

「 MENOLD
BEZLER 」

RECHTLICHE ANFORDERUNGEN BEIM EINSATZ VON
CHATGPT UND ANDEREN KI-SYSTEMEN

29. NOVEMBER 2023

DFN ■ ■ ■
CERT®



Dr. Carsten Ulbricht

Partner, Rechtsanwalt

Tel +49 711 86040 022

Fax +49 711 86040 277

carsten.ulbricht@menoldbezler.de



Profil

Dr. Carsten Ulbricht absolvierte sein Studium der Rechtswissenschaften an den Universitäten Mannheim und Adelaide (Australien). Er ist seit 2019 als Partner für Menold Bezler tätig.

DER REFERENT

Kompetenzbereiche und Tätigkeitsschwerpunkte

- IT-Recht / Gewerblicher Rechtsschutz und Datenschutz
- Spezialisierung auf Internet, E-Commerce, Mobile und Social Media
- Blog „Internet, Social Media & Recht“

www.rechtzweinux.de

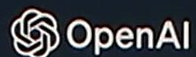
www.twitter.com/intertainment

A blurred background image of a business meeting. In the foreground, a person in a white shirt is pointing with a pen at a laptop screen. In the background, another person in a blue shirt is looking at the screen. The overall scene is brightly lit, suggesting an office environment.

TEIL 1 EINLEITUNG

ITS NOT THE AI WHO WILL REPLACE PEOPLE, IT'S THE PEOPLE WHO KNOW HOW TO USE IT





New and existing plugin developers





Der Bayerische Landesbeauftragte
für den Datenschutz

Datenschutz bei Rechtschreibkorrektur im Webbrowser

Aktuelle Kurz-Information 48

Stichwörter: KI bei Webbrowsern – Rechtschreibkorrektur, Webbrowser – Schreibhilfe, Webbrowser – Webbrowser | **Stand:** 1. Juli 2023

Was sind die Kernaussagen dieser Aktuellen Kurz-Information?

- ▶ Schreibhilfen in Webbrowsern können auf Künstliche Intelligenz zurückgreifen, um Verbesserungsvorschläge zu machen; dabei kann es zu einer Übermittlung personenbezogener Dateneingaben an den Browseranbieter kommen.
- ▶ Die Übermittlung hängt davon ab, wie der Browser konfiguriert ist.
- ▶ Bayerische öffentliche Stellen sollten die bei ihnen eingesetzten Browser insofern kritisch überprüfen.

A. GRUNDLAGEN CHATGPT

Generative Pre-Trained Model

- Large Language Model (LLM)
- Vortrainierte Sprachmodelle
- Selbstlernende Algorithmen

Schnellste Skalierung aller Zeiten

- 100 Mio. Nutzer in 2 Monaten
- TikTok brauchte 2,5 Jahre

5 Monate von GPT3-5 auf 4

- 175 Mrd Parameter → 1 Billionen Parameter!
- Text-, Ton-, Bildeingaben
- Texte bis 25.000 Wörter in kurzer Zeit

Wesentliche Merkmale

Input durch „Prompts“

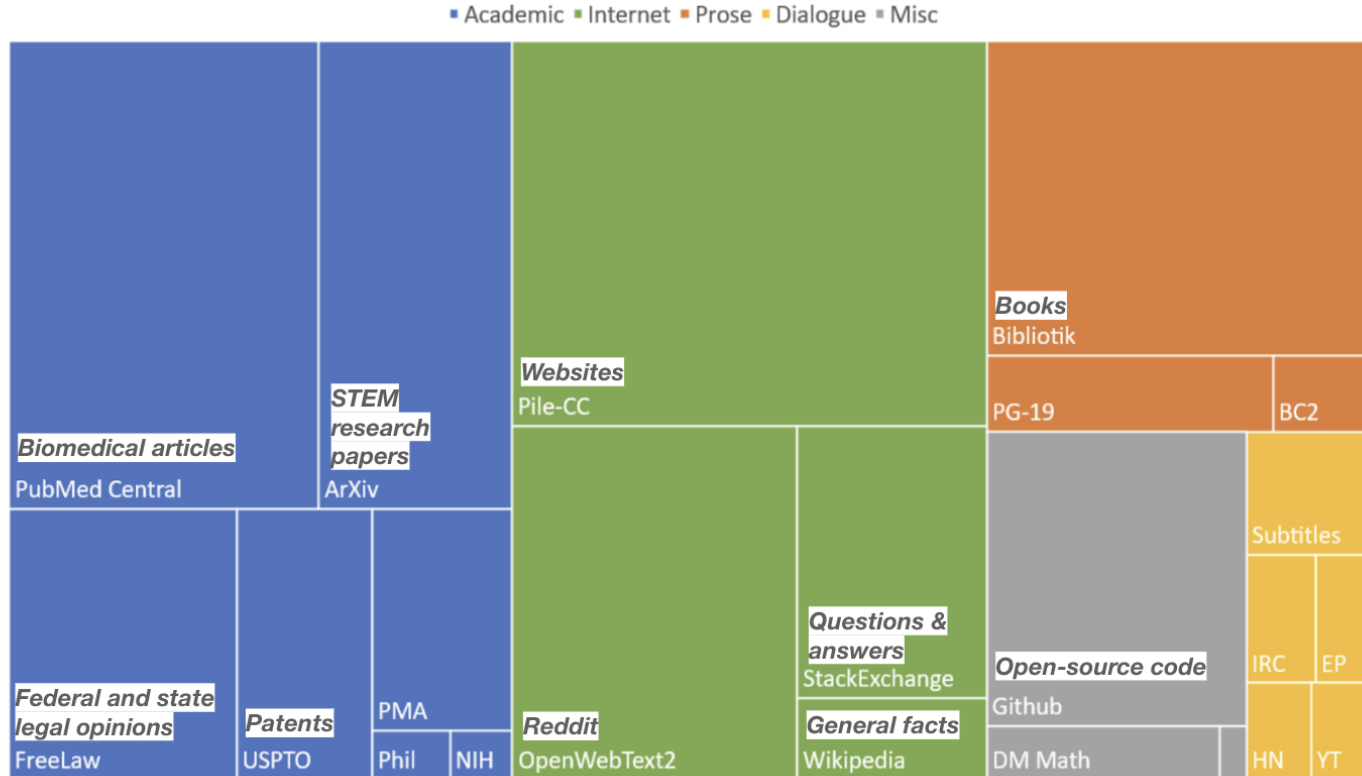
Trainingsdaten aus öffentlich zugänglichen Quellen
„Wissen des Internet“

Output nur statistisch plausibel

„contextual probability“ statt wahr/falsch

Weitere Anbieter für Übersetzung (deepL),
Paraphrasierung (quillbot), Quellenidentifizierung
(Aleph Alpha)

FOUNDATION-MODELS ARE TRAINED ON 100S OF GIGABYTES OF TEXT DATA TO BUILD AN UNDERSTANDING OF THE WORLD



A. GRUNDLAGEN CHATGPT

Rechtliche Grundlagen

- Kalifornisches Recht und Gerichtsstand
- Schiedsklausel
- Ausschluss Class Actions
- US Verbraucher ⇒ Open AI zahlt ggf. Schiedskosten
- EU-Verbraucher ⇒ Online Dispute Resolution
- Nutzer alle Rechte an Input und Output (soweit möglich)
- Copyright Complaint möglich
- US Disclaimer für Haftung und Gewährleistung („as is“)

RECHTLICHE GRUNDLAGEN

Definition „Gesetz über Künstliche Intelligenz“ (nachfolgend KI-VO):

„System der künstlichen Intelligenz“ (KI-System) eine **Software**, die mit einer oder mehreren der **in Anhang I aufgeführten Techniken und Konzepte** entwickelt worden ist und im Hinblick auf eine Reihe von **Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen** hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren.

Anhang 1

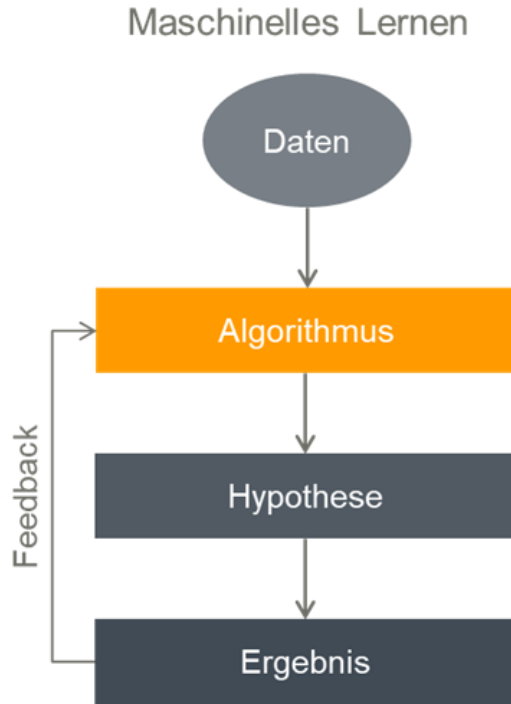
- a) Konzepte des **maschinellen Lernens**, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning);
- b) **Logik- und wissensgestützte Konzepte**, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme;
- c) Statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden.

Rechtliche Vorgaben in KI-VO für Anbieter, Nutzer, Einführer, Händler

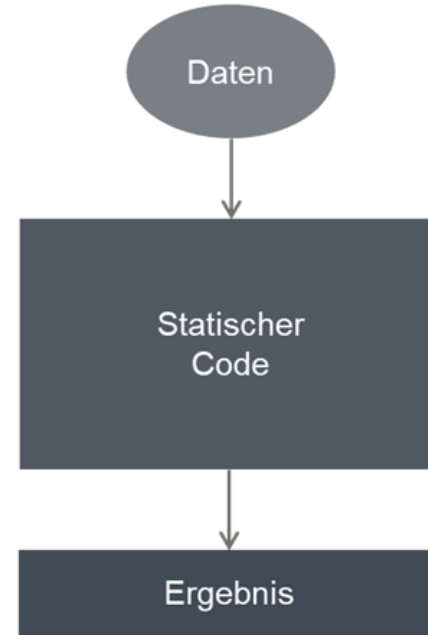
Aktuelle Regelungen:

- Urheberrecht
- Datenschutz

DEFINITION KÜNSTLICHE INTELLIGENZ



Traditionelle Programme





TEIL 2 URHEBERRECHT

URHEBERRECHTLICHE WAS SAGT CHATGPT?

CA is chatgpt copyright protected



Yes, ChatGPT is a product of OpenAI, and as such, it is protected by copyright laws. The specific terms of use and copyright protections for ChatGPT are governed by OpenAI's terms of service and license agreements. Any unauthorized use or reproduction of ChatGPT could be considered a violation of copyright law.



CA sind die texte von chatgpt urheberrechtlich geschützt



Ja, die Texte von ChatGPT sind urheberrechtlich geschützt, da sie ein Produkt von OpenAI sind. Die spezifischen Nutzungsbedingungen und Urheberrechtsschutz für ChatGPT werden durch die Nutzungsbedingungen und Lizenzvereinbarungen von OpenAI geregelt. Jegliche unautorisierte Nutzung oder Vervielfältigung von ChatGPT kann als Verstoß gegen das Urheberrechtsgesetz angesehen werden.



A. URHEBERRECHTLICHE GRUNDLAGEN

ANWENDBARES RECHT

- Erhebliche Unterschiede in nationalen Urheberrechtsgesetzen
- Deutsches Urheberrecht vs. US-amerikanisches Copyright
- Schutzlandprinzip

A. URHEBERRECHTLICHE GRUNDLAGEN

URHEBERRECHT

- § 1 UrhG: Schutz von Werken der Literatur, Kunst & Wissenschaft
- § 2 Abs.1 UrhG: Sprachwerke, Lichtbildwerke, Filmwerke u.a.



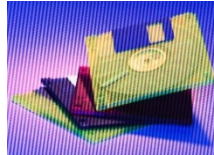
Sprachwerke



Musik



Filmwerke



Software



Lichtbildwerke



Datenbanken



Karten

- § 2 Abs.2 UrhG: Werke im Sinne dieses Gesetzes sind nur **persönliche geistige** Schöpfungen.
- US-Copyright wohl ähnlich “original creation of the human mind”

A. URHEBERRECHTLICHE GRUNDLAGEN

URHEBERRECHTSSCHUTZ BEI KI-GENERIERTEN WERKEN

- KI-Software ist urheberrechtlich geschützt
- kein Urheberrechtsschutz der KI an erzeugten Werken (keine Rechtspersönlichkeit)
- kein Urheberrechtsschutz des Entwicklers/Anbieters der KI an erzeugten Werken
- Inhalte Dritter, die in/von KI verarbeitet werden

B. URHEBERRECHT BEISPIEL



B. URHEBERRECHT

BEARBEITUNG/UMGESTALTUNG VS. FREIE BENUTZUNG



Bearbeitung/Umgestaltung (§ 23 UrhG)

Nutzungsrechte des Urhebers erforderlich

Unterlassungsansprüche

Schadenersatz (Fahrlässigkeit?)

vs.

freie Benutzung

Nutzungsrechte verzichtbar

keine Unterlassungsansprüche

kein Schadenersatz

C. SCHRANKENREGELUNGEN

ENTWICKLUNG EIGENER KI

- Vorübergehende Vervielfältigungshandlungen (§ 44a UrhG)
- Text und Datamining (§ 44b UrhG)

(1) Text und Data Mining ist die automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken, um daraus Informationen insbesondere über Muster, Trends und Korrelationen zu gewinnen.

(2) Zulässig sind Vervielfältigungen von rechtmäßig zugänglichen Werken für das Text und Data Mining. Die Vervielfältigungen sind zu löschen, wenn sie für das Text und Data Mining nicht mehr erforderlich sind.

(3) Nutzungen nach Absatz 2 Satz 1 sind nur zulässig, wenn der Rechtsinhaber sich diese nicht vorbehalten hat. Ein Nutzungsvorbehalt bei online zugänglichen Werken ist nur dann wirksam, wenn er in maschinenlesbarer Form erfolgt.

C. SCHRANKENREGELUNGEN

ZULÄSSIGKEIT VON TEXT UND DATA MINING

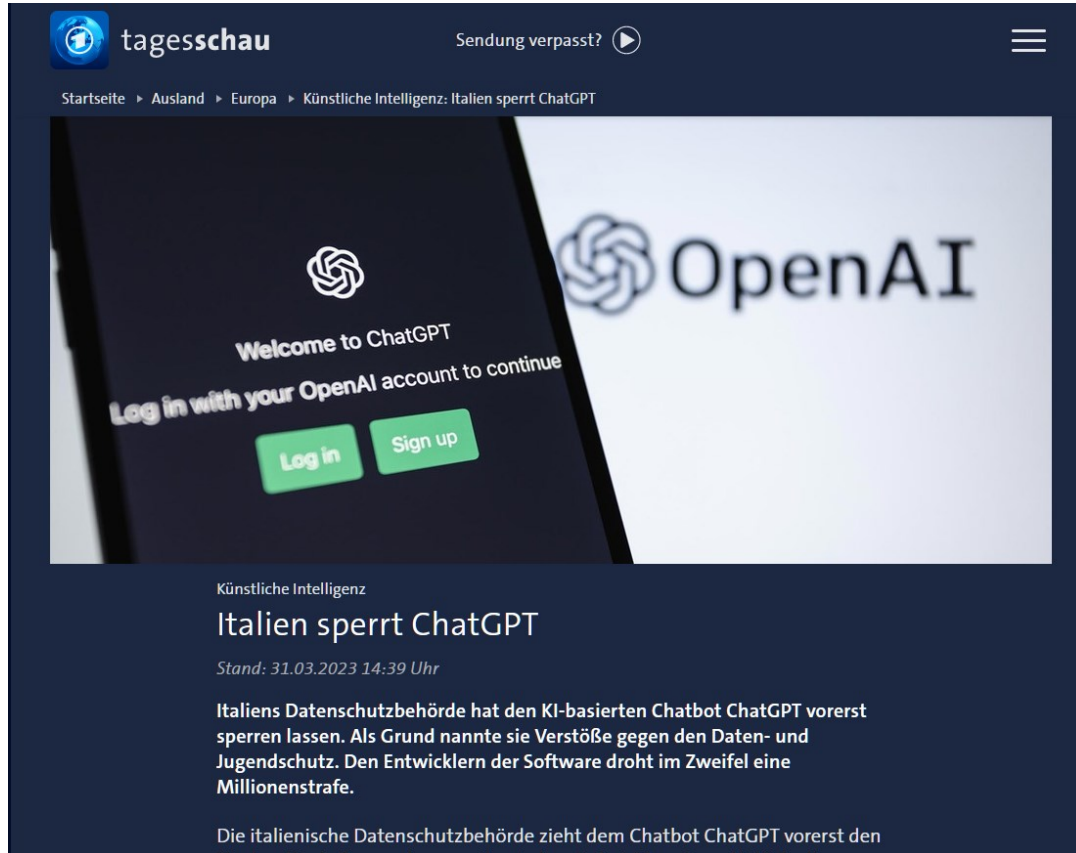
- Computergestützte und systematische Vervielfältigung zur Vorbereitung der automatisierten Auswertung
- Ausnahme: technische Schutzvorkehrungen (§ 95 UrhG) und andere Rechtsnormen (z.B. Datenschutz / Persönlichkeitsrechte)
- Nutzungsvorbehalt in maschinenlesbarer Form (z.B. in Robots.txt)
- Löschpflicht, wenn nicht mehr für vorgenannte Zwecke erforderlich

D. ZUSAMMENFASSUNG

- Urheberrechtliche Risiken bei Verwendung KI-basierter Texte derzeit wohl gering
- Urheberrechtliche Risiken bei sonstigen KI-basierten Werken (z.B. Bilder, Software) – je nach Eingabe, Werk und anwendbarem Recht – möglich
- Regelung durch AGB / Terms of Service denkbar
- Entscheidung über Schutz eigener Veröffentlichungen sinnvoll
- Entwicklung eigener KI
 - Trainingsdaten (§ 44a UrhG, DSGVO)
 - KI-Verordnung (AI Act)
 - Haftung




TEIL 3
DATENSCHUTZRECHT



The screenshot shows a news article from the German news outlet 'tagesschau'. The article is titled 'Italien sperrt ChatGPT' and is categorized under 'Künstliche Intelligenz'. The main image shows a smartphone screen displaying the OpenAI login page with the text 'Welcome to ChatGPT' and 'Log in with your OpenAI account to continue'. The article text states that Italy's data protection authority has banned ChatGPT, citing violations of data and youth protection laws, and that the developers face a potential fine of up to 10 million euros.

tagesschau Sendung verpasst? ☰

Startseite ▶ Ausland ▶ Europa ▶ Künstliche Intelligenz: Italien sperrt ChatGPT



Künstliche Intelligenz

Italien sperrt ChatGPT

Stand: 31.03.2023 14:39 Uhr

Italiens Datenschutzbehörde hat den KI-basierten Chatbot ChatGPT vorerst sperren lassen. Als Grund nannte sie Verstöße gegen den Daten- und Jugendschutz. Den Entwicklern der Software droht im Zweifel eine Millionenstrafe.

Die italienische Datenschutzbehörde zieht dem Chatbot ChatGPT vorerst den

A. ZULÄSSIGKEIT DER DATENVERARBEITUNG



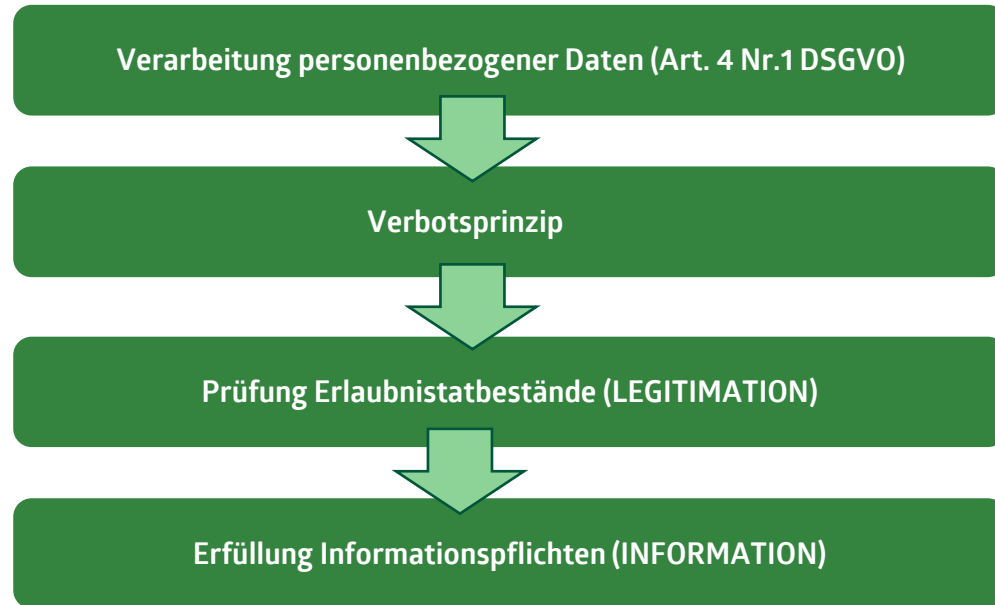
B. ANWENDUNGSBEREICH

PERSONENBEZOGENE DATEN (ART. 4 NR.1 DSGVO)

„alle Informationen, die sich auf eine **identifizierte oder identifizierbare** natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.“

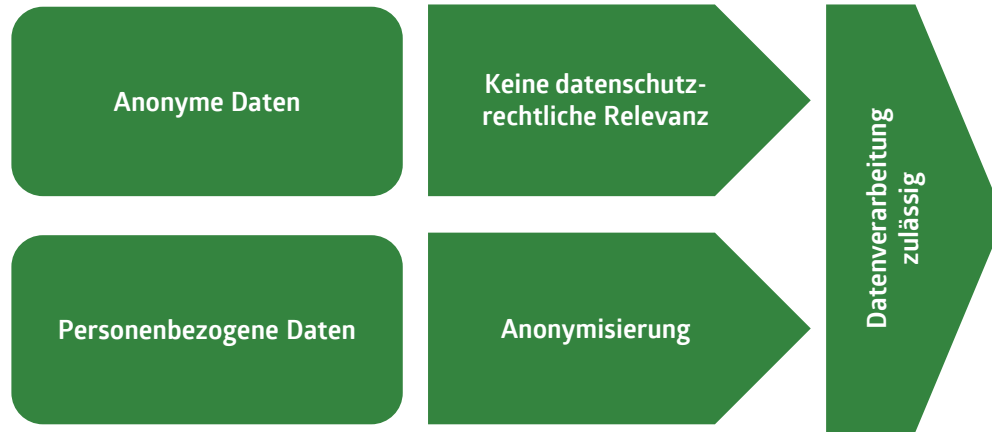
→ Weiter Begriff des Personenbezuges

A. ZULÄSSIGKEIT DER DATENVERARBEITUNG



A. ZULÄSSIGKEIT DER DATENVERARBEITUNG

ANONYMISIERUNG



A. ZULÄSSIGKEIT DER DATENVERARBEITUNG

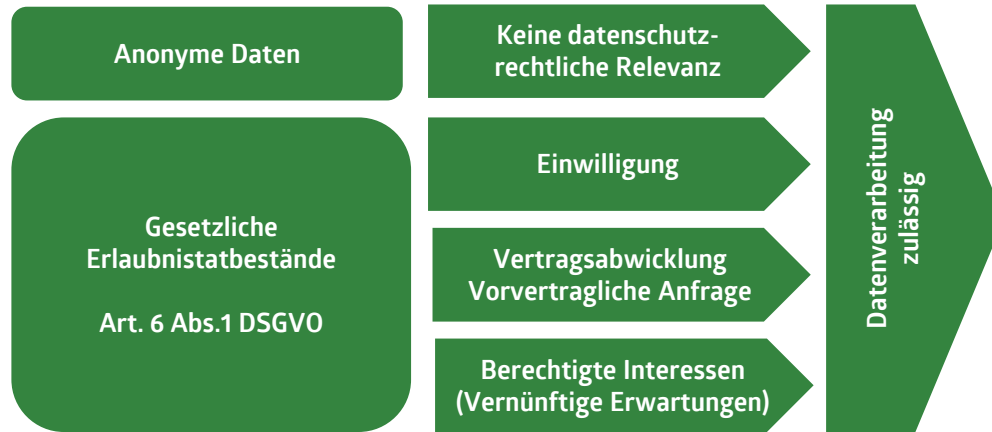
ANONYMISIERUNG

- Verändern personenbezogener Daten derart, dass diese Daten nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können.
- dazu auch Entscheidung des EuGH in der Rs. C-319/22 vom 9. November 2023 (FIN)

Umsetzung :

- Maskierung / Ersetzung
- Aggregation / Kohortenbildung (z.B. Zusammenfügen verschiedener Datensätze zu einer gemeinsamen Gruppe)
- Privacy Enhancing Technologies (PET)
- Differential Privacy Methoden
- Kryptografische Methoden (z.B. homomorphe Verschlüsselung)

B. ERLAUBNISTATBESTÄNDE



B. GESETZLICHE BESTIMMUNGEN BEI DER VERARBEITUNG VON PERSONALDATEN EINWILLIGUNG

Legitimation über Einwilligung in Einzelfällen denkbar

- Beispiel Heygen
- Informierte Einwilligung des Betroffenen (z.B. Mitarbeiter)
- Umfassende Information über Datenverarbeitung („voice und face cloning“)
- Datenübetragung in die USA (Art. 49 Abs.1 lit.a DSGVO)
- Widerruflichkeit

C. INFORMATIONSPFLICHTEN

INFORMATIONSPFLICHTEN (ART. 13 ABS.1 DSGVO)

- Identität des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Verarbeitungszwecke und Rechtsgrundlage
- Berechtigtes Interesse
- Empfänger
- Übermittlung in Drittstaaten

C. INFORMATIONSPFLICHTEN

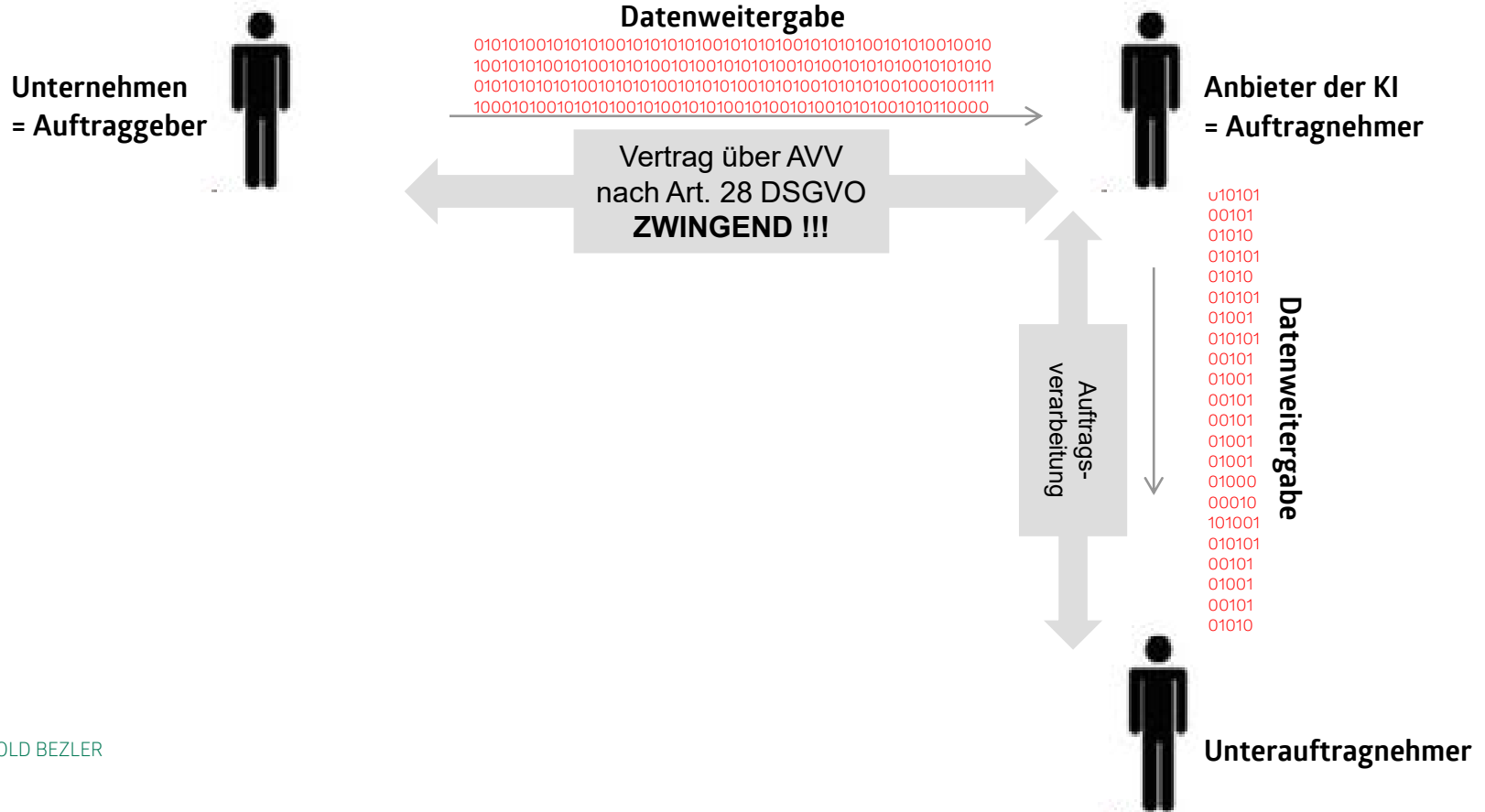
INFORMATIONSPFLICHTEN (ART. 13 ABS.2 DSGVO)

- Dauer der Speicherung
- Rechte der Betroffenen
- Widerrufbarkeit von Einwilligungen
- Beschwerderecht bei der Aufsichtsbehörde
- Verpflichtung zur Bereitstellung personenbezogener Daten
- Automatisierte Entscheidungsfindung und Profiling

D. VERANTWORTLICHKEITEN

Auftragsverarbeitung (Art. 28 DSGVO)	Gemeinsame Verantwortlichkeit (Art. 26 DSGVO)	Getrennte Verantwortlichkeit
Auftraggeber entscheidet über <u>Zwecke und Mittel</u> der Datenverarbeitung	Gemeinsame Entscheidung über <u>Zwecke und Mittel</u> der Datenverarbeitung	Jeweils eigenständige Entscheidung über <u>Zwecke und Mittel</u> der Datenverarbeitung
<ul style="list-style-type: none"> • Abschluss eines Auftragsverarbeitungsvertrages zwingend 	<ul style="list-style-type: none"> • Abschluss eines Joint Controllership Agreements zwingend • Gemeinsame Haftung im Außenverhältnis 	<ul style="list-style-type: none"> • Unabhängige Datenverarbeitung
Sinnvolle Gestaltung bei Einsatz von KI-Systemen	Komplexere Gestaltung bei Einsatz von KI-Systemen	Denkbare Gestaltung beim Einsatz bestehender KI-Systeme

D. VERANTWORTLICHKEITEN



D. VERANTWORTLICHKEITEN

Auftragsverarbeitungsvertrag bei ChatGPT

- FÜR “APIs for text completion, images, embeddings, moderations”
- NICHT FÜR: “consumer services (ChatGPT, DALL-E Labs)”

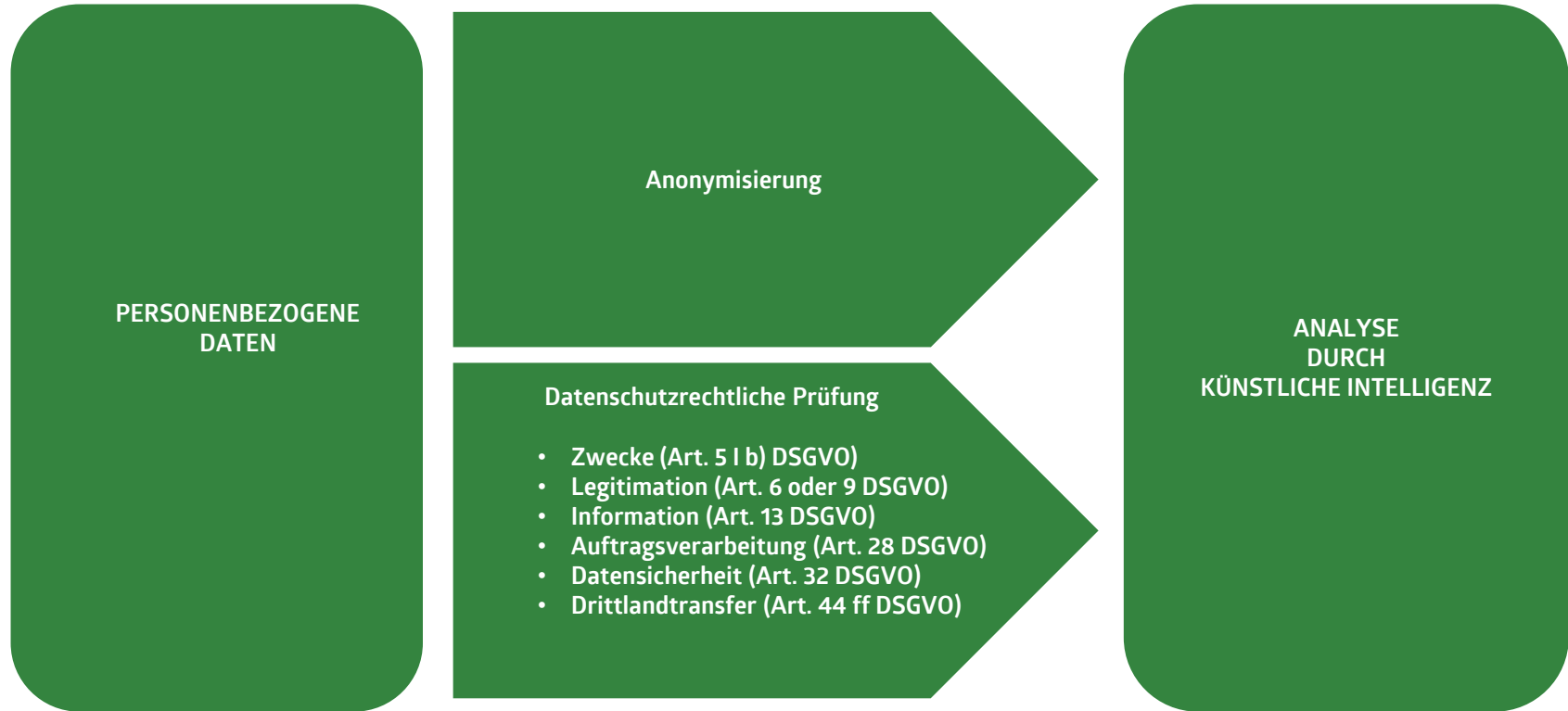
Auftragsverarbeitungsvertrag bei Aleph Alpha

- keine Speicherung API Daten
- Abschluss ansonsten möglich

D. BETROFFENENRECHTE

Art 12	Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person
Art 13	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
Art 14	Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
Art 15	Auskunftsrecht
Art 16	Recht auf Berichtigung
Art 17	Recht auf Löschung ("Recht auf Vergessenwerden")
Art 18	Recht auf Einschränkung der Verarbeitung
Art 19	Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
Art 20	Recht auf Datenübertragbarkeit
Art 21	Widerspruchsrecht

BEISPIEL



A blurred background image of a business meeting. Several people are gathered around a table, looking at a laptop. One person in a white shirt is pointing at the screen with a pen. The overall tone is professional and collaborative.

TEIL 4 GESCHÄFTSGEHEIMNISSE

CHATGPT

Samsung verbietet Mitarbeitern die Nutzung generativer KI

Samsung Electronics hat ernst gemacht und seinen Mitarbeitern verboten, generative KI wie ChatGPT zu nutzen, weil Firmendaten geleakt wurden.



2. Mai 2023, 11:15 Uhr, Michael Linden



(Bild: Samsung)

Arbeitsplatz bei Samsung Semiconductor

Samsung hatte Anfang 2023 entdeckt, dass Programmcode von seinen Entwicklern auf ChatGPT hochgeladen wurde. Nun hat das Unternehmen seinen Mitarbeitern einen Bericht von Bloomberg (Paywall) nach offiziell untersagt, dortige Plattformen zu

ANZEIGE



SCHUTZ VON GESCHÄFTSGEHEIMNISSEN

Geschäftsgeheimnis (§ 2 Nr.1 GeschGehG) ist eine Information, die

- weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und
- die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und
- bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

➔ **Faktisches und rechtliches Risiko**

➔ **Notwendigkeit angemessener Geheimhaltungsmaßnahmen**

A blurred background image of a business meeting. Several people in professional attire are gathered around a table, looking at documents and a laptop. The lighting is bright and soft, creating a professional and collaborative atmosphere.

TEIL 5 UMSETZUNG

A. VERTRAGLICHE AUSGESTALTUNG

- Prüfung Vertragsbedingungen Anbieter
- Prüfung Datenschutzhinweise Anbieter
- Abschluss Datenverarbeitungsvertrag (im Idealfall Auftragsverarbeitung (Art. 28 DSGVO))
- Standardvertragsklauseln (bei Drittlandtransfers)

B. ORGANISATORISCHE AUSGESTALTUNG

Einführung von Richtlinien

- Beschreibung zulässiger Einsatzzwecke
- Beschränkung der Nutzung auf geschäftliche Zwecke
- Vorgaben für Registrierung / Einstellungen
- Keine Eingabe personenbezogener Daten
- Keine Eingabe von Betriebs- und Geschäftsgeheimnissen
- Prüfung der Richtigkeit der Ausgaben vor weitergehender Nutzung
- Beachtung der Nutzungsbedingungen und der Nutzungsrichtlinien (optional)
- Keine Verletzung von Rechten Dritter (optional)
- Erfüllung von Transparenzpflichten (optional)

Durchführung von Schulungen

C. TECHNISCHE AUSGESTALTUNG

- On-Premise vs. Software-as-a-Service
- Bereitstellung eines „Funktions-Accounts“
- (Datensparsame) Einstellung der Dienste
- Pseudonymisierung / Anonymisierung (soweit möglich)

D. EMPFEHLUNG DES HAMBURGISCHEN BEAUFTRAGTEN FÜR DATENSCHUTZ

1. Compliance-Regelungen vorgeben
2. Datenschutzbeauftragte einbinden
3. Bereitstellung eines Funktions-Accounts
4. Sichere Authentifizierung
5. Keine Eingabe personenbezogener Daten
6. Keine Ausgabe personenbezogener Daten
7. Vorsicht bei personenbeziehbaren Daten
8. Opt-out des KI-Trainings
9. Opt-out der History
10. Ergebnisse auf Richtigkeit prüfen
11. Ergebnisse auf Diskriminierung prüfen
12. Keine automatisierte Letztentscheidung
13. Beschäftigte sensibilisieren
14. Datenschutz ist nicht alles
15. Weitere Entwicklung verfolgen

Checkliste zum Einsatz LLM-basierter Chatbots |
HmbBfDI (datenschutz-hamburg.de)

E. NUTZUNG VON TRAININGSDATEN

- Kein „Eigentum“ und kein Urheberrechtsschutz an Einzeldaten
 - Beachtung IP-Rechte Dritter
 - Urheberrechtsschutz bei Texten, Fotos, Audio- und Videoinhalten
 - Datenbankrecht (§87a UrhG)
 - Beachtung Datenschutzrecht
 - Schutz von Geschäfts- und Betriebsgeheimnisse (GeschGehG)
 - Sektorspezifische Regelungen wie zum Beispiel TK-Verkehrsdaten (§ 96 TKG) oder Energiemessdaten (§ 21 EnWG)
 - Strafrechtsschutz: Unberechtigtes Ausspähen und Abfangen von Daten (§ 202 a/b StGB)
- ➔ Vertragliche Regelung zur Nutzung von Daten und Training der KI**



TEIL 5
ZUSAMMENFASSUNG
UND AUSBLICK

RESÜMEE

- Risikobasierter Ansatz statt Verbote
 - Rechtliche Einschätzung erfordert klar definierte Anwendungsfälle
 - Verschiedene rechtliche Implikationen (z.B. Urheberrecht, Datenschutzrecht)
 - Entwicklung aktuelle Gesetzesvorhaben (z.B. KI-VO) weiter beobachten
-
- ➔ Aktive Entscheidung über Einsatz KI-basierter Werkzeuge (ob und welche)
 - ➔ Prüfung etwaiger Vereinbarungen mit Anbieter
 - ➔ Einführung technischer und organisatorischer Maßnahmen (z.B. Richtlinien)

CHECKLISTE „DATENSCHUTZ BEIM EINSATZ VON KI-SYSTEMEN“

Vorfragen (z.B. an Fachabteilung)

- a. Welche personenbezogenen Daten sollen von der KI verarbeitet werden?
- b. Wie wurden diese Daten erhoben?
- c. Zu welchem Verwendungszweck sollen die Daten verarbeitet werden?
- d. Wer verarbeitet diese Daten?
- e. Wie werden die Daten verarbeitet (Zusammenführung)?
- f. Werden die Roh- oder die verarbeiteten Daten an Dritte weitergegeben? An wen und zu welchen Zwecken?
- g. Können die Daten für den jeweiligen Use Case anonymisiert oder pseudonymisiert werden?

Grundsätze der Datenverarbeitung

- a. Wie stellen Sie sicher, dass alle Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1 DSGVO eingehalten werden?
- b. Wie werden die Grundsätze der Zweckbindung, der Datenminimierung und der Speicherbegrenzung (Art. 5 Abs. 1 lit. b) 1. Hs., lit. c) und lit. e) DSGVO), insbesondere hinsichtlich der für das Training der KI verwendeten personenbezogenen Daten, sichergestellt?
- c. Wie lange werden die personenbezogenen Daten gespeichert?
- d. Auf welche Weise wird die Richtigkeit der verwendeten Daten und der personenbezogenen Daten, die die ggfls erzeugt, (Art. 5 Abs. 1 lit. d) DSGVO), sichergestellt, insbesondere wenn eine betroffene Person das Recht auf Berichtigung (Art. 16 DSGVO) oder das Recht auf Löschung (Art. 17 DSGVO) in Anspruch nimmt?

Rechtmäßigkeit und Transparenz der Datenverarbeitung

- a. Auf welche Rechtsgrundlagen werden die verschiedenen Verarbeitungsvorgänge von personenbezogenen Daten jeweils gestützt?
- b. Wird bei der Erhebung und Weiterverarbeitung danach differenziert, ob die genutzten Daten Personenbezug aufweisen oder nicht?
- c. Wie wird die Beachtung der Rechte betroffener Personen aus Art. 12 ff. DSGVO sichergestellt (insb. Rechte auf Transparenz, Auskunft, Berichtigung, Löschung)?
- d. Wie und an welcher Stelle werden die Nutzenden über die Erhebung und Verwendung personenbezogener Daten im Sinne von Art. 13 und 14 DSGVO informiert?

CHECKLISTE „DATENSCHUTZ BEIM EINSATZ VON KI-SYSTEMEN“

Datensicherheit

- a. Wird bei der Erhebung und Verarbeitung unterschieden, ob die genutzten Daten einen Personenbezug aufweisen oder nicht?
- b. Werden personenbezogene Daten pseudonymisiert, anonymisiert oder auf andere Weise aufbereitet, bevor diese zum Training der KI verwendet werden?
- c. Wie wird das Risiko der Re- Identifizierbarkeit infolge des Trainings der KI bewertet?
- d. Welche technischen und organisatorischen Maßnahmen werden eingesetzt, um die Risiken für die Rechte und Freiheiten etwaiger Betroffener einzudämmen?
- e. Besteht ein Sicherheitskonzept, mit dem nachgewiesen werden kann, dass solche Maßnahmen getroffen wurden?.
- f. Wie werden Grundsätze des „Data Protection by Design“ und „Data Protection by Default“ umgesetzt?

Datenweitergabe

- a. Werden personenbezogene Daten von Dritten erhoben, die zu eigenen Zwecken genutzt werden?
- b. Werden personenbezogene Daten an Dritte (z.B. bei Nutzung der KI) weitergegeben?
- c. Wer ist bei der Nutzung durch andere Dienste oder Unternehmen Verantwortlicher nach Art.4 Nr.7 DSGVO?
- d. Erfolgt die Nutzung durch Dritte im Rahmen einer Auftragsverarbeitung nach Art. 28 DSGVO oder im Rahmen einer gemeinsamen Verantwortlichkeit nach Art 26 DSGVO?

Datenschutz-Folgenabschätzung (DSFA)

- a. Ist eine DSFA erforderlich?
- b. Wurde eine DSFA nach Art. 35 DSGVO durchgeführt?

Übermittlung von Daten außerhalb der Europäischen Union

- a. Wo befinden sich die Server für den Dienst?
- b. Werden von Ihnen personenbezogene Daten an andere Unternehmen mit Sitz außerhalb der Europäischen Union übermittelt?

WEITERFÜHRENDE LINKS

- **KI & Recht – Richtlinien für die rechtssichere Nutzung von ChatGPT**
<http://www.rechtzweinull.de/ki-kuenstliche-intelligenz-recht-richtlinien-fuer-den-einsatz-von-chatgpt/>
- **KI & Recht – Rechtsfragen zu ChatGPT und künstlichen Intelligenzen**
<http://www.rechtzweinull.de/ki-recht-rechtsfragen-zu-chatgpt-und-kuenstlichen-intelligenzen/>
- **ChatGPT & Co – Urheberrecht bei Werken der Künstlichen Intelligenz**
<http://www.rechtzweinull.de/chatgpt-co-urheberrecht-bei-werken-der-kuenstlichen-intelligenz-ki-2>
- **AI Act: EU-Verordnung zu künstlicher Intelligenz (KI) in 3 Minuten erklärt**
Video: <https://www.youtube.com/watch?v=eLaqIGCfCwY&t=116s>

EU Datengesetze

MENOLD BEZLER

Rechtsanwälte Partnerschaft mbB

Rheinstahlstraße 3 · 70469 Stuttgart

Heilbronner Straße 190 · 70191 Stuttgart

Tel +49 711 86040 00

Fax +49 711 86040 01

carsten.ulbricht@menoldbezler.de

www.menoldbezler.de

www.rechtzweinull.de

MITTELSTAND IM MITTELPUNKT®

Linked in

twitter  /entertainment