MENOLD BEZLER

RECHT UND DATENSCHUTZ BEIM EINSATZ VON CHATGPT UND ANDEREN KI-SYSTEMEN

ekom21

10. OKTOBER 2024



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.

Kompetenzbereiche und Tätigkeitsschwerpunkte

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

www.rechtzweinull.de
www.twitter.com/intertainment



TEIL 1
EINLEITUNG

AI WILL NOT REPLACE YOU, BUT THE PERSON USING AI WILL





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. ORIENTIERUNGSHILFE DER DATENSCHUTZKONFERENZ



Orientierungshilfe

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024

Künstliche Intelligenz und Datenschutz

Version 1.0

Viele Unternehmen, Behörden und andere Organisationen fragen sich derzeit, unter welchen Voraussetzungen sie KI-Anwendungen datenschutzkonform einsetzen können. Dabei lag der Schwerpunkt ab dem Jahr 2023 auf sogenannten Large Language Models (LLM), die häufig als Chatbots angeboten werden, aber auch als Grundlage für andere Anwendungen dienen können. Der Schwerpunkt der folgenden Orientierungs-

B. RECHTLICHE GRUNDLAGEN

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

„KI-System“ ist ein maschinengestütztes System, das **für einen in unterschiedlichem Grade autonomen Betrieb** ausgelegt ist und das nach seiner Betriebsaufnahme **anpassungsfähig** sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können;

Rechtliche Vorgaben in KI-VO für Anbieter, Betreiber, Nutzer

Aktuelle Regelungen:

- Urheberrecht
- Datenschutz

C. GRUNDLAGEN LARGE LANGUAGE MODELLE

Generative Pre-Trained Model

- Vortrainierte Sprachmodelle
- Selbstlernende Algorithmen

Beispiel ChatGPT:

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 Billiarde 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

Nicht: Wahr/unwahr – korrekt/falsch



TEIL 2
URHEBERRECHT

A. URHEBERRECHTLICHE GRUNDLAGEN
URHEBERRECHT AM OUTPUT

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



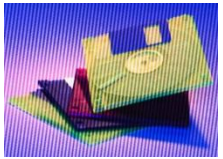
Sprachwerke



Musik



Filmwerke



Software



Lichtbildwerke



Datenbanken



Karten

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

A. URHEBERRECHTLICHE GRUNDLAGEN
URHEBERRECHT AM OUTPUT

- KI-Software ist urheberrechtlich geschützt
- kein Urheberrechtschutz der KI an erzeugten Werken (keine Rechtspersönlichkeit)
- kein Urheberrechtsschutz des Nutzers der KI an den erzeugten Werken
- kein Urheberrechtsschutz des Entwicklers/Anbieters der KI an erzeugten Werken

➔ KI-generierte Inhalte grundsätzlich gemeinfrei

B. URHEBERRECHT
BEISPIEL



B. URHEBERRECHT
BEARBEITUNG/UMGESTALTUNG VS. FREIE BENUTZUNG



Bearbeitung/Umgestaltung (§ 23 UrhG)	**vs.**	**freie Benutzung**
Nutzungsrechte des Urhebers erforderlich		**Nutzungsrechte verzichtbar**
Unterlassungsansprüche		**keine Unterlassungsansprüche**
Schadenersatz (Fahrlässigkeit?)		**kein Schadenersatz**

B. URHEBERRECHT
RISIKOABWÄGUNG

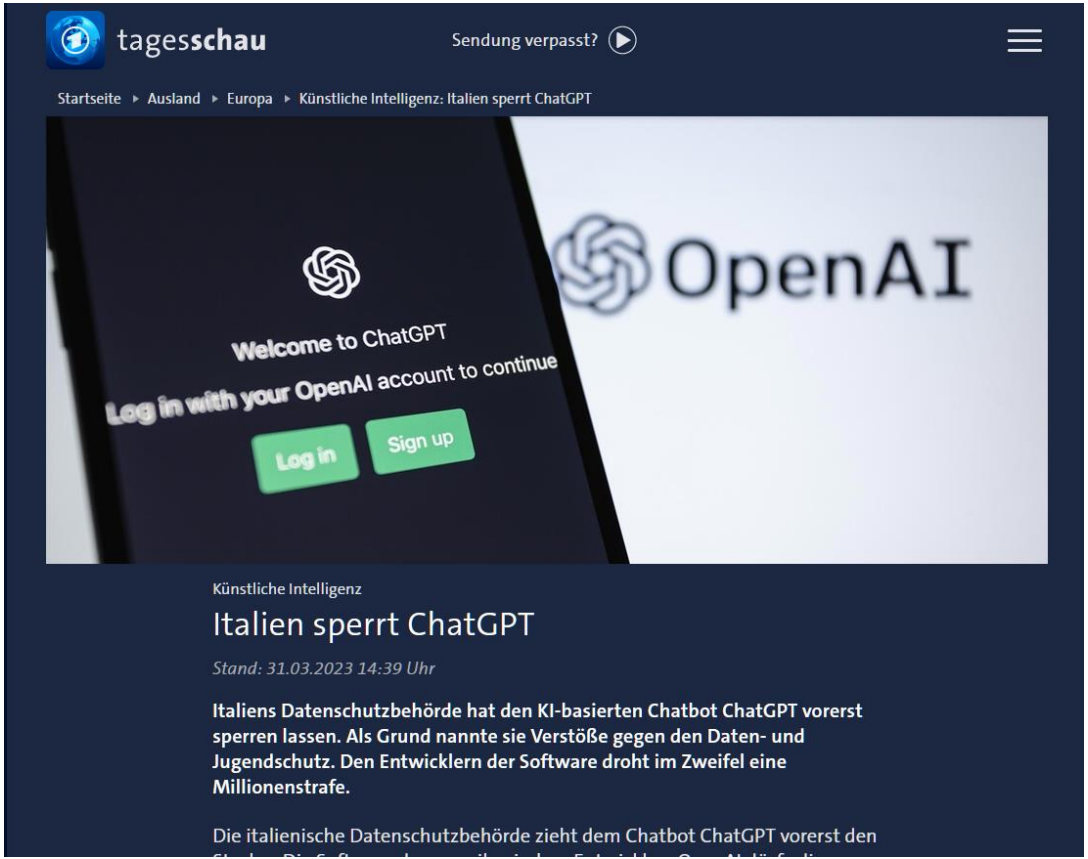
- Urheberrechtliche Risiken bei Verwendung KI-basierter Texte gering
- Urheberrechtliche Risiken bei sonstigen KI-basierten Werken (z.B. Bilder, Software) – je nach Eingabe, Werk und anwendbarem Recht – möglich

➔ Richtlinien zum Einsatz (generativer) KI-Systeme mit risikoreduzierenden Maßnahmen

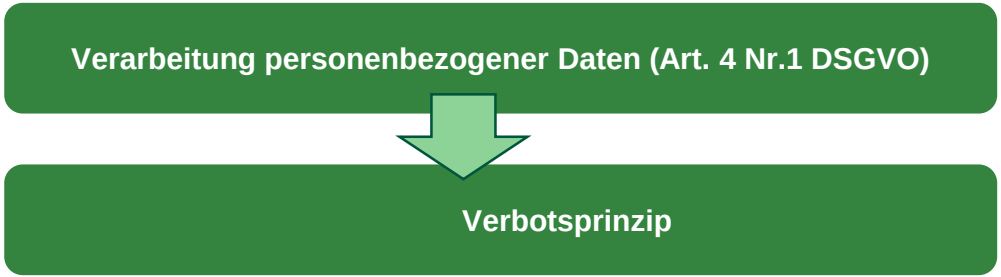
- (Weiter-)Entwicklung eigener KI
  - Trainingsdaten (§ 44b UrhG, DSGVO)
  - KI-Verordnung (AI Act)
  - Haftung
- Entscheidung über Schutz eigener Veröffentlichungen sinnvoll



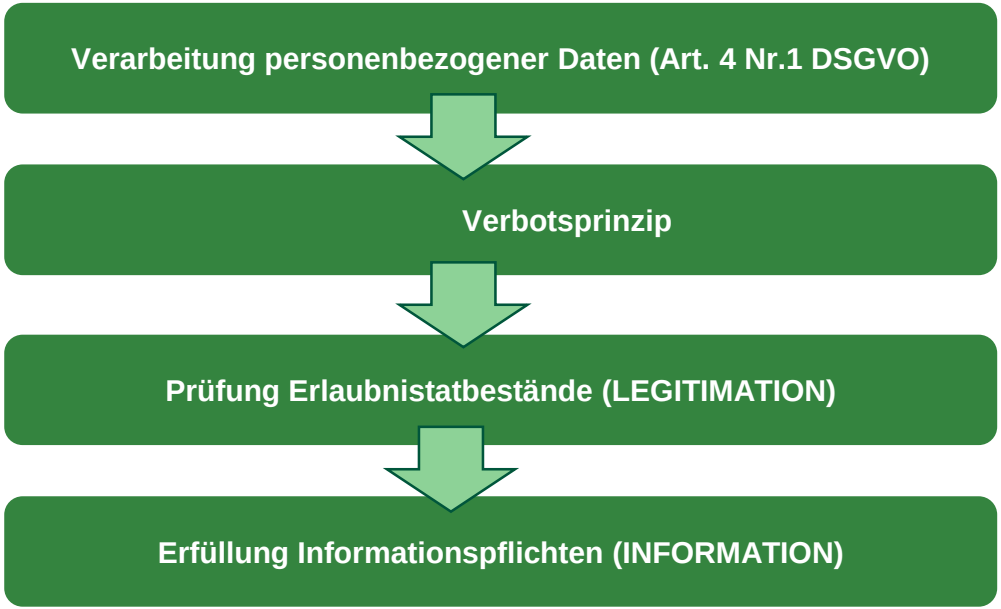
TEIL 3
DATENSCHUTZRECHT


tagesschau
Sendung verpasst?
Startseite ▸ Ausland ▸ Europa ▸ Künstliche Intelligenz: Italien sperrt ChatGPT
Welcome to ChatGPT
Log in with your OpenAI account to continue
Log in
Sign up
OpenAI
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



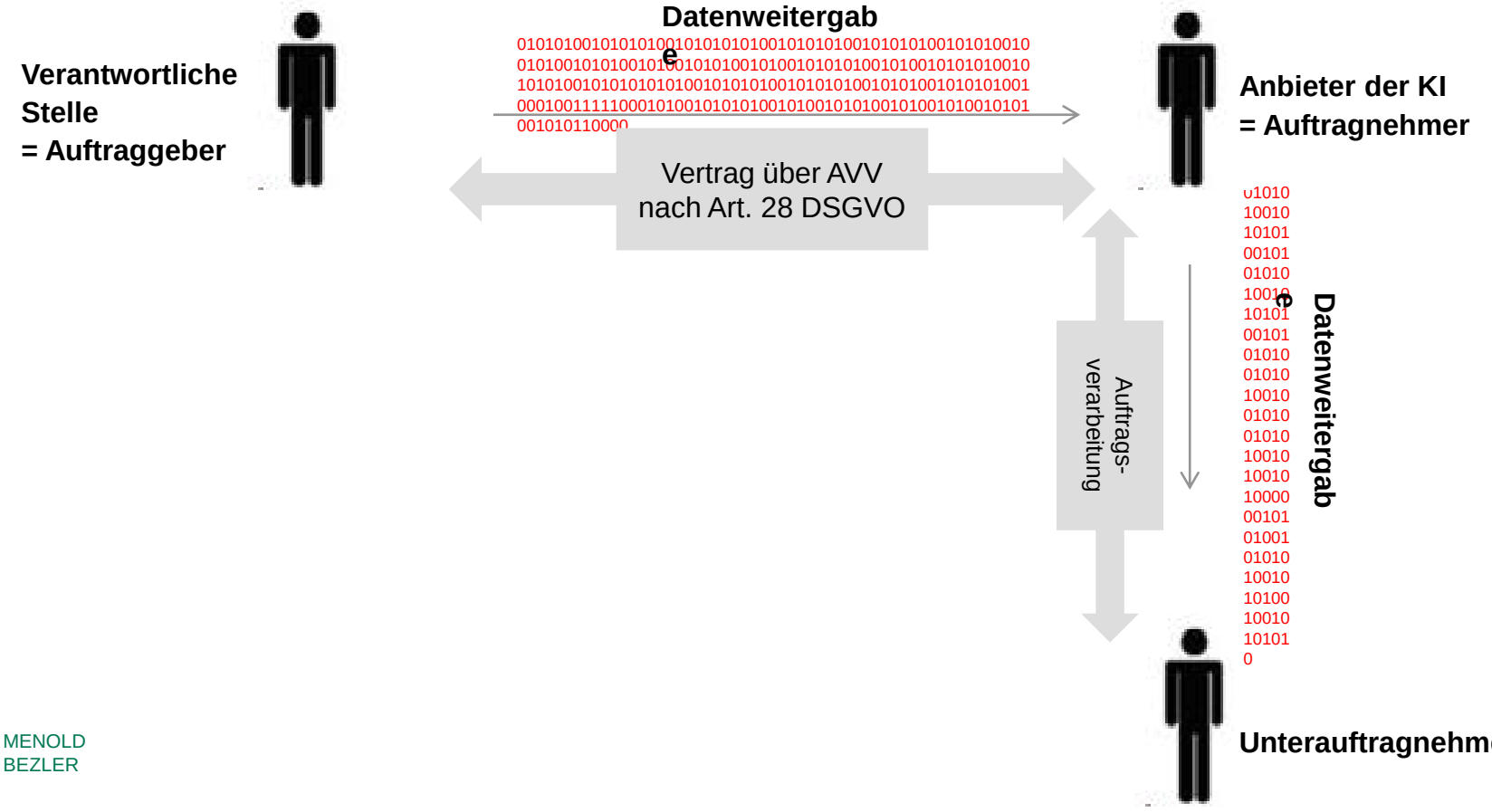
A. ZULÄSSIGKEIT DER DATENVERARBEITUNG



B. ÜBERSICHT DATENSCHUTZKONFORMITÄT



C. VERANTWORTLICHKEITEN



C. VERANTWORTLICHKEITEN

Auftragsverarbeitung (Art. 28 DSGVO)	**Gemeinsame Verantwortlichkeit (Art. 26 DSGVO)**	**Getrennte Verantwortlichkeit**
Auftraggeber entscheidet über **Zwecke und Mittel** der Datenverarbeitung	Gemeinsame Entscheidung über **Zwecke und Mittel** der Datenverarbeitung	Jeweils eigenständige Entscheidung über **Zwecke und Mittel** der Datenverarbeitung
• Abschluss eines Auftragsverarbeitungsvertrages zwingend	• Abschluss eines Joint Controllership Agreements zwingend • Gemeinsame Haftung im Außenverhältnis	• Unabhängige Datenverarbeitung
Sinnvolle Gestaltung bei Einsatz von KI-Systemen	**Eher unwahrscheinlich bei Einsatz bestehender KI-Systeme**	**Denkbare Gestaltung beim Einsatz bestehender KI-Systeme**

	ChatGPT Free	ChatGPT Plus	ChatGPT Team	ChatGPT Enterprise	OpenAI API	Microsoft Copilot	Microsoft Copilot Pro	Microsoft Copilot with commercial data protection	Microsoft Copilot for Microsoft 365	Microsoft Azure OpenAI Service	Google Bard	Google Vertex AI
Terms of use	Terms of use As of 15.2.2024 Europe Terms of Use		Business terms			Microsoft Services Agreement and additional conditions	Microsoft Services Agreement	Microsoft Services Agreement and additional conditions	Microsoft Customer Agreement and Microsoft Product Terms		Bard Privacy Hub Terms of Service	Google Cloud Platform Terms of Service
Data Processing Agreement (DPA)	Not available		OpenAI Data processing addendum			Not available	Not available	Not available	Microsoft Products and Services Data Protection Addendum (DPA)		Not available	Cloud Data Processing Addendum (Customers)
Use with personal data	No		Possible (if DPA is in place)			No	No	Not recommended (there is no DPA)	Possible		No	Possible
Use with confidential data	No		Possible (excluding official and professional secrets)			No	No	Not recommended (No confidentiality obligation)	Possible (legal professional secrets only if the correct amendments are in place)		No	Possible (legal professional secrecy only if additional contractual assurances are provided by Google)
Use for the provider's own purposes (e.g. training, service improvement)	Yes (Use for training can be deactivated)		No			Yes (Use for training and other purposes - including publication of the data by Microsoft)	Unclear (according to the Microsoft Privacy Statement at least partially possible)	No	No		Yes	No
Use within a company	**Possible with restrictions** (no personal data / no confidential data / training deactivated)		**Possible**			**Not recommended**	**Not recommended**	**Possible with restrictions** (no personal data / no confidential data)	**Possible**		**Not recommended**	**Possible**

Quelle: AI Tools - Data Protection (Overview EN) (rosenthal.ch)

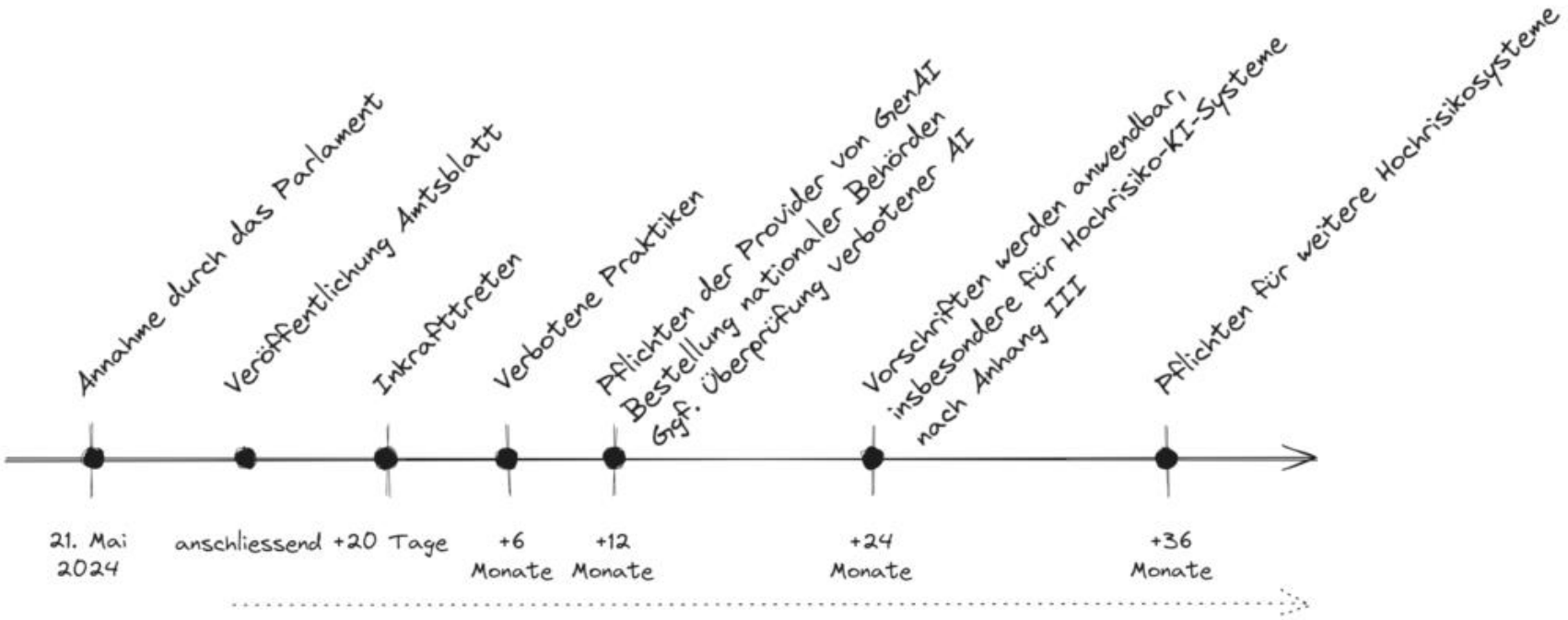


TEIL 4
KI-VERORDNUNG

A. KI-VERORDNUNG (AI-ACT)
GRUNDLAGEN

- Vorgaben für Anbieter, Betreiber, Nutzer, Händler, Einführer u.ä,
- Risikobasierter Ansatz
  - Verbotene KI-Systeme (Art. 5 KI-VO)
  - Hochrisikosysteme (Art. 6–49 KI-VO)
  - Transparenzpflichten (Art. 50 KI-VO)
  - KI-Modelle für allgemeine Zwecke (Art. 51-56 KI-VO)
- Bußgelder (bis zu 6% des Jahresbruttoumsatzes)
- KI-Haftungs-Richtlinie (AI Liability Directive)

B. KI-VERORDNUNG (AI-ACT)
UMSETZUNG



C. KI-VERORDNUNG (AI-ACT)
TRANSPARENZPFLICHTEN (ART. 50 KI-VO)

Transparenzpflicht für

- Anbieter von KI-Systemen, die für die direkte Interaktion mit natürlichen Menschen bestimmt sind (Abs. 1)
- Anbieter von GPAI, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen (Abs.2)
- Betreiber von Emotionserkennung oder eines Systems zur biometrischen Kategorisierung (Abs. 3)
- Betreiber eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake sind (Abs. 4 Satz 1)
- Betreiber eines KI-Systems, das Text erzeugt oder manipuliert, der veröffentlicht wird, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren (Abs. 4 Satz 2)



TEIL 5
UMSETZUNG VON KI-SYSTEMEN

A. EMPFEHLUNGEN ZUR AKTUELLEN RECHTSLAGE

- Rechtslage teilweise unklar
- Regulierung „hinkt“ hinterher
- Risikobasierter Ansatz statt Verbote
- Rechtliche Einschätzung erfordert klar definierte Anwendungsfälle
- Frühzeitige rechtliche Auseinandersetzung für Anbieter und Nutzer von KI-Systemen erforderlich
- Einführung technischer und organisatorischer Maßnahmen

B. TECHNISCHE AUSGESTALTUNG

- On-Premise vs. Software-as-a-Service
- (Datensparsame) Einstellung der Dienste
- Pseudonymisierung / Anonymisierung (soweit möglich)

C. ORGANISATORISCHE AUSGESTALTUNG

Einführung von Richtlinien

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

Durchführung von Schulungen (Art. 4 KI-VO)

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



TEIL 6
ZUSAMMENFASSUNG UND AUSBLICK

BEREITSTELLUNG UND NUTZUNG VON KI-SYSTEMEN
ZUSAMMENFASSUNG

- Risikobasierter Ansatz statt Verbote
- Rechtliche Einschätzung erfordert klar definierte Anwendungsfälle
- Frühzeitige rechtliche Auseinandersetzung für Anbieter und Nutzer von KI-Systemen erforderlich
- Ausgestaltung der Verträge mit Anbieter prüfen
- Einführung technischer und organisatorischer Maßnahmen

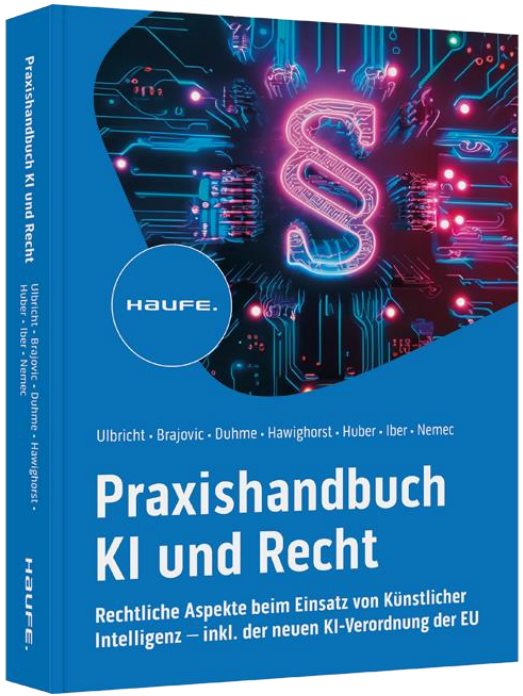
WEITERFÜHRENDE LINKS

- **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
- **Künstliche Intelligenz: Aktuelles zur KI-Verordnung**

  https://www.menoldbezler.de/blog/kuenstliche-intelligenz-aktuelles-zur-ki-verordnung

PRAXISHANDBUCH „KI & RECHT“



Dr. Carsten Ulbricht M.C.L.
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®

LinkedIn
twitter/intertainment