



# RECHTLICHE RAHMENBEDINGUNGEN FÜR DIE ARBEIT MIT KI UND DATEN

WEITERBILDUNGSPROGRAMM DATA SCIENCE & KÜNSTLICHE INTELLIGENZ 2023



# INHALT

- 1) Überblick über den rechtlichen Rahmen
- 2) Vorgaben für die Trainings- und Eingabedaten
- 3) Vorgaben für das KI-System
- 4) Haftungsrechtliche Fragen

# RECHTLICHER RAHMEN

- Welche Rechtsgebiete und Rechtsakte können relevant werden?
  - 1) Allgemeines Zivilrecht (insbes. BGB für vertrags- und haftungsrechtliche Fragen)
  - 2) Datenschutz (insbes. DSGVO)
  - 3) Immaterialgüterrecht (insbes. UrhG, GeschGehG)
  - 4) Europäisches Digitalrecht (insbes. KI-VO-E, KI-HaftungsRL-E)



# RECHTLICHE VORGABEN FÜR TRAININGS- UND EINGABEDATEN

DATENSCHUTZRECHTLICHE UND URHEBERRECHTLICHE BEDENKEN



# DATENSCHUTZ

- 1) Handelt es sich um eine Verarbeitung personenbezogener Daten?
  - Personenbezug = mind. Identifizierbarkeit einer natürlichen Person
- 2) Ist die Datenverarbeitung zulässig?
  - Rechtsgrundlage bspw. Einwilligung oder Interessenabwägung
- 3) Welche Pflichten ergeben sich?
  - Bspw. Informations- oder Löschpflichten

# PERSONENBEZOGENE DATEN

Datum ist auf irgendeine Art mit einer bestimmten natürlichen Person verknüpft

- Fahrplananzeige?
- Kfz-Kennzeichen?
- GPS-Daten zur Ortung eines Firmenfahrzeugs?
- Schrittzähler einer Kuh?
- Schriftliche Antworten in einer Prüfung?
- Sprachaufnahmen?
- IP-Adresse?

# RECHTMÄßIGKEIT DER VERARBEITUNG

## Grundsätze, Art. 5 DSGVO

- a) Rechtmäßigkeit, Treu und Glauben, **Transparenz**
- b) **Zweckbindung**
- c) **Datenminimierung**
- d) Richtigkeit
- e) Speicherbegrenzung
- f) Integrität und Vertraulichkeit

# RECHTMÄßIGKEIT DER VERARBEITUNG

Maßgebliche Vorschrift: Art. 6 DSGVO

- a) **Einwilligung**
- b) Erfüllung eines Vertrags
- c) Erfüllung einer rechtlichen Verpflichtung
- d) Erforderlich zu dem Schutz lebenswichtiger Interessen
- e) Öffentliches Interesse oder in Ausübung öffentlicher Gewalt
- f) **Wahrung berechtigter Interessen**

# BETROFFENENRECHTE

- Informationspflichten, Art. 13, 14 DSGVO
- Auskunftsanspruch, Art. 15 DSGVO
- Recht auf Berichtigung, Art. 16 DSGVO
- Recht auf Löschung, Art. 17 DSGVO
- Recht auf Einschränkung der Verarbeitung, Art. 18 DSGVO
- Recht auf Datenübertragbarkeit, Art. 20 DSGVO
- Widerspruchsrecht, Art. 21 DSGVO

# ANONYMISIERUNG

- Vorteil der Anonymisierung: Entfernung des Personenbezugs und damit der Anwendbarkeit der DSGVO
- Aber: Keine Einigkeit darüber, wann eine rechtssichere Anonymisierung vorliegt
- Objektive oder subjektive Betrachtung?
  - Obj. Betrachtung: keine Anonymisierung, wenn irgendjemand den Personenbezug wiederherstellen kann
  - Subj. Betrachtung: keine Anonymisierung, wenn Verantwortlicher den Personenbezug wiederherstellen kann

# SENSIBLE DATEN

- Besondere Kategorien personenbezogener Daten, Art. 9 DSGVO
  - Ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit
  - Genetische, biometrische oder Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung
- Verarbeitung grundsätzlich unrechtmäßig!

# FORSCHUNGSPRIVILEG

- DSGVO sieht gewisse Privilegien für wissenschaftliche Forschung vor
- Erlaubt:
  - (1) Verarbeitung sensibler Daten
  - (2) Einschränkung der Informations- und Löschpflichten
  - (3) Einschränkung von Auskunfts-, Berichtigungs-, Einschränkungs- und Widerrufsrechten der betroffenen Person
  - (4) Einfachere Zweckänderung

# URHEBERRECHT

Vorwurf der Urheberrechtsverletzung

## Bestsellerautoren reichen Sammelklage gegen ChatGPT-Hersteller OpenAI ein

John Grisham und George R.R. Martin werfen OpenAI vor, ihre Werke unerlaubt für ChatGPT zu nutzen. Zu ihren Beweisen zählt ein KI-Prequel zu »Game of Thrones«.

21.09.2023, 12.34 Uhr

Artikel zum Hören • 3 Min

Anhören



Foto: der Spiegel, John Grisham: RT und Dennis D. Martin: Ende AD

<https://www.spiegel.de/netzwelt/web/bestseller-autoren-reichen-sammelklage-gegen-chatgpt-hersteller-openai-ein-a-7a6eb560-425c-44e6-92f8-0dc6ecd8ba71>

heise online > Recht > Urheberrecht > Was darf KI? Stockfotograf und KI-Verein streiten um das Copyright

## Was darf KI? Stockfotograf und KI-Verein streiten um das Copyright

Ein Stockfotograf verklagt LAION — der gemeinnützige KI-Verein gibt an, geltendes Recht eingehalten zu haben. Der Streit wirft über den Fall hinaus Fragen auf.

Lesezeit: 14 Min. In Pocket speichern

59



(Bild: nep0/Shutterstock.com)

05.05.2023 16:48 Uhr | Developer

Von Silke Hahn

<https://www.heise.de/hintergrund/Was-darf-KI-Stockfotograf-und-KI-Verein-streiten-um-das-Copyright-8984836.html>

# URHEBERRECHT

- 1) Liegt ein Urheberrecht oder ein anderes nach UrhG geschütztes Recht vor?
  - Urheberrechtlich geschütztes Werk oder ein sog. Leistungsschutzrecht
- 2) Wurde dieses Recht verletzt?
  - Vornahme einer dem Urheber vorbehaltenen Handlung
- 3) War diese Verletzung widerrechtlich?
  - Rechtmäßigkeit durch gesetzliche Schranke oder Lizenzierung

# WERK

§ 2 Abs. 1 UrhG:

- a) Sprachwerke
- b) Musik
- c) Pantomimische Werke
- d) Werke der bildenden Künste
- e) Lichtbildwerke
- f) Filmwerke
- g) Darstellungen wissenschaftlicher oder technischer Art

## § 44b UrhG:TEXT UND DATA MINING

Drei Voraussetzungen für das Greifen der Schranke:

- 1) **Rechtmäßig zugängliche Werke**
  - Im Internet frei verfügbare Werke, Abruf ohne Rechtsverstoß möglich
- 2) **Erforderlichkeit der Nutzung für das Text und Data Mining**
  - Nach Ende der Nutzung müssen die Werke gelöscht werden
- 3) **Kein Opt Out des Urhebers**
  - Urheber hat der Nutzung nicht in maschinenlesbarer Form widersprochen

## § 60d UrhG: TEXT UND DATA MINING FÜR ZWECKE DER WISSENSCHAFTLICHEN FORSCHUNG

- Berechtigung für Forschungsorganisationen
- Auch anwendbar, wenn ein Opt Out des Urhebers vorliegt
- Erlaubt längerfristige Speicherung und Teilen der Daten mit einzelnen Dritten

# DATENQUALITÄT

- Aktuell noch keine einheitlichen Vorgaben zur Datenqualität bzgl. KI
- Art. 5 Abs. 1 lit. d DSGVO: Grundsatz der Datenrichtigkeit
  - Richtigkeit der mit den Daten übermittelten Informationen
- Art. 10 Abs. 1, 3 KI-VO-E
  - Daten sollen möglichst relevant, repräsentativ, fehlerfrei und vollständig sein

# KNOW-HOW-SCHUTZ

- Daten als Geschäftsgeheimnisse → Schutz durch das GeschGehG
- Wann liegt ein Geschäftsgeheimnis vor?
  - a) Information ist weder gesamt noch in Teilen allgemein bekannt oder ohne Weiteres zugänglich
  - b) Information wird durch angemessene Geheimhaltungsmaßnahmen geschützt
  - c) Berechtigtes Interesse an der Geheimhaltung



# RECHTLICHE VORGABEN FÜR DAS KI-SYSTEM

SCHUTZ DES SYSTEMS UND PFLICHTEN BEI DER NUTZUNG





# RECHTLICHER SCHUTZ DES KI-SYSTEMS?



# SCHUTZ DES KI-SYSTEMS?

- Schutz als Computerprogramm?
  - iErg wird nur der Quellcode, nicht die errechneten Parameter geschützt sein
  - Bei Nachahmung: Unterlassungs- sowie Beseitigungs- und Schadensersatzansprüche
- Schutz als Datenbank?
  - Einzelne Bestandteile lassen sich nicht unabhängig voneinander betrachten

# SCHUTZ DER KI-ERZEUGNISSE?

- Im Mittelpunkt der Diskussion: generative KI
- Maßgeblich: inwieweit hat der Mensch noch Kontrolle über den Schaffensprozess?
  - Kontrolle durch Erstellen des Modells?
  - Kontrolle durch Prompt?
  - Kontrolle durch nachträglichen Eingriff?



# PFLICHTEN BEI DER NUTZUNG EINES KI-SYSTEMS



# EXKURS: KI-VO-E

- Zukünftiges Hauptregelungswerk für KI in der EU
- Risikobasierter Ansatz: unterschiedliche Regelungen je nach Risiko der Nutzung des KI-Systems
  - a) „Verbotene Systeme“: bspw. Social Scoring, Echtzeit-Gesichtserkennung im öffentlichen Raum
  - b) „Hochrisiko-Systeme“: hohes Risiko für Gesundheit, Sicherheit und Grundrechte natürlicher Personen
  - c) „Bestimmte Systeme“: insbes. generative Modelle
  - d) „Restliche Systeme“: keine spezifischen Pflichten

# PFLICHTEN BEI DER NUTZUNG: KI-VO-E

- Bei Hochrisiko-Systemen: Einführung eines Risikomanagementsystems, Dokumentations- und Informationspflichten, CE-Konformitätskennzeichnung, weitere spezifische Pflichten je nach Rolle (Anbieter, Produkthersteller, Einführer, Händler, Nutzer)
- Bei bestimmten Systemen: Transparenzpflichten gegenüber Nutzern
  - Information darüber, dass Interaktion mit einer KI stattfindet

# PFLICHTEN BEI DER NUTZUNG: DSGVO

Risikobasierter Ansatz: zu treffende Maßnahmen, um die datenschutzrechtlichen Grundsätze zu wahren, müssen anhand des bestehenden Risikos für Grundrechte und Freiheiten der betroffenen Person analysiert werden

- Privacy by Design und Privacy by Default: Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
- Dokumentationspflichten: insbes. Verzeichnis über alle Verarbeitungstätigkeiten
- Ggf. Datenschutzfolgenabschätzung

Folge eines Verstoßes: ggf. Schadensersatzanspruch

# PFLICHTEN BEI DER NUTZUNG: PRODUKTSICHERHEIT

- Aktuelles Produktsicherheitsgesetz gilt nur für körperliche Gegenstände
- Überarbeitung der Produktsicherheitsrichtlinie als Verordnung: auch Software soll erfasst werden
- Sicherheit des Produktes muss nach Inverkehrbringen weiter gewährleistet werden, insbes. durch Updates



# HAFTUNG BEI DEM EINSATZ VON KI

WER MUSS FÜR DIE KI EINSTEHEN?



# HAFTUNG

RECHTLICHE SCHRITTE

## Von KI erstellt? Ärger um erfundenes Schumacher-Interview

AKTUALISIERT AM 20.04.2023 · 16:14



Seit einem schweren Unfall lebt Michael Schumacher zurückgezogen. Nun hat eine Zeitschrift mithilfe einer KI ein Interview mit ihm erstellt. Schumachers Familie will rechtliche Schritte einleiten.

MERKEN ☆ 10 | 1 Min.

# HAFTUNG

TECH **Artificial Intelligence** Help Desk Internet Culture Space Tech Policy

INNOVATIONS

## ChatGPT invented a sexual harassment scandal and named a real law prof as the accused

The AI chatbot can misrepresent key facts with great flourish, even citing a fake Washington Post article as evidence

By [Pranshu Verma](#) and [Will Oremus](#)

April 5, 2023 at 2:07 p.m. EDT



<https://www.washingtonpost.com/technology/2023/04/05/chatgpt-lies/>

# HAFTUNG

ChatGPT

## Bürgermeister in Australien will KI-Unternehmen OpenAI wegen Falschaussagen verklagen

Den Entwicklern der auf künstlicher Intelligenz (KI) beruhenden Anwendung ChatGPT droht erstmalig eine Verleumdungsklage. Der Bürgermeister einer australischen Kleinstadt wird von dem Programm fälschlicherweise als Krimineller bezeichnet.

07.04.2023



Wo sind die Grenzen der KI? (Imago / Christian Ohde)

<https://www.deutschlandfunk.de/buergermeister-in-australien-will-ki-unternehmen-openai-wegen-falschaussagen-verklagen-102.html>

# RECHTSGRUNDLAGEN: BGB

§§ 280ff. BGB: Nur anwendbar, wenn ein Vertrag zwischen den Parteien besteht

§§ 823ff. BGB: Deliktische Haftung

- § 823 Abs. I BGB als wichtigste Anspruchsgrundlage
  - a) Verletzung eines Rechtsguts (Leben, Körper, Gesundheit, Freiheit, Eigentum oder ein sonstiges Recht)
  - b) Verletzungshandlung
  - c) Kausalität zwischen Verletzungshandlung und der Verletzung
  - d) Widerrechtlichkeit
  - e) Verschulden
  - f) Schaden (Einbuße infolge der Rechtsgutverletzung)
- Zurechenbarkeit über § 83 I S. I BGB?

# RECHTSGRUNDLAGEN: PRODUKTHAFTUNG

- Ziel: Absicherung von Nutzern gegen fehlerhafte Produkte
- a) Verletzung eines Rechtsguts? Körper, Gesundheit, Sachen
- b) Produkt?
  - Aktuelles Produkthaftungsgesetz gilt nur für körperliche Gegenstände
  - Neuerung mit überarbeiteter ProdHaftRL:
    - „Produkt“ kann auch eine Software sein
- c) Fehler?
  - Für Vorliegen eines Produktfehlers ist zukünftig auch die Lernfähigkeit eines Produktes zu beachten
- d) Keine Entlastung des Herstellers

# BEWEISSCHWIERIGKEITEN

- Autonomierisiko: Risiko, dass die KI schädigende Entscheidung selbstständig ohne menschliches Verschulden trifft
  - Risiko bei geschädigter Person
- Opazitätsrisiko: Risiko, dass Entscheidungsfindung nicht mehr nachvollziehbar ist, sodass die Auswirkungen einer menschlichen Pflichtverletzung auf das Ergebnis nicht feststellbar sind
  - Risiko bei geschädigter Person

# BEWEISSCHWIERIGKEITEN: KI-HaftungsRL-E

- Anwendungsbereich:
  - Grundsätzlich anwendbar auf alle KI-Systeme
  - Nichtvertragliche, verschuldensabhängige Schadensersatzansprüche
- Beweislastregelungen: Kausalität wird vermutet, wenn...
  - relevante Beweise nicht offengelegt wurden oder der Anspruchsteller nachweist, dass Sorgfaltspflichten verletzt wurden,
  - nach vernünftigem Ermessen die Sorgfaltspflichtverletzung das schädliche Ergebnis beeinflusst haben kann, und
  - der Kläger nachweist, dass das schädliche Ergebnis den Schaden verursacht hat



VIELEN DANK FÜR EURE AUFMERKSAMKEIT!

