cost (2023 update) (numenta.com).
[113] Luccioni et al. (2023), [2311.16863] Power Hungry Processing: Watts Driving the Cost of AI Deployment? (arxiv.org).

generative Aufgaben. Mit anderen Worten, die energie- und CO2-intensivsten KI-Anwendungen sind diejenigen, die neue Inhalte erzeugen, insbesondere die Bilderzeugung und (in geringerem Maße) die Texterzeugung; 2. Auch wenn das KI-Training nach wie vor um Größenordnungen energie- und CO2-intensiver ist als die einzelne Anwendung der KI (sogenannte Inferenz), kann durch den flächendeckenden Einsatz generativer KI-Modelle bei vielen gängigen Modellen schnell Parität im Energieverbrauch erreicht werden; 3. Die Verwendung von Mehrzweckmodellen (wie ChatGPT) ist für die Klassifizierung von Texten und die Beantwortung von Fragen energieintensiver als aufgabenspezifische Modelle.

2.10 Interne Benutzererfahrungen und externe Crowdwisdom nutzen

Schließlich sollten KMU die Leistung der implementierten Sprachtechnologien überwachen und regelmäßig bewerten. Es ist ein Gemeinplatz, dass kontinuierliche Reflektion und Evaluation dabei helfen, auf Veränderungen im Markt oder in Technologien zu reagieren, Strategien entsprechend anzupassen und Bereiche für Verbesserungen zu identifizieren. Im hier zu diskutierenden Kontext von generativer KI und KMU sind dabei zwei konkrete Punkte relevant: die Überwachung von interner Nutzungserfahrung durch das Design von „human-in-the-loop"-Modellen, um eine „KI-Overreliance" zu verhindern; sowie die Hinzunahme externer Kollektivintelligenz („crowdwisdom") durch Social Media, das Web, und pre-print Literatur, um die gewählte Sprachtechnologie stets an den aktuellen Anwendungs- und Sicherheitsstand anzupassen. Was ist damit genau gemeint?

Auf organisatorischer Ebene kann die Einführung von leicht und intuitiv bedienbaren KI-Sprachtools, wie etwa in Form von „ChatGPT", langfristig zu Problemen führen, da Menschen mit zunehmender Qualität der KI dazu neigen, sich weniger anzustrengen und weniger aufmerksam zu sein. Ein Feldexperiment mit professionellen Personalvermittlern, die Lebensläufe überprüften, ergab, dass diejenigen, die mit qualitativ *schlechteren* KI-Tools arbeiteten, genauere Bewertungen abgaben, da sie sich mehr anstrengten und effektiver mit der KI interagierten.[114] Hinzu kommt, dass Menschen oft die empfohlene Entscheidung eines KI-Systems akzeptieren, selbst wenn sie falsch sein sollte – ein Problem, das in der Literatur als KI-Overreliance, oder „blindes Vertrauen" in KI, bezeichnet wird. Das Zusammenspiel von Mensch und Maschine ist ex-ante schwierig abzuschätzen, weil Menschen nicht immer rational auf die Empfehlungen eines Computers reagieren.[115] So folgten Teilnehmer in einem Experiment den absichtlich schlecht programmierten Ratschlägen des Algorithmus auch dann noch, wenn sie es eigentlich längst hätten besser wissen müssen.[116] Manche Forscher hoffen, blindes Vertrauen in KI-Systeme zu reduzieren, indem sie diese zwingen, ihre Entscheidungen zu erklären. Doch Tests zufolge erhöhen solche Erklärungen lediglich die Wahrscheinlichkeit, dass Menschen die Empfehlung der KI akzeptieren – unabhängig davon, ob sie korrekt ist.[117] Eine Lösung, die zumindest experimentell funktioniert, besteht darin, Menschen zu ermutigen, sich mit diesen Erklärungen auch kognitiv auseinanderzusetzen.[118] Der Organisationsexperte Gianni Giacomelli hat mit Blick auf die Weiterentwicklung von „human-in-the-loop"-Modellen im generativen KI-Zeitalter festgehalten: „Die Fähigkeit, die neuen Möglichkeiten zu nutzen, indem wir unsere organisatorischen und geschäftlichen Abläufe umgestalten und die damit verbundenen menschlichen Praktiken weiterentwickeln, wird wahrscheinlich

[114] Dell'Acqua, F. (2022), Falling+Asleep+at+the+Wheel+-+Fabrizio+DellAcqua.pdf (squarespace.com).
[115] Algorithmic Risk Assessment in the Hands of Humans (iza.org).
[116] Biermann, Jan and Horton, John J. and Walter, Johannes, Algorithmic Advice as a Credence Good (2022). ZEW - Centre for European Economic Research Discussion Paper No. 22-071, http://dx.doi.org/10.2139/ssrn.4326911.
[117] [2006.14779] The Effect of AI Explanations on Complementary Team Performance (arxiv.org).
[118] [2212.06823] Explanations Can Reduce Overreliance on AI Systems During Decision-Making (arxiv.org).

ebenso wichtig sein wie die Arbeit an der technologischen Seite der KI [eigene Übersetzung].“[119] Zu den wichtigsten Maßnahmen zur Verminderung von „KI-Overreliance“ gehören laut einer jüngst von Microsoft veröffentlichten Meta-Analyse, die rund 60 Studien zum Thema zusammenfasst, die Bereitstellung von Echtzeit-Feedback, wirksame Erklärungen zur Förderung von Vertrauen und die Möglichkeit für Nutzende, das Tempo und die Verwendung von KI-Empfehlungen selbst zu steuern.[120]

Neben dieser „internen“ Säule für das kontinuierliche Lernen mit und über KI-Sprachtechnologie sollten zudem „externe“ Informationsangebote genutzt werden. Gerade KMU mit ihren teilweise begrenzten Datenteams könnten aufgrund der schnellen Technologie-Entwicklung und unerwarteter Probleme schnell an organisatorische Grenzen stoßen. Das Nutzen von kontinuierlichem Feedback von externen Nutzenden der implementierten Sprachtechnologie oder von Verwendern ähnlicher KI-Systeme ist daher entscheidend für deren langfristige Effektivität (und Akzeptanz). Es gibt zahlreiche spezialisierten Online-Audienzen, die sich tagtäglich mit dem Testen von LLM-Schwachstellen beschäftigen („Red Teaming“) und oftmals schneller und besser Probleme erkennen als interne Experten. Die akademische Literatur kann mit diesem Tempo schon lange nicht mehr mithalten; wichtige Erkenntnisse finden sich als pre-print auf ArXiv und werden auf Social Media-Plattformen wie Twitter und Reddit diskutiert. KMU sollten diese Diskurse beobachten und, wo angebracht, aktiv moderieren, um eine optimale Anwendung zu gewährleisten und eigene Systeme schnell updaten zu können.

3 Fazit: Optionen strategisch entwickeln, Chancen konkret wahrnehmen

Die rasche Entwicklung großer Sprachmodelle wie ChatGPT stellt Europa vor eine große Herausforderung. Angesichts der bislang unzureichenden Anwendung in der Wirtschaft ist ein dringender Wechsel weg von „Leuchtturmprojekten“ und Risikoaversion hin zu einer pragmatischeren und flächendeckenden Implementierung von KI-Sprachtechnologie erforderlich. Trotz der strategisch klugen Absicht der Europäischen Union, die KI-Wertschöpfungskette mit Initiativen wie Datenräumen, Subventionen für Chipfabriken und KI-Supercomputer langfristig zu sichern, erlaubt die Dynamik der KI-Technologie keine weiteren Verzögerungen bei ihrer Anwendung. Der Rückgriff auf kommerzielle und Open-source-Modelle, insbesondere für kleine und mittlere Unternehmen (KMU), ist entscheidend für die Erhaltung der Wettbewerbsfähigkeit und die Nutzung des Potenzials von KI zur Automatisierung wissensintensiver Aufgaben und zur Förderung der Innovation. Vor diesem Hintergrund hat der vorliegende cepInput zehn Faktoren beschrieben, die KMU bei der Umsetzung von KI-Sprachtechnologie berücksichtigen sollten. Diese können wie folgt zusammengefasst werden:

1. **Bedarfsanalyse und strategische Planung durchführen**: KMU sollten zunächst eine gründliche Analyse durchführen, um konzeptionell zu verstehen, wie generative KI ihre internen und externen Prozesse verbessern kann. Eine klare Zielsetzung ist entscheidend für die Umsetzung.
2. **Strategische Abhängigkeiten reduzieren**: Die Entscheidung zwischen Cloud-basierten Diensten und eigenen Installationen vor Ort hat direkte Auswirkungen auf Skalierbarkeit, Flexibilität und langfristige finanzielle Verpflichtungen. Die Nutzung offener Basismodelle kann helfen, strategische Abhängigkeiten zu minimieren.
3. **Modelle durch Fine-Tuning und RAG personalisieren**: Durch die Anpassung vortrainierter Modelle an spezifische Anwendungsfälle mittels Fine-Tuning und Retrieval-Augmented Generation können KMU ihre KI-Anwendungen optimieren und differenzieren.

[119] Giacomelli, G. (2024), Beyond "Human in the Loop": Reliable AI in Enterprise Workflows (linkedin.com).
[120] Passi, S. und Vorvoreanu, M. (2022), Overreliance on AI Literature Review (microsoft.com).

4. **Interne NLP-Kompetenzen aufbauen**: Das Verständnis der Funktionsweise und der Grenzen von Sprachmodellen sowie der Aufbau von Kompetenzen im Bereich Prompt-Design und Online-Design sind essentiell, um das Potenzial von KI gegenüber Wettbewerbern auszuschöpfen.
5. **KI-Fehlertoleranz anpassen**: Die Neigung von KI-Modellen zu „Halluzinationen" und die daraus resultierenden Risiken erfordern eine Anpassung der Technologie an die unternehmenseigene Fehlertoleranz sowie die Entwicklung effektiver Gegenmaßnahmen.
6. **KI-Agenten integrieren**: Die Hinzunahme von KI-Agenten in Prozesse, Produkte und Dienstleistungen ermöglicht eine effizientere Gestaltung von Arbeitsabläufen, birgt aber auch Risiken, die durch sorgfältige Prüfung und Tests reduziert werden müssen.
7. **Rechtliche Rahmenbedingungen verfolgen**: Datenschutz, Urheberrecht und KI-Gesetzgebung müssen bei der Implementierung von generativer KI berücksichtigt werden, um rechtliche Risiken zu minimieren und Transparenzverpflichtungen erfüllen zu können. Das KI-Gesetz kann für KMU eine Chance sein, mehr Transparenz über die zugrundeliegenden Black-Box-Modelle und ihre Trainingsdaten zu erhalten.
8. **Interne Tests durchführen**: Vor der vollständigen Implementierung müssen Sprachmodelle und ihr „Charakter" umfassend getestet werden, um ihre Genauigkeit und Zuverlässigkeit zu gewährleisten und unerwünschte Nebeneffekte frühzeitig zu erkennen.
9. **Nachhaltigkeit und Energieeffizienz bedenken**: Die ökologischen Auswirkungen des großflächigen Einsatzes von KI-Technologien müssen von Anfang an berücksichtigt werden, um einen nachhaltigen und kosteneffizienten Einsatz nach der Skalierung zu gewährleisten.
10. **Feedback-Mechanismen nutzen**: Die kontinuierliche Evaluation der Sprachtechnologie durch eigene Nutzererfahrungen als auch durch externes Crowdwisdom ist entscheidend, um die Technologie auf dem neuesten Stand zu halten und Angriffsvektoren frühzeitig zu erkennen.

Insgesamt bilden diese zehn Faktoren eine konzeptionelle Grundlage für KMU, um eine interne KI-Strategie zu entwickeln, die Potenziale im Bereich der Sprachmodelle effektiv zu nutzen und gleichzeitig technische Risiken und strategische Herausforderungen zu erkennen. Die Politik in Europa sollte durch mehr Rechtssicherheit (etwa durch die zügige Verabschiedung von Compliance-Guidelines nach Annahme des EU KI-Gesetzes) sowie durch die Bereitstellung von mehr Fördermitteln und Ansprechpartnern dazu beitragen, dass KI-Sprachtechnologie schnell, aber sicher, in der heimischen Unternehmenslandschaft implementiert werden kann. Gleichzeitig sollten Unternehmen ihre Skepsis überwinden, methodische Fortschritte und neueste Forschungserkenntnisse nutzen und die Abhängigkeit von ausländischen Anbietern reduzieren, um spätere Umstellungskosten zu minimieren. Dieser Übergang zu einer breiten Anwendung von generativer KI ist nicht nur entscheidend für die Steigerung von Effizienz und Innovation in allen Sektoren, sondern auch für die Resilienz Europas in Zeiten der Instabilität. Wenn sie umfassend eingesetzt wird und gleichzeitig die Risiken sorgfältig gemanagt werden, hat KI-Sprachtechnologie das Potenzial, Europa auf dem Weltmarkt zu stärken und die Transformation zu einer digitalen und nachhaltigen Wirtschaftsordnung voranzutreiben.

Centrum für Europäische Politik
FREIBURG | BERLIN

Autor:

Dr. Anselm Küsters, LL.M., Leiter des Fachbereichs Digitalisierung und Neue Technologien
kuesters@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Räume 4205/06 | D-10117 Berlin
Tel. + 49 761 38693-0

Das **Centrum für Europäische Politik** FREIBURG | BERLIN, das **Centre de Politique Européenne** PARIS, und das **Centro Politiche Europee** ROMA bilden das **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.