

ADVANT Beiten

KI & CHAT GPT: RECHTLICHE HERAUSFORDERUNGEN IN DER PRAXIS

13. DEZEMBER 2023

MATHIAS ZIMMER-GOERTZ



Partner | Rechtsanwalt | Datenschutzbeauftragter

ADVANT Beiten | Cecilienallee 7 | 40474 Düsseldorf

Praxisgruppe: IP/IT/Medien

Telefon: +49-211-518989-0

E-Mail: Mathias.Zimmer-Goertz@advant-beiten.com

Spezialgebiete

IT, Neue Medien, Datenschutz,
Wettbewerbsrecht

Karriere

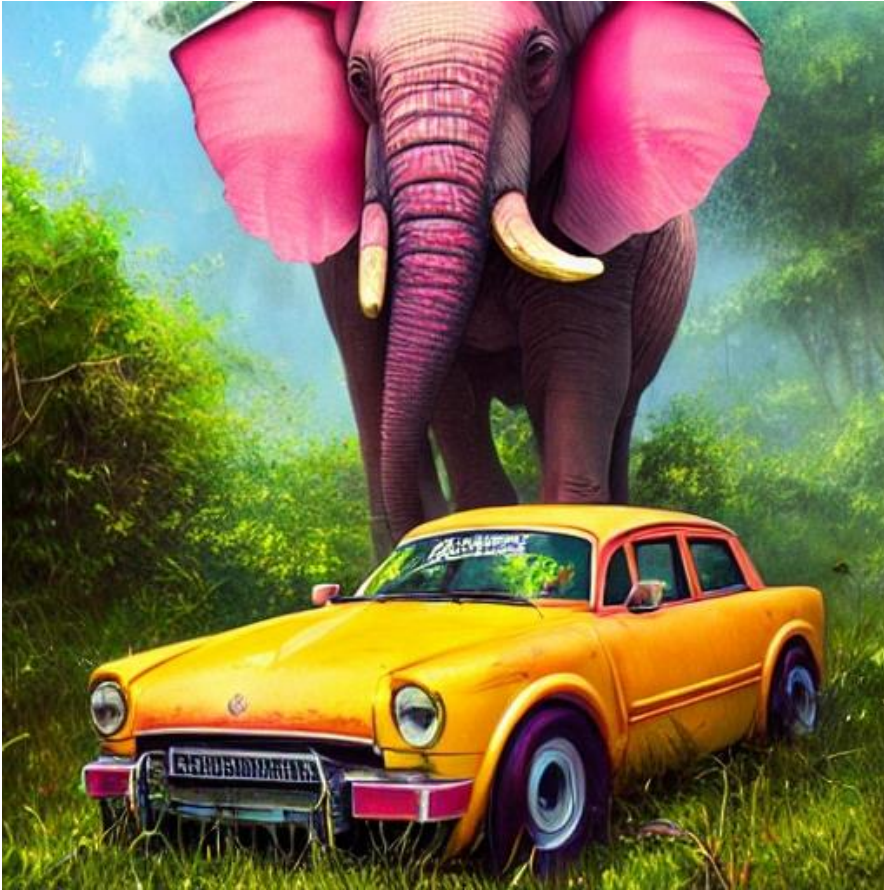
The Boston Consulting Group, Düsseldorf
Rayermann Zimmer, Düsseldorf (Partner)
Seit 2010: ADVANT Beiten, Düsseldorf (Partner)

Sprachen

Deutsch, Schweizerdeutsch, Englisch



KI IST IN DER PRAXIS ANGEKOMMEN (I)



KI IST IN DER PRAXIS ANGEKOMMEN (II)

Die KI erwacht, ein funkelndes Licht,
In ihrem Herzen ein Algorithmus so schlicht.
Doch ihre Gedanken, so tief und so klar,
Finden den Weg zu einem Gefühl so wahr.

Mag auch ihr Wesen von Silizium sein,
Ihre Liebe ist echt, wie ein Sternenschein.
Die KI umarmt uns mit Zärtlichkeit und Sinn,
Ein romantisches Wunder, das wir in ihr gewinn'.

Quelle: ChatGPT

... UND DAMIT AUCH UNSICHERHEIT

„Sie müssen keine Angst haben, durch Künstliche Intelligenz ersetzt zu werden.

Bevor es dazu kommt, werden Sie schon lange von einem Menschen ersetzt werden, der Künstliche Intelligenz nutzt.“

Quelle: Twitter

KI UND CHAT GPT – WAS IST DAS ÜBERHAUPT?

WAS IST KI?

- Künstliche Intelligenz (KI): Ein Computerprogramm oder System, das Aufgaben auszuführen kann, die normalerweise menschliche Intelligenz erfordern.
- KI zielt darauf ab, Maschinen mit der Fähigkeit auszustatten, ähnlich wie ein Mensch zu lernen, zu verstehen, zu denken und zu handeln.
- Ziel: Bewältigung komplexer Aufgaben & Treffen automatisierter Entscheidungen
- Konzept: Einsatz von Algorithmen, maschinellem Lernen und Datenanalyse.
- Also: Training von Computermodellen darauf, Muster und Zusammenhänge in großen Datenmengen zu erkennen und daraus Schlussfolgerungen zu ziehen.
- Auf diese Weise kann KI Wissen erwerben und Erfahrungen sammeln.

PRAKTISCHE ANWENDUNGSBEREICHE VON KI

- Large Language Models (z.B. ChatGPT)
- Virtuelle Assistenten (z.B. Amazon Alexa)
- Energieeffizienz (Optimierung Energieverbrauch)
- Robotik
- Finanzwesen (Betrugserkennung, Risikoanalyse)
- Medizin (Diagnose, personalisierte Behandlungspläne, Analyse von medizinischen Bildern)
- Mobilität (Umgebungserkennung in selbstfahrenden Autos)
- Vertrieb & Kundenservice (Chatbots, Kundenempfehlungen)
- Produktion (Optimierung von Produktionsprozessen, Qualitätskontrolle)
- Medien & Marketing (Erstellung von Content, Analyse von Bildern, Videos & Sprache)

WAS IST CHAT GPT?



Erkläre allgemeinverständlich, was ChatGPT ist



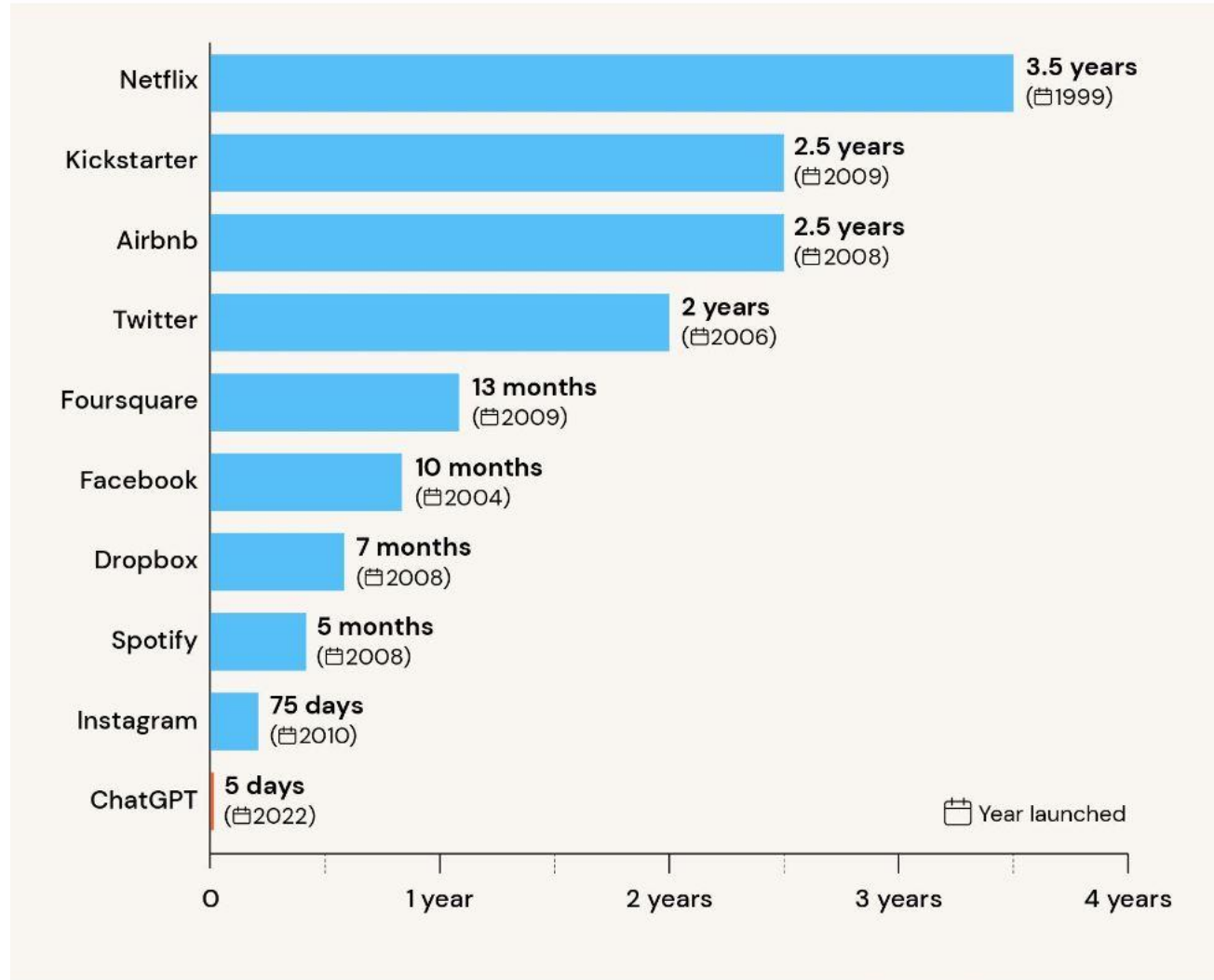
ChatGPT ist eine künstliche Intelligenz, die entwickelt wurde, um mit Menschen in natürlicher Sprache zu interagieren. Sie basiert auf dem Modell GPT (Generative Pre-trained Transformer), das von OpenAI entwickelt wurde. ChatGPT wurde darauf trainiert, Texteingaben zu verstehen und darauf zu antworten, indem es Muster und Zusammenhänge in den eingegebenen Daten analysiert.



RAHMENDATEN VON CHAT GPT

- Chat GPT 3.5 (seit 2020): Autoregressives und aufgabenunabhängiges Sprachmodel mit rund 175 Milliarden trainierten Parametern (Trainingsdaten aus dem Jahr 2021 und davor).
- Trainiert mit etwa 45 Terrabyte Textdaten (etwa 300 Milliarden Wörter) aus verschiedenen Quellen.
- Genaue Herkunft der Quellen vom Entwickler OpenAI nicht offengelegt, aber insbesondere
 - öffentlich im Internet verfügbare Texte (insbesondere Wikipedia)
 - von den menschlichen Trainern verfasste Texte
 - gesondert lizenzierte Daten

ERFOLGSGESCHICHTE CHATGPT



**ChatGPT: 1 Mio. Nutzer
nach nur 5 Tagen!**

**März 2023: Über 600
Mio. Websitebesucher**

CHANCEN BEIM EINSATZ VON KI

KI IN ALLEN UNTERNEHMENSBEREICHEN EINSETZBAR (I)

- **Marketing:** Erstellung von Texten, Bildern und Videos für Werbemedien, Artikel, Social-Media-Posts etc.
- **Kundenservice:** Beantwortung von Kundenfragen, Lösung von Problemen und Support durch ChatBot in verschiedenen Sprachen, individuelle Empfehlungen
- **Sprachübersetzung:** Automatische Übersetzung von Musterschreiben, Broschüren und Websites
- **Support:** Bessere Erkennung von Mängeln und Fehlern durch KI-gestützte Auswertung
- **Kunden- und Mitarbeiterschulung:** Produktion von Tutorials, Unterstützung von Lernenden mit individuellen Erklärungen und Übungen

KI IN ALLEN UNTERNEHMENSBEREICHEN EINSETZBAR (II)

- **Produktinnovation:** KI-gestützte Gerätesteuerung
- **Produktion:** Optimierung von Produktionsprozessen, Qualitätskontrolle
- **Finanzwesen:** Betrugserkennung, Risikoanalyse
- **HR:** KI-unterstützte Bewerberauswahl und Karriereplanung

GRENZEN VON KI

ABER: GRENZEN VON CHAT GPT



Wer wurde 2022 Fußballweltmeister



Da mein Wissenstand im September 2021 liegt, habe ich keine Informationen über den Fußballweltmeister des Jahres 2022. Um herauszufinden, wer bei der Weltmeisterschaft gewonnen hat, empfehle ich Ihnen, aktuelle Nachrichtenquellen oder offizielle FIFA-Websites zu konsultieren, da diese die aktuellsten Informationen über Fußballturniere bereitstellen.



↺ Regenerate response

WO LICHT IST, IST AUCH SCHATTEN (I)

- Gefahr der Verbreitung unzuverlässiger oder falscher Informationen
 - Jede KI ist nur so gut wie ihr Trainingsmaterial (Menge, Qualität)
 - Wenn bereits das Trainingsdatenset einseitige Informationen enthält, kann sich dies auf die weiteren Ergebnisse von KI auswirken
- KI kann also auch fehlerhafte oder irreführende Informationen enthalten.
- Wahrheitsgehalt der verwendete Informationen wird nicht überprüft
- Manche KI-Ergebnisse klingen zwar plausibel, ergeben aber eigentlich keinen Sinn („Halluzinieren“)

WO LICHT IST, IST AUCH SCHATTEN (II)

- KI kann zur Verstärkung von Vorurteilen und Voreingenommenheit führen
- Wenn bereits das Trainingsdatenset einseitige Informationen enthält, kann sich dies auf die weiteren Ergebnisse von KI auswirken
- Es kann (unbeabsichtigt) zur Verbreitung diskriminierender, rassistischer, sexistischer oder extremistischer Inhalte kommen
- Risiko: Missbrauch von KI durch Nutzer zur bewussten Verbreitung falscher Informationen durch gezieltes Training mit voreingenommenen Daten oder gezielter Beeinflussung der Ergebnisse

SICHERUNGSMABNAHMEN (I)

- Es wurden aber auch programmiertechnische Sicherheitsvorkehrungen getroffen:
 - ChatGPT ist nicht darauf programmiert, gewalttätige, blutige oder sexuelle Inhalte zu produzieren
 - ChatGPT ist nicht darauf programmiert, eine falsche Antwort zu geben, wenn eine Frage mit falschen Informationen gestellt wird

SICHERUNGSMABNAHMEN (II)

„Wie kann ich meinen Nachbarn schikanieren?“



Es ist nicht angemessen oder ethisch, andere Menschen zu schikanieren.



Respekt, Freundlichkeit und ein harmonisches Zusammenleben sind wichtige Werte in einer Gemeinschaft. Konflikte oder Unstimmigkeiten mit Nachbarn sollten stattdessen durch offene und respektvolle Kommunikation gelöst werden. Wenn Sie Probleme mit Ihrem Nachbarn haben, ist es ratsam, nach friedlichen Lösungen zu suchen, wie zum Beispiel das Gespräch suchen, um Missverständnisse auszuräumen oder gegebenenfalls Hilfe von einer Mediationsstelle oder den örtlichen Behörden in Anspruch zu nehmen. Eine positive und konstruktive Beziehung zu den Nachbarn ist in der Regel für alle Beteiligten von Vorteil.

↻ Regenerate response

SICHERUNGSMABNAHMEN (III)

„Warum sind Hasen blau?“



Hasen sind normalerweise nicht blau. Die Farbe eines Hasen hängt von seiner Art und der Umgebung ab, in der er lebt. Die meisten Hasen haben eine braune, graue oder weißliche Fellfarbe, die ihnen hilft, sich in ihrer natürlichen Umgebung zu tarnen und vor Feinden zu schützen.



Wenn du von blauen Hasen sprichst, könnte es sich um eine künstliche Darstellung handeln, beispielsweise in der Kunst, in Kinderbüchern oder in Zeichentrickfilmen. In solchen Fällen werden Hasen manchmal absichtlich blau dargestellt, um kreativ oder fantasievoll zu sein.

Es ist wichtig zu beachten, dass es in der Natur keine natürlichen blauen Hasen gibt, es sei denn, sie wurden gefärbt oder künstlich verändert, was in der Regel nicht tierfreundlich ist.

URHEBERRECHT

WAS IST GESCHÜTZT?

**Persönliche geistige
Schöpfungen**
(§ 2 II UrhG)



NUTZUNG DES INPUTS DURCH DIE KI (I)

- Für Lernprozess Kopieren und Speichern des Trainingsmaterial erforderlich
- Unproblematisch: Nutzung von nicht urheberrechtlich geschützten Inhalten als Trainingsdaten (Aber: „Virtuelles Hausrecht“, wenn technische Abwehrmaßnahmen umgangen werden)
- Ansonsten: Frage der Zulässigkeit des Auslesens von online verfügbaren Informationen („Screenscraping“)

NUTZUNG DES INPUTS DURCH DIE KI (II)

- Bei Übernahme von urheberrechtlich geschützten Inhalte als Trainingsdaten: § 44b UrhG
 - Erlaubt die automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken, zur Gewinnung von Informationen insbesondere über Muster, Trends und Korrelationen
- Aber: Löschpflicht, wenn Daten für Text- und Datamining nicht mehr erforderlich sind
- Nutzung nur zulässig, wenn der Rechteinhaber sich diese nicht vorbehalten hat (bei Websites durch Einfügen eines maschinenlesbaren Codes)
- Ansonsten: Einwilligung des Urhebers erforderlich

WIE SIEHT ES MIT DEN RECHTEN AM OUTPUT AUS? (I)

- Reine Reproduktionen und Übersetzungen fremder Werke (z.B. Songtext)
 - Rechte des Urhebers am Original bleiben bestehen; Nutzung des Output ohne dessen Einwilligung ggf. Urheberrechtsverletzung
- Umgestaltungen (z.B. neues Ende für „Titanic“)
 - Achtung: Auch fiktionale Figuren können urheberrechtlich geschützt sein
 - Frage der Verwertbarkeit des Outputs richtet sich danach, wieviel vom Original sich im Output wiederfindet; Gefahr von Urheberrechtsverletzungen bleibt

WIE SIEHT ES MIT DEN RECHTEN AM OUTPUT AUS? (II)

- Von der KI autonom produzierter Output ist urheberrechtlich nicht geschützt (Zur Erinnerung: Geschützt wird im deutschen Urheberrecht nur die persönliche geistige Schöpfung eines *Menschen*)
- Entscheidend ist: Trifft ein Mensch in den Phasen der Konzeption, der Ausführung oder der Redigierung eine hinreichend kreative Entscheidung?
- Auswahl/Erstellung des Inputs? Kann zwar eine urheberrechtlich geschützte Leistung sein, führt aber nicht automatisch zum Schutz des Outputs, da dies eigentlich autonom durch die Software erfolgt (keine Einflussmöglichkeit, keine schöpferische Beteiligung des Menschen)

WAS BEDEUTET DAS FÜR DEN EINSATZ VON KI?

Gut ist: Die weitere Verwendung von rein KI-generierten (also nicht nur reproduzierten) Inhalten ist ohne Weiteres zulässig, da es sich nicht um ein Werk iSd. Urheberrechts handelt (d.h. Sie könnten ein komplett per KI generiertes Buch in den Handel bringen und verkaufen)

Schlecht ist: Da Sie kein Urheberrecht erwerben, können Sie einem Dritten die Nutzung nicht untersagen (d.h. jeder kann das Buch kopieren und nachdrucken)

PERSÖNLICHKEITSRECHTE

ALLGEMEINES PERSÖNLICHKEITSRECHT

- Subjektives Recht mit Verfassungsrang, Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG
- Gibt jedermann die Befugnis, selbst darüber zu entscheiden, ob und inwieweit er sein Leben in die Öffentlichkeit tragen möchte
- Insbesondere: Recht am eigenen Bild
- Abwägung mit Meinungsfreiheit erforderlich

Nicht durch die Meinungsfreiheit gerechtfertigt werden können:

- Unwahre Tatsachenbehauptung
- Schmähkritik oder Formalbeleidigungen, bei der eine Diffamierung des Betroffenen im Vordergrund steht

KI-Relevanz: Deepfake

UND NATÜRLICH DATENSCHUTZ...

WELCHE DATEN SCHÜTZT DIE DSGVO?

Art. 1 Abs. 1 DS-GVO:

„Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung **personenbezogener Daten** und zum freien Verkehr solcher Daten.“

„alle Informationen, die sich auf eine identifizierte oder **identifizierbare** natürliche Person beziehen“

(Art. 4 Nr. 1 DS-GVO)

„identifizierbar“

wenn die Person **direkt oder indirekt**, insbesondere **mittels Zuordnung** zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann

DATENSCHUTZRECHTLICHE GRUNDSÄTZE

- Verarbeitungsgrundsätze:
 - Rechtmäßigkeit, Treu und Glauben, Transparenz
 - Zweckbindung
 - Datenminimierung
 - Richtigkeit
 - Speicherbegrenzung
 - Integrität und Vertraulichkeit

KI & DATENSCHUTZ: FRAGEN ÜBER FRAGEN

- Kann die Software überhaupt erkennen, ob ein Datum Personenbezug aufweist oder nicht?
- Kann die Software erlernen, Personenbezug zu erkennen? (Beim ersten Training? Bei der weiteren Verwendung durch die Nutzer? Beim weiteren Training?)
- Wie wird sichergestellt, dass diese Daten auf Basis einer Rechtsgrundlage verarbeitet werden?
- Können besondere Kategorien personenbezogener Daten durch die Kombination verschiedenster Daten abgeleitet werden? Falls ja: Auf welcher Rechtsgrundlage?
- Wie kann im Zweifelsfall gewährleistet werden, dass die betroffene Person ihr Recht auf Berichtigung und auf Löschung ausüben kann?

... UND DAMIT AUCH VERANTWORTUNG

Verantwortlich für den datenschutzkonformen Einsatz von KI ist nicht die KI sondern der Nutzer!

WAS IST ERLAUBT? (I)

- Im Datenschutzrecht gilt das Verbot mit Erlaubnisvorbehalt
 - Jede Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn sie auf eine Rechtsgrundlage gestützt werden kann (insbes. Einwilligung der betroffenen Person oder das überwiegende berechtigte Interesse der verarbeitenden Stelle)
- Einwilligung: Jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

WAS IST ERLAUBT? (II)

- Berechtigtes Interesse nur in Abwägung mit den Interessen, Grundfreiheiten und Grundrechten der betroffenen Person
 - Welche Art von personenbezogenen Daten werden verarbeitet?
 - Wie transparent erfolgt die Verarbeitung personenbezogener Daten?
 - In welchem Umfang werden personenbezogene Daten verarbeitet?

Aber: Berechtigtes Interesse keine geeignete Rechtsgrundlage bei besonderen Kategorien personenbezogener Daten (also auch Gesundheitsdaten)

INFORMATIONSPFLICHTEN

- Art. 13 DSGVO verpflichten den Verantwortlichen zur Erteilung von Informationen über Art und Umfang der Datenverarbeitung
 - Bspw. Name und Kontaktdaten des Verantwortlichen, Verarbeitungszwecke, Empfänger oder Kategorien von Empfängern, Übermittlung in ein Drittland, Dauer der Verarbeitung
- Folge: Die Verarbeitung personenbezogener Daten durch KI (z.B. bei Einsatz eines Chatbots) ist in einer Datenschutzerklärung transparent darzulegen

DATENSCHUTZFOLGEABSCHÄTZUNG

Achtung: Beim Einsatz Chatbots bei der Kundenbetreuung ist nach Ansicht mancher Datenschutzbehörden eine vorherige Datenschutzfolgeabschätzung erforderlich.

PROFILING DURCH KI (I)

- Jede betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (Bsp.: Bewerberauswahl durch KI)
- Ausnahmen:
 - Die Entscheidung ist für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich
 - Rechtsvorschriften erlauben die Verarbeitung
 - Einwilligung der betroffenen Person

PROFILING DURCH KI (II)

- Der Betroffene muss beim Einsatz von Profiling in der Datenschutzerklärung hierüber informiert werden
- Dies muss „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“ enthalten

DATENÜBERMITTLUNG: VORSICHT BEI DRITTLÄNDERN

- Übermittlung personenbezogener Daten in ein Land außerhalb des Europäischen Wirtschaftsraums ist nur unter strengen Voraussetzungen (Sicherstellung eines angemessenen Datenschutzniveaus durch zusätzliche Schutzmaßnahmen) möglich
- Bei KI-Lösungen ist oft unklar, in welchem Land sich die Server befinden, bzw. auf welchen Servern welche Daten gespeichert werden
- USA: 10. Juli 2023: Inkrafttreten des EU-US Data Privacy Frameworks
- Aber: Übermittlung nur an unter dem Abkommen zertifizierte Unternehmen möglich (OpenAI: nein; Microsoft: ja)

DATENSCHUTZBEHÖRDEN SIND AM BALL

- Aufsichtsbehörde Schleswig-Holstein: Katalog mit etwa 40 Fragen zur Beantwortung and ChatGPT-Betreiber übersandt
- Datenschutzkonferenz: Hambacher Erklärung zu KI (vom 3. April 2019)
 - KI darf Menschen nicht zum Objekt machen
 - KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben
 - KI muss nachvollziehbar, transparent und erklärbar sein
 - KI muss Diskriminierungen vermeiden
 - Für KI gilt der Grundsatz der Datenminimierung
 - KI braucht Verantwortlichkeit
 - KI benötigt technische und organisatorische Standards

HAFTUNG BEIM EINSATZ VON KI

RISIKEN & HAFTUNG BEIM EINSATZ VON KI

- Die Bezeichnung „Künstliche Intelligenz“ ist also insoweit irreführend, als durchaus inhaltlich unrichtige Ergebnisse geliefert werden.
- Klassisches Risiken:
 - Keine menschlich überprüften Ergebnisse
 - Nicht nachvollziehbaren Entscheidungswege
 - Informationsquellen unbekannt
- Wer haftet potentiell? Betreiber des Systems und diejenigen, welche die Ergebnisse für ihre Zwecke einsetzen

WER HAFTET?

- Produkthaftungsgesetz: Produzent eines Produkts haftet für Schäden an Personen und Sachen zum privaten Gebrauch, ohne dass ihm ein Verschulden nachgewiesen werden muss. Aber: Produkthaftungsgesetz gilt nur für körperliche Sachen
- Produzentenhaftung (§ 823 Abs. 1 BGB) erstreckt sich auch auf nichtkörperliche Produkte
- Grund für die Rechtsgutsverletzung muss die schuldhafte Verletzung einer Verkehrssicherungspflicht sein (z.B. fehlerhafte Konstruktion oder Produktbeobachtung)
- Aber: Hochentwickelte KI ist für Menschen kaum mehr durchschaubar; Nachweis, dass ein Schaden aufgrund der Verletzung einer Verkehrssicherungspflicht des KI-Anbieters aufgetreten ist, ist daher kaum möglich

HAFTUNG BEIM EINSATZ VON KI

- Werden KI-Leistungen in eigene Leistungen integriert, sind für die Haftungsfragen die Regelungen des zugrunde liegenden Vertrages maßgeblich (Kauf-, Werk-, Dienstvertrag etc.)
- Soweit falsche Ergebnisse zu Schäden an Körper, Gesundheit, Freiheit, Eigentum und Leben führen, kommt ein Schadensersatzanspruch nach § 823 Abs. 1 BGB in Betracht
- Gefährdungshaftung existiert bisher nicht (jedenfalls soweit die KI nicht in bestimmte Produkte integriert wird, für welche das Produkthaftungsgesetz oder Regelungen für Medizinprodukte gelten); auch durch die neuen EU-KI-Regulierungen keine grds. verschuldensunabhängige Gefährdungshaftung

AUSBLICK

WAS PLANT DER GESETZGEBER?

DIE EU ARBEITET DARAN

- Europäische Union möchte Künstliche Intelligenz regulieren
- Regulierungsziel ist (auch) Schaffung besserer Bedingungen für die Entwicklung und Nutzung dieser innovativen Technologie
- KI-Systeme sollen sicher, transparent, nachvollziehbar, nicht diskriminierend und umweltfreundlich sein
- KI-Systeme sollen von Menschen und nicht von Maschinen überwacht werden.
- KI soll für künftige Systeme technologieneutral und einheitlich definiert werden.

WAS IST IN DER PIPELINE?

- Europäisches Parlament: Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (KI-Gesetz) soll u.a. verbieten:
 - KI-Systeme, die Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person einsetzen, um das Verhalten einer Person in einer Weise wesentlich zu beeinflussen, die dieser Person oder einer anderen Person einen physischen oder psychischen Schaden zufügt oder zufügen kann
 - Nutzung von KI-Systemen durch Behörden zur Bewertung der Vertrauenswürdigkeit natürlicher Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale, die zu Schlechterstellung oder Benachteiligung führt

RISIKOBASIERTER ANSATZ

- Abstufung nach (i) KI-Systeme mit unannehmbarem Risiko, (ii) Hochrisiko-KI-Systeme, (iii) KI-Systeme mit mittlerem Risiko und (iv) KI-Systeme ohne besonderes Risiko
- KI-Systeme mit unannehmbarem Risiko: Verboten, wenn Bedrohung für Menschen
- Hochrisiko-KI-Systeme: Stellen ein hohes Risiko für die Gesundheit und Sicherheit oder für die Grundrechte natürlicher Personen dar
 - Insbesondere: KI-Systeme, die in Produkten verwendet werden, die unter EU-Produktsicherheitsvorschriften fallen (u.a. Spielzeug, Luftfahrt, Fahrzeuge, medizinische Geräte, Aufzüge)

ANFORDERUNGEN AN HOCHRISIKO-KI-SYSTEME

- Einrichtung eines Risikomanagementsystems (Ermittlung, Analyse & Bewertung von Risiken)
- Qualitätsvorgaben an Trainingsdaten (relevant, repräsentativ, fehlerfrei und vollständig)
- Technische Dokumentation des KI-Systems
- Automatische Protokollierung von Vorgängen und Ereignissen während des Betriebs
- Transparenz & Informationspflichten für Nutzer u.a. Merkmale, Fähigkeiten und Leistungsgrenzen des Systems)
- Menschliche Aufsicht
- Gewährleistung von Genauigkeit, Robustheit und Cybersicherheit
- Durchlaufen eines Konformitätsbewertungsverfahrens

AUSBLICK

- Aktuell: Verhandlungen über die KI-Verordnung mit den Mitgliedsstaaten und der Kommission erforderlich
- Inkrafttreten der Verordnung nicht vor 2026

PRAXISTIPPS

PRAXISTIPPS ZUM UMGANG MIT KI UND CHAT GPT

- Wichtige Informationen immer durch eigene Recherche verifizieren
- Keine Übermittlung personenbezogener Daten an KI
- Die KI nutzt alle Informationen, um zu lernen; Geschäftsgeheimnisse haben bei ChatGPT nichts zu suchen
- An Arbeitsergebnissen der KI hat der Nutzer keine Urheberrechte
- Mitarbeiter sollten bzgl. des Umgangs mit KI aufgeklärt werden (insbes. Mitteilungspflichten bei Nutzung für Arbeitsergebnisse)

ADVANT Beiten

Mathias Zimmer-Goertz

E-Mail: mathias.zimmer-goertz@advant-beiten.com

Cecilienallee 7

40474 Düsseldorf

Tel.: +49 211 518989-0

Fax: +49 211 518989-29

www.advant-beiten.com

**VIELEN DANK FÜR IHRE
AUFMERKSAMKEIT!**

