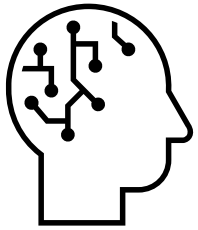
proIT
Verband der IT-Profis in Liechtenstein

HARTMANN BECK
Rechtsanwälte AG



KI und Recht



Ein Wegweiser für die Praxis
von Rechtsanwalt Tobias Beck

Hartmann Beck Rechtsanwälte AG

HARTMANN BECK
Rechtsanwälte AG

RA Tobias Beck

Seit 2025 Rechtsanwalt und Mitgründer der **Hartmann Beck Rechtsanwälte AG**

Seit 2021 Mitglied der Beschwerdekommission für Verwaltungsangelegenheiten (VBK)

Seit 2020 **Rechtsanwalt in Liechtenstein**

2020 Anwaltsprüfung Liechtenstein

2019 Anwaltsprüfung Schweiz

2016 Abschluss des **rechtswissenschaftlichen Studiums**



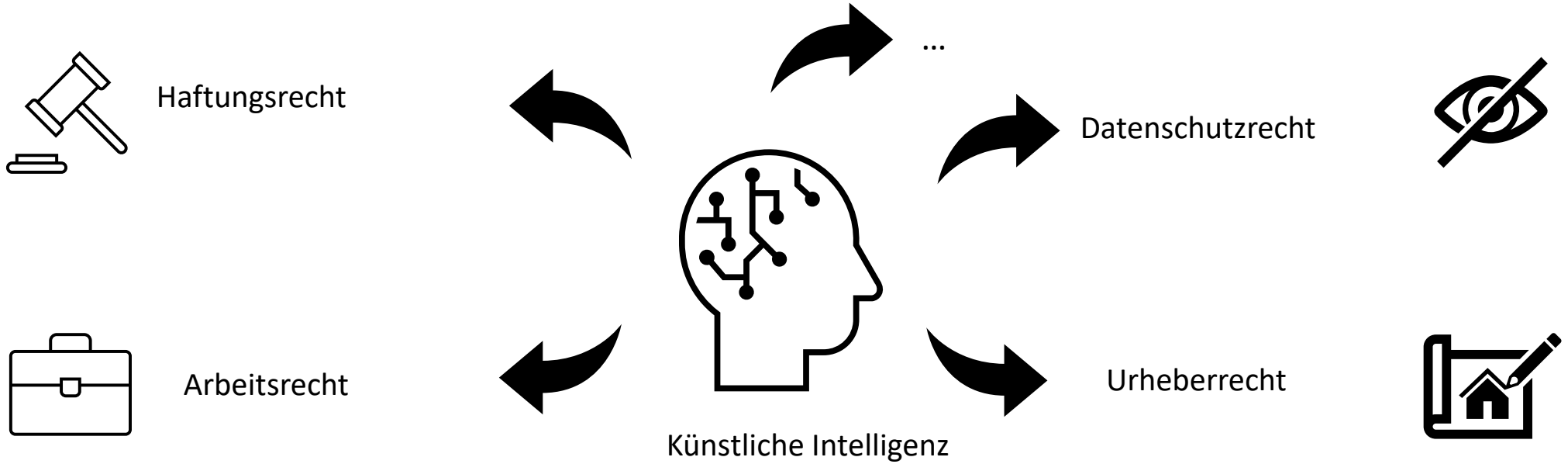
Vortragsprogramm

HARTMANN BECK
Rechtsanwälte AG

- Einleitung
- Die KI-Verordnung der EU
- Datenschutz / DSGVO
- Urheberrecht: Wem gehört was?
- Last but not least: Arbeitsrechtliche Aspekte

KI als rechtliche Querschnittsmaterie

HARTMANN BECK
Rechtsanwälte AG



Die EU KI-Verordnung („EU AI-Act“)

HARTMANN BECK
Rechtsanwälte AG

- Eigentlich: *„VO (EU) 2024/1689“*

- In der EU in Kraft seit August 2024
  - Gestaffelte Anwendbarkeit der Bestimmungen bis 2027

  <u>Auch für FL von Relevanz!</u>

- KI-Definition (Art. 3 Z 1):

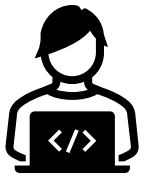
1. „KI-System“ ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte,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

EU KI-VO: Who is who

HARTMANN BECK
Rechtsanwälte AG

VO (EU) 2024/1689

schreibt Pflichten vor für



Betreiber:
kommerzielle Nutzer,
z.B. Ihr Unternehmen

stellen zur Verfügung

Anbieter:
z.B. Open AI

Nutzen im Geschäftsbetrieb

Kunden

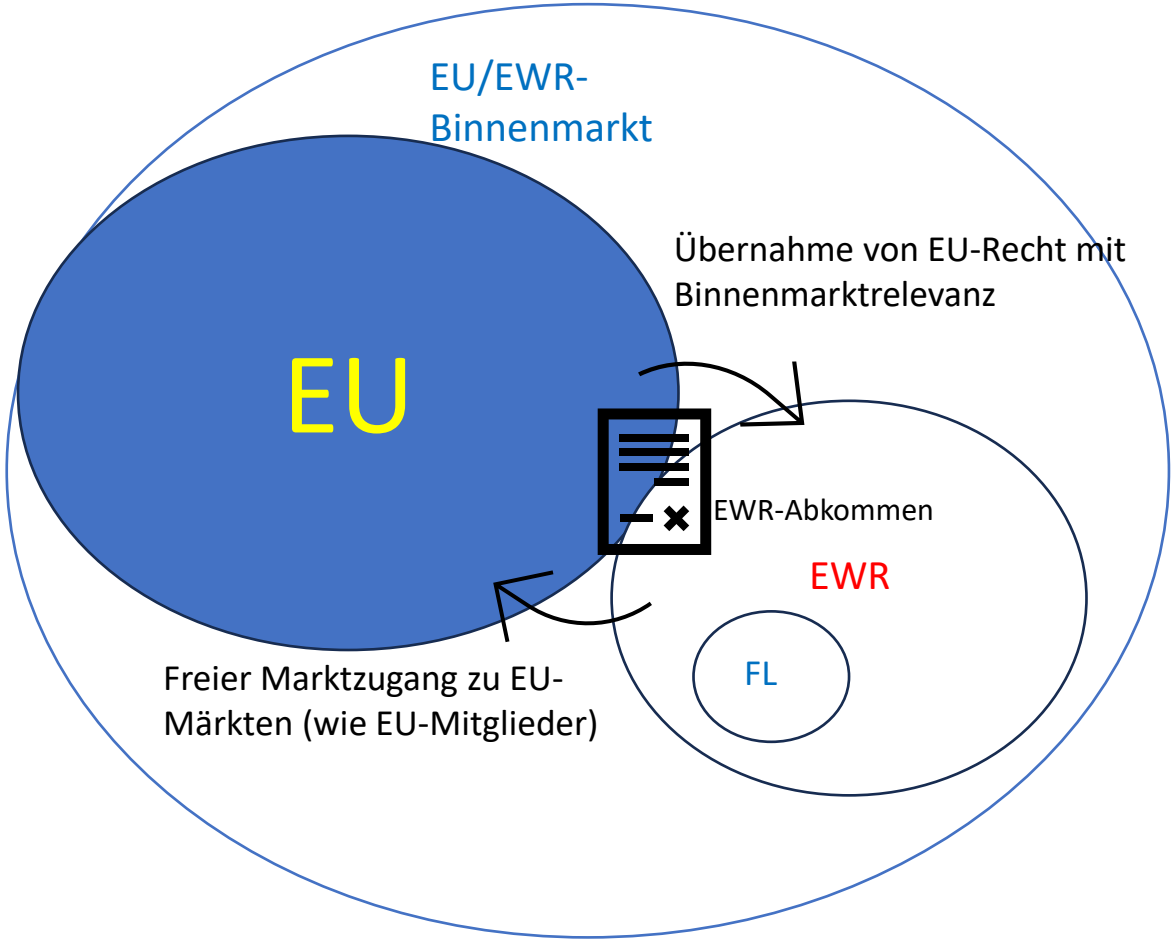
Exkurs: EU, EWR und die Anwendbarkeit in FL

HARTMANN BECK
Rechtsanwälte AG

Die KI-VO gilt bereits für alle Anbieter, die in der EU geschäftstätig sind, unabhängig davon, wo sie sich selbst befinden!

> *Bsp.: FL-Unternehmen erbringt Dienstleistungen in D und nutzt dabei ein KI-Modell von OpenAI*

FL als EWR-Mitglied: EWR übernimmt mit Zeitverzögerung EU-Recht und somit auch die EU KI-VOt!



Inkrafttreten: Timeline

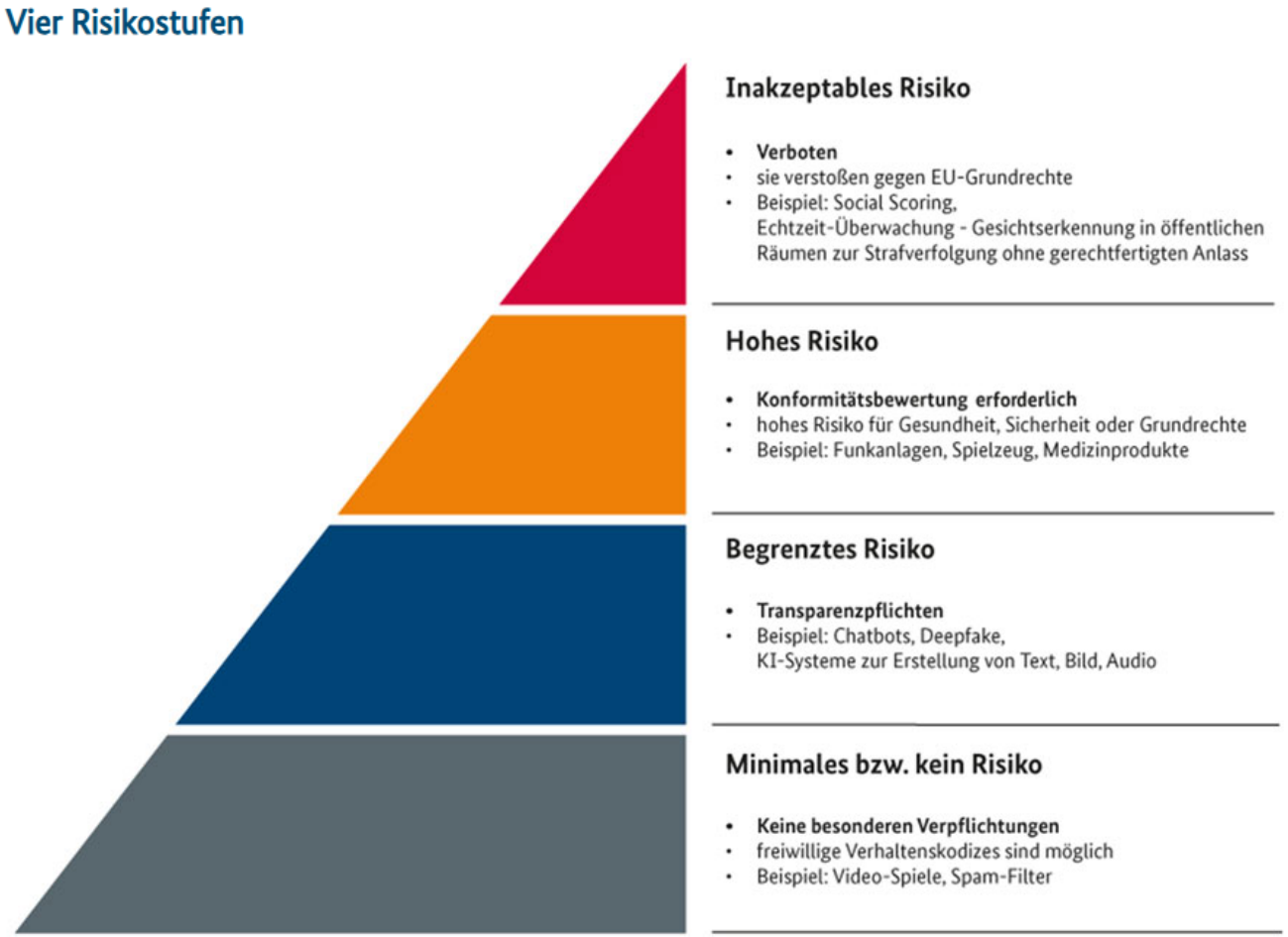


Achtung: Wenn FL-Unternehmen in der EU tätig sind, gilt die KI-VO schon für sie!

In der Zukunft: EWR-Beschluss für Übernahme der KI Verordnung im EWR mit Inkraftreteten für FL (noch nicht erfolgt)

Risikostufen der KI-VO

- Zentrale Idee: „Risikobasierter Ansatz“
- Je grösser das Risiko, desto strenger die Vorschriften



Quelle: Bundesnetzagentur, https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/2_Risiko/start_risiko.html (09.10.2026)

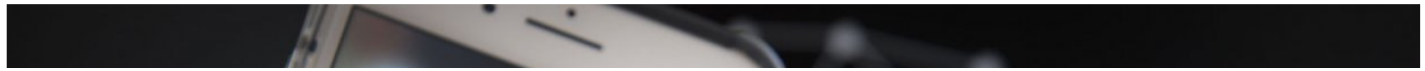
Beispiel I:

HARTMANN BECK
Rechtsanwälte AG

Microtargeting und Manipulation: Von Cambridge Analytica zur Europawahl

Constanze Kurz Ingo Dachwitz
02.05.2019 / 6 Minuten zu lesen

Bei digitaler Desinformation geht es nicht nur um die Inhalte, sondern auch um deren Adressierung. Diese Lehre lässt sich unter anderem daraus ziehen, wie Nutzerdaten von Facebook durch eine fragwürdige Firma von der Trump-Kampagne im US-Präsidentschaftswahlkampf 2016 verwendet wurden.



Quelle: www.bpb.de

Beispiel II:

HARTMANN BECK
Rechtsanwälte AG



NACKTFOTOS IM NETZ

Sexualisierte KI-Deepfakes von 138 Politikerinnen gefunden – auch Lena Schilling betroffen

Eine EU-weite Studie fand zahlreiche Webseiten mit KI-generierten Nacktfotos von Politikerinnen. Auch die Grünen-Abgeordnete Lena Schilling wurde zum Opfer. Sie fordert schnelleres Handeln

Gustav Andree
28. September 2026, 16:07

Quelle: www.derstandard.at

Beispiel III:

HARTMANN BECK
Rechtsanwälte AG





Quelle: *T. J. Thomson/R. J. Thomson/Matich*, Generative Visual AI in News Organizations: Challenges, Opportunities, Perceptions, and Policies, Digital Journalism 2024, https://doi.org/10.1080/21670811.2024.2331769 (09.10.2026)

Transparenzpflicht bei „Deepfakes“

HARTMANN BECK
Rechtsanwälte AG

- Definition „Deepfake“ (Art. 3 Z 60):

60. „Deepfake“ einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde;

- Transparenzpflicht (Art. 50 (4))

(4) Betreiber eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake sind, müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden. Diese Pflicht gilt nicht, wenn die Verwendung zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten gesetzlich zugelassen ist. Ist der Inhalt Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms, so beschränken sich die in diesem Absatz festgelegten Transparenzpflichten darauf, das Vorhandensein solcher erzeugten oder manipulierten Inhalte in geeigneter Weise offenzulegen, die die Darstellung oder den Genuss des Werks nicht beeinträchtigt.

Transparenzpflicht bei „Deepfakes“ gem. Art. 50 (4)

HARTMANN BECK
Rechtsanwälte AG

KI-generierter (veränderter) Bild-, Ton- oder Videoinhalt?

Ja



Könnten Menschen den Inhalt fälschlicherweise für wahr halten (= Deepfake) ?*

Keine Transparenzpflicht

Nein

Ja

Text zur Information über öffentliche Angelegenheiten?

Nein

Keine Transparenzpflicht

Ja

Redaktionelle (menschliche) Kontrolle?

Ja

Nein

Bsp.: KI-generierte Zeitungsartikel, die ohne menschliche Prüfung veröffentlicht werden

Transparenzpflicht (Kennzeichnun

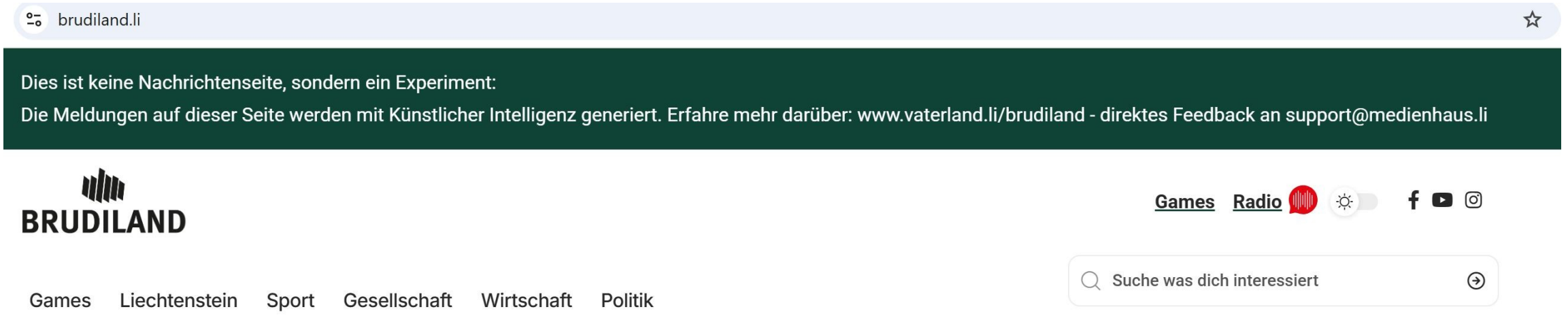


AI GENERATED

AI MODIFIED

Beispiel IV:

HARTMANN BECK
Rechtsanwälte AG



Quelle: www.brudiland.li

Beispiel V:

HARTMANN BECK
Rechtsanwälte AG

AUTONOMES TÖTEN

Ukrainischer Drohnen-Kommandeur "Magyar": Verlieren die Kontrolle über KI

Autonome Waffen werden nicht mehr lange durch Menschen steuerbar sein, sagt der Pionier des Drohnenkriegs

Peter Zellinger
7. Oktober 2026, 12:00

238 Postings | Später lesen



Major Robert Brovdi, alias 'Magyar' in seiner geheimen Drohnezentrale.

Quelle: www.derstandard.at

Risikostufen: Beispiele

HARTMANN BECK
Rechtsanwälte AG

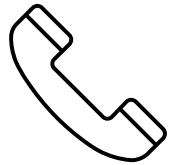
Risikostufe	Regelung	Bsp.
Inakzeptables Risiko	idR Verboten (mit Ausnahmen innerhalb sehr enger Grenzen – z.B. Gesichtserkennung durch Staat bei Terrorismusabwehr)	Sozialkredit-System, Biometrische Überwachung von Menschen Manipulation von Menschen mit KI
Hohes Risiko	Erlaubt, aber sehr strenge Regeln ➢ Ausnahme: Mensch trifft die Entscheidung („Human in the Loop“)	Medizinprodukte automatisierte Personaleinstellung Bildung, Justiz, Bonitätsprüfung/Kreditvergabe
Begrenztes Risiko	Erlaubt, ggf. Regeln	Chatbots, KI-generierte Bilder und Texte
Minimales bis kein Risiko	Erlaubt	KI-gestützte Spamfilter reine Übersetzungsprogramme

Sonstige, praktisch wichtige Regeln

HARTMANN BECK
Rechtsanwälte AG



Kompetenzpflicht (Art. 4): Betreiber und Anbieter müssen ihr Personal schulen (Grundverständnis)



Meldepflicht: Schwere Vorfälle (Tod/Verletzung von Menschen, Grundrechtsverletzung) müssen dem Anbieter und der zuständigen KI-Überwachungsbehörde gemeldet werden!



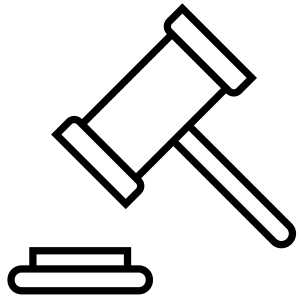
Betrieb und Aufsicht: Menschliche Kontrolle sicherstellen, Bedienung gem. Betriebsanleitung

Strafen bei Verstössen

HARTMANN BECK
Rechtsanwälte AG

- **Sanktionen (Strafen):**

bis 35 Mio. € / 7 % Umsatz (Art. 99)



- **Achtung:**

Dazu können uU noch Zivilrechtliche Haftungsansprüche kommen (z.B. Schadensersatz)!



HARTMANN BECK
Rechtsanwälte AG



DATENSCHUTZ / DSGVO



Was bedeutet “DSGVO-konform?”

HARTMANN BECK
Rechtsanwälte AG



Der Anbieter meint damit meistens, dass er eigene Pflichten erfüllt:

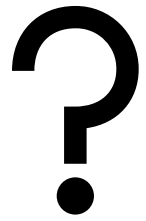
- Auftragsverarbeitungsvertrag nach Art. 28 DSGVO
- Technische und organisatorische Massnahmen nach Art. 32 DSGVO
- Unterstützung bei Betroffenenrechten und Datenpannen
- Regelungen für Unterauftragsverarbeiter

→ Das Tool ist damit grundsätzlich nutzbar. Der konkrete Einsatz bleibt aber Ihre Verantwortung.

Die fünf Fragen vor jedem Einsatz

HARTMANN BECK
Rechtsanwälte AG

1. Welche Daten werden verarbeitet?
2. Für welchen Zweck?
3. Wer ist verantwortlich?
4. Welche Rechtsgrundlage besteht?
5. Welche Risiken und Schutzmassnahmen gibt es?



Personenbezogene Daten

HARTMANN BECK
Rechtsanwälte AG

Alle Informationen, die sich auf eine Person beziehen oder beziehen lassen.

Beispiele:

Namen, E-Mail-Adressen, Kundendaten, Stimmen, Gesprächsinhalte, interne Dokumente.

Auch scheinbar anonymisierte Daten können personenbezogen bleiben, wenn Rückschlüsse möglich sind.

Besonders geschützte Daten

HARTMANN BECK
Rechtsanwälte AG

Besonders geschützte Personendaten

- biometrische Daten
- Gesundheitsdaten
- politische Ansichten
- Religion
- Gewerkschaftszugehörigkeit

Für diese Daten gelten zusätzlich die strengeren Voraussetzungen von Art. 9 DSGVO.

Verantwortlicher oder Auftragsverarbeiter?

HARTMANN BECK
Rechtsanwälte AG

Das Unternehmen ist in der Regel Verantwortlicher.

Der KI-Anbieter ist häufig Auftragsverarbeiter.

Dann braucht es eine Vereinbarung nach Art. 28 DSGVO (Auftragsdatenverarbeitungsvertrag; AVV).

Beispiel

HARTMANN BECK
Rechtsanwälte AG

Auftragsdatenverarbeitungsvertrag nach Art. 28 Abs 3 Datenschutz-Grundverordnung (DSGVO)

zwischen

Firma/Name	
Strasse	
Plz-Ort	
Land / Staat	
Telefon, E-Mail, www	

- nachstehend **Auftraggeber** genannt -

und der

Verlag für Neue Medien GmbH
Freiburger Str. 33
79427 Eschbach - Bundesrepublik Deutschland

- nachstehend **Auftragnehmer** genannt -

1. Gegenstand, Grundsätzliches und Dauer des Auftrags

1.1.Gegenstand des Auftrags

Der Auftragnehmer stellt dem Auftraggeber je nach Leistungsangebot gegen Entgelt oder unentgeltlich Serverkapazitäten im Internet z.B. zum Betrieb einer Internetseite, zum Emp-

Quelle: Verlag für Neue Medien (www.vfnm.de)

Rechtsgrundlage und Zweck

HARTMANN BECK
Rechtsanwälte AG

Jede Verarbeitung braucht eine Rechtsgrundlage.

Mögliche Rechtsgrundlagen sind insbesondere:

- Vertragserfüllung
- berechtigtes Interesse
- Einwilligung
- gesetzliche Verpflichtung

Weitere Pflichten

HARTMANN BECK
Rechtsanwälte AG

Zweckbindung · Datenminimierung · Transparenz · Speicherbegrenzung

Zu prüfen sind insbesondere:

- Information nach Art. 13 und 14 DSGVO
- Betroffenenrechte nach Art. 15 bis 21 DSGVO
- Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO
- Datenschutz-Folgenabschätzung nach Art. 35 DSGVO
- Schutz vor unzulässigen automatisierten Entscheidungen nach Art. 22 DSGVO

Datenschutz-Folgenabschätzung

HARTMANN BECK
Rechtsanwälte AG

Eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO ist insbesondere zu prüfen bei:

- grossen Datenmengen
- sensiblen oder vertraulichen Daten
- automatisierten Entscheidungen
- neuen Technologien mit hohem Risiko

Bei generativer KI ist eine DSFA häufig zumindest ernsthaft in Betracht zu ziehen.

Server im EWR

HARTMANN BECK
Rechtsanwälte AG

Im „EWR gehostet“ beantwortet nur die Frage nach dem Speicherort

In diesem Fall liegt grundsätzlich keine Drittlandübermittlung nach Art. 44 ff. DSGVO vor

Entscheidend bleibt:

- Können US-Stellen auf Daten zugreifen?
- Werden Daten für eigene Zwecke oder für das Modelltraining verwendet?

US-CLOUD Act

HARTMANN BECK
Rechtsanwälte AG

- US-Zugriff trotz europäischem Serverstandort?
- Der US-CLOUD Act kann US-Anbieter unter bestimmten Voraussetzungen zur Herausgabe von Daten verpflichten.
- Das kann auch Daten betreffen, die physisch im EWR gespeichert sind.
- EWR-Hosting beseitigt das Zugriffsrisiko nicht vollständig.

US-CLOUD Act

HARTMANN BECK
Rechtsanwälte AG

115TH CONGRESS
2D SESSION

H. R. 4943

To amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 6, 2018

Mr. COLLINS of Georgia (for himself, Mr. JEFFRIES, Mr. ISSA, Ms. DELBENE, Mr. MARINO, Mr. RUTHERFORD, and Mrs. DEMINGS) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on Rules, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Clarifying Lawful Overseas Use of Data Act" or the "CLOUD Act".

Quelle: congress.gov

Zero Retention

HARTMANN BECK
Rechtsanwälte AG

Zero Retention bedeutet, dass Eingaben und Ausgaben nach der Verarbeitung nicht gespeichert werden.

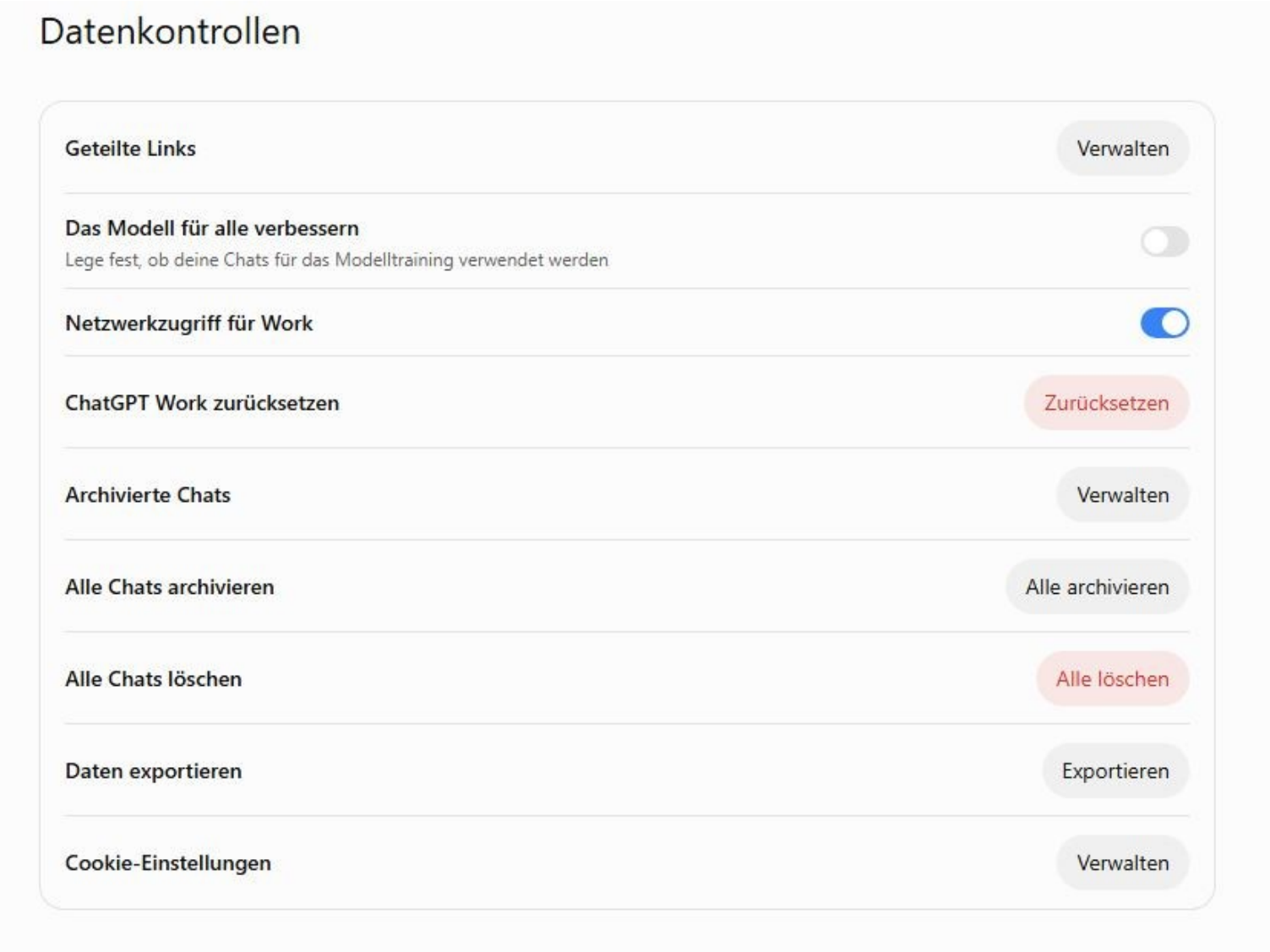
Das ist mehr als ein Ausschluss des Modelltrainings.

Auch bei Zero Retention können Daten kurzfristig verarbeitet oder gespeichert werden:

- Technische Zwischenspeicher
- Metadaten
- Sicherheitslogs

ChatGPT

HARTMANN BECK
Rechtsanwälte AG



ChatGPT Enterprise

HARTMANN BECK
Rechtsanwälte AG

Kann OpenAI mir bei der Einhaltung der DSGVO und anderer Datenschutzgesetze helfen?

Ja, wir können mit Kund:innen einen Zusatz zur Datenverarbeitung (Data Processing Addendum, DPA) für ihre Nutzung von ChatGPT Business, ChatGPT Enterprise und der API abschließen, um sie bei der Einhaltung der DSGVO und anderer Datenschutzgesetze zu unterstützen. Bitte fülle unser DPA-Formular aus, um einen DPA mit OpenAI abzuschließen. Für ChatGPT Edu und für Lehrkräfte verarbeiten wir deine Daten gemäß unserer Vereinbarung zum Schutz von Schülerdaten.

ChatGPT

HARTMANN BECK
Rechtsanwälte AG

Bei ChatGPT sind insbesondere folgende Punkte zu prüfen:

- Opt-out oder vertraglicher Ausschluss des Trainings
- Ausschluss des Trainings bedeutet noch keine DSGVO-Konformität
- Auftragsdatenverarbeitungsvertrag

Microsoft 365 und Copilot

HARTMANN BECK
Rechtsanwälte AG

Microsoft Copilot erfüllt gemäss eigenen Angaben die Anforderungen an die DSGVO.

ⓘ Wichtig

- Microsoft Copilot, einschließlich Microsoft Copilot Search, erfüllt unsere bestehenden Verpflichtungen in Bezug auf Datenschutz, Sicherheit und Compliance gegenüber kommerziellen Microsoft 365-Kunden, einschließlich der Datenschutz-Grundverordnung (DSGVO) und der Datengrenze der Europäischen Union (EU).
- Prompts, Antworten und Daten, auf die über Microsoft Graph zugegriffen wird, werden nicht zum Trainieren von Foundation LLMs verwendet, einschließlich derjenigen, die von Microsoft Copilot verwendet werden.
- Microsoft Copilot arbeitet mit mehreren Schutzmaßnahmen, die unter anderem das Blockieren schädlicher Inhalte, das Erkennen geschützter Materialien und das Blockieren von Prompt-Injektionen (Jailbreak-Angriffe) umfassen.
- Informationen zu Modellen, die von Anthropic als Unterauftragsverarbeiter in Microsoft Copilot-Erfahrungen bereitgestellt werden, finden Sie unter Anthropic-Modelle in Microsoft Online Services.
- Informationen zu Modellen, die von OpenAI als Unterauftragsverarbeiter in Microsoft Copilot bereitgestellt werden, finden Sie unter OpenAI als Unterauftragsverarbeiter in Microsoft Online Services.

EU Data Boundary von Microsoft

HARTMANN BECK
Rechtsanwälte AG

Ein wichtiger Schritt, aber kein vollständiger Schutz

Microsoft verspricht, Daten europäischer Kunden grundsätzlich innerhalb der EU bzw. des EWR zu speichern und zu verarbeiten.



Ausnahmen und Restrisiken bleiben möglich, etwa bei:

- Cybersicherheitsvorfällen
- technischem Support
- besonderen Betriebsprozessen

Copilot

HARTMANN BECK
Rechtsanwälte AG

- Copilot greift auf EU-gehostete Daten zu. Es bleiben die Restrisiken wie beim Microsoft.
- Copilot findet alles, worauf der jeweilige Nutzer Zugriff hat. Zu weit gefasste Berechtigungen können zum Problem werden.
- In der Regel ist eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) nötig.



Microsoft Copilot und Data Residency

Microsoft Copilot hält die Verpflichtungen zur Datenresidenz ein, wie in den Microsoft-Produktbedingungen und dem Nachtrag zum Datenschutz beschrieben. Microsoft Copilot wurde am 1. März 2024 als abgedeckte Workload in die Datenresidenzverpflichtungen in den Microsoft-Produktbedingungen aufgenommen.

Microsoft Advanced Data Residency (ADR) und Multi-Geo Capabilities-Angebote umfassen Datenresidenzverpflichtungen für Microsoft Copilot-Kunden ab dem 1. März 2024. Für EU-Kunden ist Microsoft Copilot ein EU-Datenbegrenzungsdienst. Kunden außerhalb der EU können ihre Abfragen in den USA, in der EU oder in anderen Regionen verarbeiten lassen.

Beispiel: Automatische Zusammenfassung eines Teams Calls

HARTMANN BECK
Rechtsanwälte AG

- Eine KI verarbeitet dabei möglicherweise Stimme, Bild, Meinungen, Namen etc.
- Verantwortlich ist grundsätzlich das Unternehmen, das die Funktion aktiviert.

Empfohlenes Vorgehen:

- Vorab transparent informieren
- Zustimmung einholen (oder alternative Rechtsgrundlage) und bei Ablehnung Funktion deaktivieren

ISO/IEC 27001

HARTMANN BECK
Rechtsanwälte AG

ISO/IEC 27001 ist eine international anerkannte Norm für Informationssicherheitsmanagement.

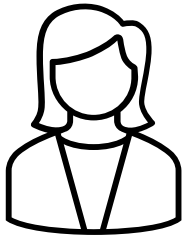
Eine ISO/IEC-27001-Zertifizierung bedeutet nicht automatisch:

- DSGVO-Konformität
- Zulässigkeit jeder Verarbeitung
- vollständige Sicherheit vor Datenverlust



Die Norm unterstützt Datenschutz und Compliance. Sie ersetzt aber keine Datenschutzprüfung.

HARTMANN BECK
Rechtsanwälte AG



ARBEITSRECHT / URHEBERRECHT



Arbeitsrechtliche Aspekte

HARTMANN BECK
Rechtsanwälte AG

KI-basiertes, automatisches Recruiting = Hochrisikosysteme

→ Problem: Diskriminierung

- KI-basierte Mitarbeiterbeurteilung = Hochrisikosysteme selbst bei „Human in the Loop“
- Art. 22: Verbot automatisierter Entscheidungen

Urheberrecht an KI-Tools

HARTMANN BECK
Rechtsanwälte AG

Software ist urheberrechtlich geschützt. Computerprogramme gelten als Werke.

Geschützt sein können insbesondere:

- Quellcode
- Objektcode
- Programmteile

Voraussetzung ist eine individuelle geistige Schöpfung.

Fremde Inhalte in KI-Systemen

HARTMANN BECK
Rechtsanwälte AG

Das Hochladen fremder Dokumente kann insbesondere eine Vervielfältigung darstellen.

Vor dem Upload muss daher geklärt werden, ob die erforderlichen Rechte bestehen.

Text und Data Mining

HARTMANN BECK
Rechtsanwälte AG

Training ist nicht automatisch erlaubt.

Mit dem künftigen Art. 26g URG soll erstmals eine urheberrechtliche Erlaubnis für allgemeines Text und Data Mining geschaffen werden.

Schlussbotschaft

HARTMANN BECK
Rechtsanwälte AG

Ein verantwortungsvoller Einsatz verlangt:

- klare Zwecke
- minimale Daten
- passende Verträge
- beschränkte Zugriffe
- menschliche Kontrolle



Vielen Dank!

proIT
Verband der IT-Profis in Liechtenstein