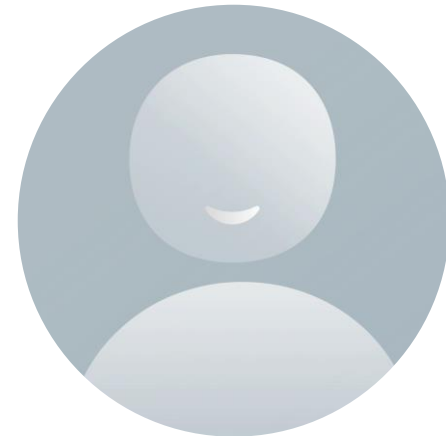




Multimedia Kontor Hamburg

Ein Unternehmen der
Hamburger Hochschulen



Neue Regeln zur künstlichen Intelligenz (KI) - Was bedeutet das für Hochschulen?!

Inhalte der KI-Verordnung & Bezüge zu OpenData & zum
Datenschutz- & Urheberrecht





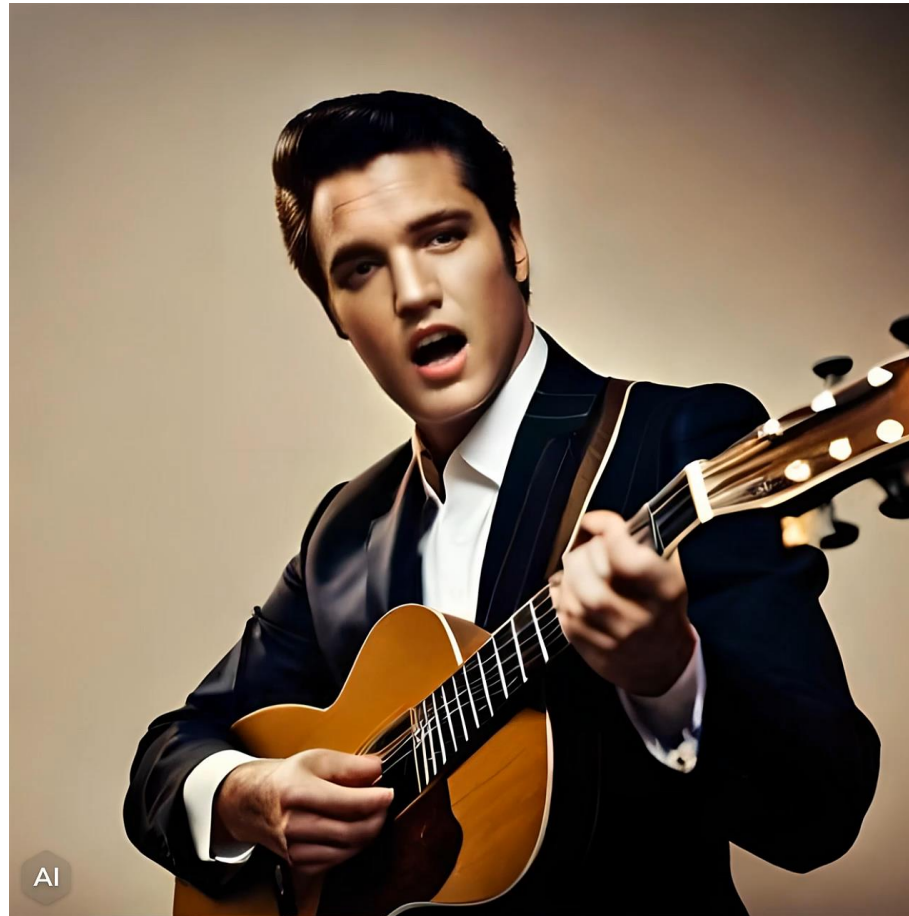
Neue Regeln zur künstlichen Intelligenz (KI) - Was bedeutet das für Hochschulen?!

Inhalte der KI-Verordnung & Bezüge zu OpenData & zum
Datenschutz- & Urheberrecht





Worum geht es? Zum Beispiel?





Worum geht es? Zum Beispiel?

Nach dem Entwurf (noch kein Gesetz!) der KI-Verordnung (sog. AI-Act) würde gelten: Nutzer eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die wirklichen Personen, Gegenständen, Orten oder anderen Einrichtungen oder Ereignissen merklich ähneln und einer Person fälschlicherweise als echt oder wahrhaftig erscheinen würden („Deepfake“), müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden.

Zum Beispiel: „AI by Meena Stavesand“

- Text von Meena Stavesand und zusammengefügt über ChatGPT
 - Bild erstellt mit: <https://www.bluewillow.ai>
 - Sprache umgesetzt mit: <https://beta.elevenlabs.io>
 - Alles zusammengefügt und generiert mit D-ID: <https://studio.d-id.com/>
-



Worum geht es? Zum Beispiel!

Die KI-Anwendung „Replika“

Die italienische Datenschutzbehörde (Garante per la protezione dei dati personali – GPDP) ließ mit Bescheid vom 02.02.2023 die Datenverarbeitung durch die **Chat-Anwendung „Replika“** des US-amerikanischen Unternehmens Luka Inc. gem. Art. 58 Abs. 2 lit. f DS-GVO einschränken und forderte das Unternehmen auf, die festgestellten Datenschutzverstöße zu beseitigen (GPDP v. 02.02.2023; vgl. Etteldorf ZD-Aktuell 2023, 01088).

„Replika“ ist eine KI-basierte Chat-Seelsorge. Sie soll die Stimmung und das emotionale Wohlbefinden verbessern können und dabei helfen, Stress und Ängste zu bewältigen, indem die Nutzenden laut Aussage der Betreiber täuschend echt wirkende Gespräche mit einem Chatbot führen können. Der Werbeslogan lautet: „The AI companion who cares – Always here to listen and talk. Always on your side“ (Luka Inc. v. 30.5.2023; vgl. Etteldorf ZD-Aktuell 2023, 01088).



Worum geht es? Zum Beispiel!

Die KI-Anwendung „Replika“

Konkret beanstandete die Behörde einen **unzureichenden Schutz besonderer Kategorien personenbezogener Daten, insbesondere bei Minderjährigen**. Die App sei zwar in Italien mit einer Altersbeschränkung von 17 Jahren versehen, allerdings finde keine Überprüfung des Alters statt. Nicht einmal, wenn Nutzende im Chat erklären, sie seien minderjährig, werde das Programm abgebrochen (GPDP v. 02.02.2023). In den Datenschutzhinweisen erklärte Luka Inc., dass wissentlich keine Daten von Minderjährigen unter 13 Jahren verarbeitet würden (Luka Inc. v. 02.02.2023). Anders als Deutschland hat Italien von der Öffnungsklausel für die Altersgrenze bei Einwilligungen in Art. 9 Abs. 1 S. 3 DS-GVO Gebrauch gemacht. Dennoch ermöglicht Art. 2d des italienischen Datenschutzgesetzes (Codice in materia di protezione dei dati personali) eine Einwilligung von Minderjährigen erst ab 14 Jahren – in Deutschland liegt sie weiterhin bei 16 Jahren. Die **Unklarheit bei der Verarbeitung personenbezogener Daten von minderjährigen Personen** wertete die GPDP als einen **Verstoß gegen das Transparenzgebot** nach Art. 5 Abs. 1 lit. a DS-GVO sowie **gegen die Informationspflichten** aus Art. 13 DS-GVO (GPDP v. 02.02.2023).



Worum geht es? Zum Beispiel!

Die KI-Anwendung „Replika“

Darüber hinaus bedürfe die Verarbeitung von **besonderen Kategorien personenbezogener Daten einer besonderen Rechtfertigung gem. Art. 9 DS-GVO**. Dass die Informationen über die mentale Gesundheit der Nutzenden zu den besonderen Kategorien gehören, ergibt sich aus Art. 4 Nr. 15 DS-GVO. Danach sind Gesundheitsdaten solche „personenbezogenen Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“.

Bis heute (Stand: 11.07.2023) ist die Anwendung „Replika“ in Italien gesperrt (s. garanteprivacy.it vom 01.06.2023). Ob Gespräche zwischen Luka Inc. und GPDP stattfinden, ist nicht bekannt.



Workshop - Inhaltsübersicht

- Zum Verständnis des Regelungskontextes: **Gesamtüberblick europäische Datenstrategie & EU-Digitalgesetzgebung**: von der DSGVO über DGA/DSA/DMA bis zur Open Data-Richtlinie und zum AI-Act
- Schwerpunkt dieses Workshops: **AI-Act**, d.h. die Entwürfe KI-Verordnung (**insbesondere** sog. „Hochrisiko-KI“, **weniger** KI-Nutzung wie im „Elvis“-Beispiel) & KI-Richtlinie
- Sonderprobleme: **keine neuen Regeln**, daher hier nur „Randthemen“ ganz zum Schluss:
 - Datenschutz & Persönlichkeitsrechte
 - Urheberrecht
- **Nicht** Inhalt dieses Workshops sind prüfungsrechtliche Fragen, dazu mehr beim Online-Workshop "KI-Generatoren in der Hochschul(lehr)e – Potenziale und rechtliche Implikationen von ChatGPT, DALL-E & Co." vom 14. März 2023: Herausforderungen für das Prüfungsrecht an Hochschulen (Prof. Dr. Dirk Heckmann, TUM)

KI-GENERATOREN IN DER HOCHSCHUL[LEHR]E

Potenziale und rechtliche Implikationen
von ChatGPT, DALL-E & Co.

ONLINE-VERANSTALTUNG

14. März 2023, 10:00 – 12:30 via Zoom

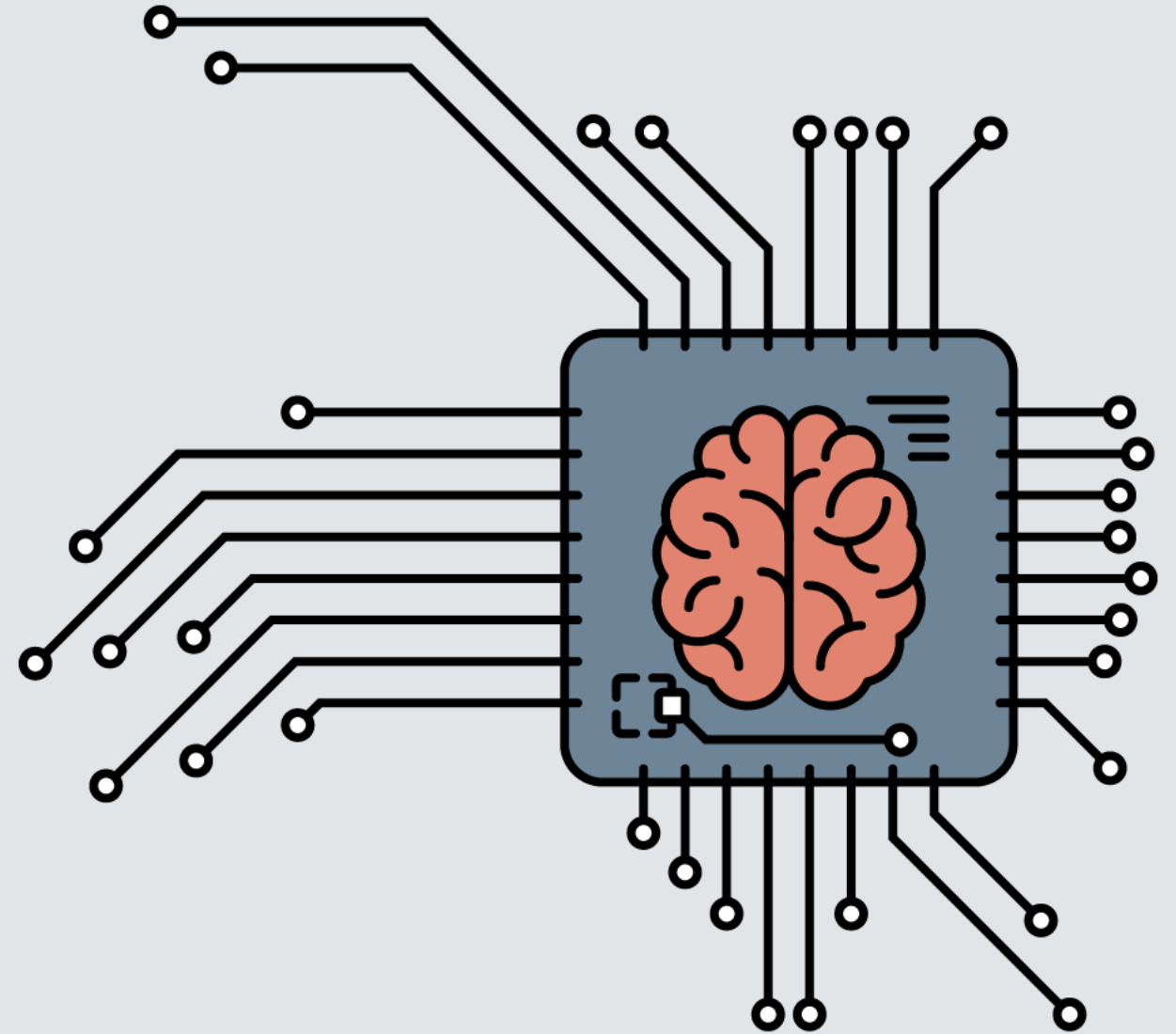
VORTRAGENDE

Prof. Dr. Christian Spannagel, PH Heidelberg

Prof. Dr. Dirk Heckmann, TUM

Jens O. Brelle, MMKH

Dr. Janine Horn, ELAN e.V.



MMKH.DE

Die europäische Datenstrategie





Die europäische Datenstrategie

- Im Februar 2020 veröffentlichte die EU-Kommission die **europäische Datenstrategie** – einen **Rahmenplan für den digitalen Wandel der EU**, welcher den Austausch und die Nutzung von Daten erleichtern sowie die Entwicklung eines EU-Binnenmarkts für Daten fördern soll. Hierin enthalten sind **vier strategischen Säulen**:
 - Schaffung eines sektorübergreifenden Governance-Rahmens für den Zugang zu und die Nutzung von Daten.
 - Förderung von Investitionen in Daten, Dateninfrastrukturen
 - Stärkung der Kontrolle des Einzelnen über seine Daten und digitaler Kompetenzen
 - Schaffung von gemeinsamen, sektorspezifischen europäischen Datenräumen (Data Spaces) in verschiedenen strategischen Sektoren und Gesellschaftsbereichen von öffentlichem Interesse.
-



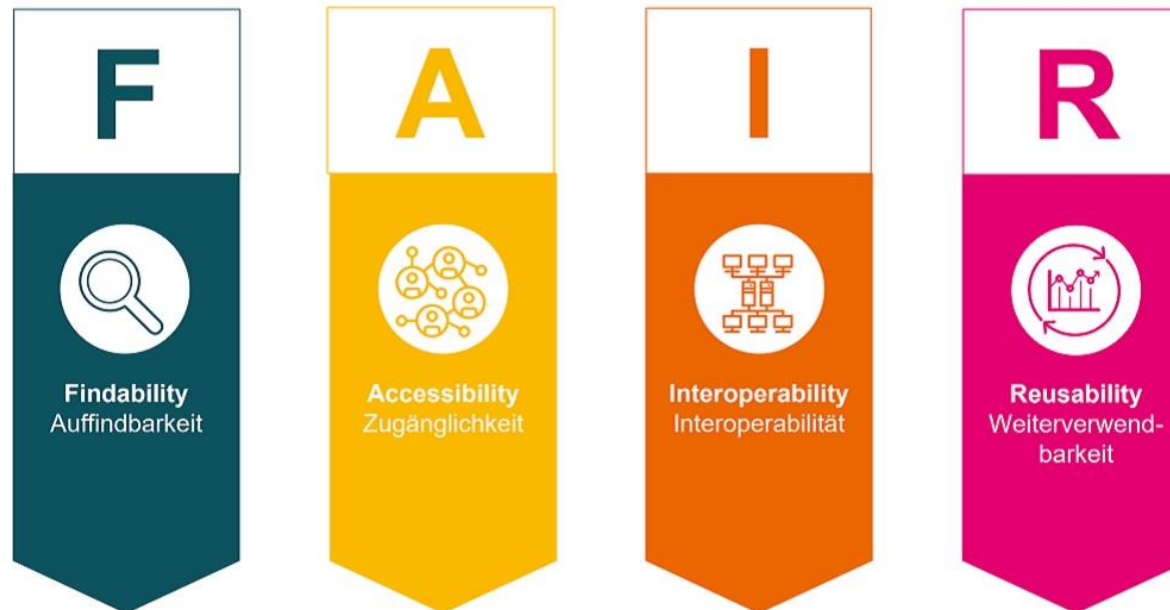
Die europäische Datenstrategie

- Mit der Datenstrategie wird eine enge **Verzahnung der Digitalpolitik mit der Umsetzung des europäischen Grünen Deals** betont. Die **Dekarbonisierung** und der **Übergang zu einer nachhaltigen Kreislaufwirtschaft** stehen somit **im Fokus einer innovativen Datennutzung**.
 - Die Strategie selbst enthält noch keine verbindlichen Verordnungen oder Richtlinien, sondern bildet die strategische Grundlage für die folgende Gesetzgebungen und flankierende Maßnahmen.
-



Die europäische Datenstrategie

Die Europäische Datenstrategie
Die FAIR-Datengrundsätze



Übersicht EU-Digitalgesetzgebung





Übersicht EU-Digitalgesetzgebung

- Datenschutz-Grundverordnung (DSGVO)
 - Richtlinie über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt (DSM-RL), z.B. auch Text & Data Mining
 - E-Privacy-Richtlinie bzw. E-Privacy-Verordnung
 - Digital Markets Act (DMA)
 - Digital Services Act (DSA)
 - Data Act (DA)
 - eIDAS & European Digital Identity Regulation
 - Verordnung zur Festlegung harmonisierter Vorschriften über künstliche Intelligenz (AI-Act): Verordnung über den europäischen Raum für Gesundheitsdaten (EHDS)
-



Übersicht EU-Digitalgesetzgebung

- Data Governance Act (DGA)
 - KI-Verordnung (AI-Act)
 - KI-Richtlinie
-



Datenschutz-Grundverordnung (DSGVO)

- **Worum geht es:** Schutz personenbezogener Daten & Durchsetzung des Rechts auf informationelle Selbstbestimmung natürlicher Personen
 - **Stand der Dinge:** Unmittelbare Geltung in der EU seit 25.05.2018
 - **Wer ist betroffen:** Verantwortliche Stellen (Ausnahme: Haushaltsprivileg), die personenbezogene Daten verarbeiten
-



Datenschutz-Grundverordnung (DSGVO)

- EU/US-Data Privacy Framework kommt im Juli 2023

beck-online berichtet am 05.07.2023, dass der EU-Kommissar für Justiz Didier Reynders verlauten ließ, dass der Angemessenheitsbeschluss für den EU/US-Datenschutzrahmen möglicherweise in der Woche vom 10. bis 14.07.2023 angenommen werde.

Diese Annahme wird durch eine Agenda der 21. Sitzung des Ausschusses nach Art.93 DS-GVO v. 29.06.2023 gestützt. Unter Tagesordnungspunkt 1 wird sinngemäß folgender Punkt zur Diskussion gestellt: „Diskussion über die überarbeitete Fassung des **Entwurfs des Durchführungsbeschlusses gemäß der DS-GVO über die Angemessenheit des Schutzniveaus personenbezogener Daten gemäß des Datenschutzrahmens zwischen der EU und den USA** (die Ausschussmitglieder werden gebeten, keine Stellungnahme zum Entwurf des Durchführungsbeschlusses in dieser Sitzung abzugeben). Auf Grund der Aufforderung an die Ausschussmitglieder in dieser Sitzung keine Stellungnahme abzugeben, ist davon auszugehen, dass in dieser Sitzung noch nicht abgestimmt werden soll und ein weiterer Termin für die Abstimmung angesetzt wird“



Datenschutz-Grundverordnung (DSGVO)

- **EU/US-Data Privacy Framework am 10.07.2023 in Kraft getreten**

Lt. BfDI Meldung vom 10.07.2023 um 17:38h:

„Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework in Kraft getreten: Die Europäische Kommission hat heute den Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework (Nachfolger des „Privacy Shields“) angenommen. Der Angemessenheitsbeschluss kann nunmehr als Grundlage für Datenübermittlungen an zertifizierte Organisationen in den USA dienen.“

Vollständiger Angemessenheitsbeschluss der EU-Kommission vom 10.07.2023

<https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework.pdf>



Datenschutz-Grundverordnung (DSGVO)

- **EU/US-Data Privacy Framework am 10.07.2023 in Kraft getreten**

Der durch den Beschluss nun in Kraft tretende Datenpakt führe neue und verbindliche Garantien ein, um alle vom Europäischen Gerichtshof geäußerten Bedenken auszuräumen, heißt es in einer Pressemitteilung der EU-Kommission. So werde etwa der **Zugriff von US-Geheimdiensten auf EU-Daten auf ein notwendiges und verhältnismäßiges Maß beschränkt.**

Zudem soll ein **spezielles Gericht** aufgebaut werden, zu dem EU-Bürger Zugang haben und das die **Einhaltung von Datenschutzmaßnahmen prüft**. Stelle jenes Gericht fest, dass Daten unter Verstoß gegen die neuen Richtlinien erhoben wurden, könnte es die Löschung der Daten anordnen, betont die EU-Kommission. US-Unternehmen könnten dem Pakt beitreten, indem sie sich verpflichten, eine Reihe von Datenschutzverpflichtungen einzuhalten.



Datenschutz-Grundverordnung (DSGVO)

- Kritik am EU/US-Data Privacy Framework: the same procedure?

Der SPIEGEL berichtet am 11.07.2023, Zitat: Schrems, der inzwischen die Bürgerrechtsorganisation noyb mitgegründet hat, kommentierte zum Abkommen: **»Man sagt, die Definition von Wahnsinn ist, dass man immer wieder das Gleiche tut und dennoch ein anderes Ergebnis erwartet. (...) Wir hatten jetzt ›Harbors‹, ›Umbrellas‹, ›Shields‹ und ›Frameworks‹ – aber keine substantielle Änderung des US-Überwachungsrechts.«** Die aktuellen Presseerklärungen seien fast eine wortwörtliche Kopie derer von vor 23 Jahren. **»Die bloße Behauptung, etwas sei ›neu‹, ›robust‹ oder ›wirksam‹, reicht vor dem Gerichtshof nicht aus«,** so Schrems. **»Wir brauchten eine Änderung des US-Überwachungsrechts und die gibt es nicht.«**



Datenschutz-Grundverordnung (DSGVO)

- Kritik am EU/US-Data Privacy Framework: the same procedure?

Der SPIEGEL berichtet am 11.07.2023, Zitat: *Ralf Wintergerst, der Präsident des Tech-Branchenverbands Bitkom, sagte hingegen, mit dem »Data Privacy Framework« gehe »eine dreijährige Hängepartie« zu Ende: »Unternehmen erhalten damit grundsätzlich wieder Rechtssicherheit, wenn sie personenbezogene Daten zwischen der EU und den USA transferieren müssen.« Allerdings betonte auch Wintergerst, dass abzusehen sei, »dass die nun gefundene Neuregelung erneut von den Gerichten überprüft werden wird«: »Dort wird sich zeigen, ob der EU-Gesetzgeber mit dem »Data Privacy Framework« eine rechtlich belastbare Regelung gefunden hat.«*



Datenschutz-Grundverordnung (DSGVO)

- **Trans-Atlantic Data Privacy Framework (TADPF) – Einsatz von US-Dienstleistern nun DSGVO-sicher?**

Checkliste von Dr. Thomas Schwencke vom 10.07.2023

<https://datenschutz-generator.de/data-privacy-framework>



Richtlinie über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt (DSM-RL)

- **Worum geht es:** Verschärfung des Urheberrechts im Internet. Neuregelung der urheberrechtlichen Verantwortlichkeit. Statuierung von einheitlichen Ausnahmen für die Verwendung von Inhalten für Zwecke des Zitats, der Kritik, der Rezension, der Karikatur, der Parodie und der Pastiche.
 - **Stand der Dinge:** Die Richtlinie wurde im April 2019 verabschiedet; der Umsetzungsakt in Deutschland „Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarkts“ ist am 07.06.2021 in Kraft getreten. Die Regelungen zur urheberrechtlichen Verantwortlichkeit von Upload-Plattformen im Urheberrechts-Diensteanbieter-Gesetz (UrhDaG) folgten zum 01.08.2021.
 - **Wer ist betroffen:** Insbesondere Online-Content-Sharing Plattformen (Upload-Plattformen)
-



E-Privacy-Richtlinie bzw. E-Privacy-Verordnung

- **Worum geht es:** Der europäische Gesetzgeber hat sich entschlossen, die Datenschutzrichtlinie für elektronische Kommunikation (sog. E-Privacy-Richtlinie) durch eine E-Privacy-Verordnung zu ersetzen. Nachdem der deutsche Gesetzgeber zuletzt mit einer Novelle des Telekommunikationsgesetzes (TKG) und dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) zum 01.12.2021 noch die europäischen Vorgaben aus der E-Privacy-Richtlinie in deutsches Recht umsetzte, wird die künftige E-Privacy-Verordnung unmittelbar in den Mitgliedstaaten gelten.
 - **Stand der Dinge:** Ursprünglich sollte vom 25.05.2018 an zusammen mit der Datenschutz-Grundverordnung (DSGVO) auch die ePrivacy-VO gelten. Doch anders als bei der DSGVO konnten sich die EU-Staaten im Falle der ePrivacy-VO bis heute noch auf keinen gemeinsamen Gesetzentwurf einigen. Voraussichtliches Inkrafttreten Ende 2023, voraussichtliche unmittelbare Geltung Ende 2025.
-



E-Privacy-Richtlinie bzw. E-Privacy-Verordnung

- **Wer ist betroffen:** Ziel der Verordnung ist es, die Regeln zur elektronischen Kommunikation an die Datenschutz-Grundverordnung (DSGVO) anzunähern, ohne dabei über die Vorschriften der DSGVO hinauszugehen. Eines der großen Ziele der Verordnung ist die Erweiterung der Datenschutzregeln auf sogenannte Over-the-Top (OTT)-Kommunikationsdienste. Hierzu zählen beispielsweise Voice over IP (VoIP)-Dienste wie WhatsApp und Skype, die in ihrer Funktion den „klassischen“ Sprachtelefonie- und SMS-Diensten entsprechen.
-



Digital Markets Act (DMA)

- **Worum geht es:** Regulierung der digitalen Märkte und insbesondere sehr großer Online-Plattformen.
 - **Stand der Dinge:** Der DMA wurde am 14.09.2022 vom Europäischen Parlament und vom Rat angenommen und am 12.10.2022 im Amtsblatt veröffentlicht. Zum 01.11.2022 ist das EU-Gesetz über digitale Märkte (DMA) in Kraft getreten und gilt ab dem 02.05.2023.
 - **Wer ist betroffen:** Insbesondere Betreiber zentraler Plattformdienste, welche als „Gatekeeper“ einzuordnen sind.
 - **Im Detail:** Die Einordnung als Gatekeeper orientiert sich hauptsächlich an den Auswirkungen der Plattform auf den Binnenmarkt, der Vermittlereigenschaft zwischen gewerblichen Nutzern und Endnutzern und der (absehbaren) Festigkeit und Dauerhaftigkeit der Tätigkeit der Plattform.
-



Digital Services Act (DSA)

- **Worum geht es:** Schaffung eines sicheren digitalen Raums, der frei von illegalen Inhalten ist und einen Schutz der Grundrechte der Nutzer gewährleistet.
 - **Stand der Dinge:** Das Gesetz über digitale Dienste wurde am 23. April 2022 vom Europäischen Parlament und vom Rat angenommen. Am 27. Oktober 2022 wurde es im Amtsblatt veröffentlicht. Damit tritt das Gesetz zum 16. November 2022 in Kraft und gilt ab dem 17. Februar 2024 in allen EU-Staaten.
 - **Wer ist betroffen:** Alle Anbieter von Vermittlungsdiensten (Intermediäre), darunter insbesondere Anbieter von Online-Plattformen. Gestufte Regulierung für Vermittlungsdienste, Host-Provider, Online-Plattformen und sehr große Online-Plattformen.
-



Digital Services Act (DSA)

- **Im Detail:** Umfassende Regelungen beispielsweise betreffend die Haftung, den Umgang mit illegalen Inhalten, des Vorsehens eines „Notice-and-Takedown“-Verfahrens und der Regulierung (sehr großer) Online-Plattformen. Insbesondere die Haftungsregeln bringen allerdings nicht wirklich viele Neuerungen mit sich. Die Frage nach dem „Ob“ der Haftung richtet sich weiterhin nach den Regelungen der Mitgliedsstaaten.
-



Data Act (DA)

- **Worum geht es:** Gewährleistung einer gerechten Verteilung der Wertschöpfung aus Daten aus dem Internet der Dinge auf die Akteure der Datenwirtschaft und Förderung des Datenzugang und der Datennutzung.
 - **Stand der Dinge:** Die Europäische Kommission hat zur Umsetzung der europäischen Datenstrategie am 23.02.2022 den Vorschlag für einen Data Act veröffentlicht. Das Europäische Parlament hat am 14.03.2023 mit großer Mehrheit seine Position zum Entwurf der EU-Kommission beschlossen. Auch der EU-Ministerrat hat sich auf eine gemeinsame Position zum Data Act geeinigt. Das Gesetzgebungsvorhaben wurde mit den sogenannten Trilog-Verhandlungen zwischen Parlament, EU-Kommission und Mitgliedstaaten fortgesetzt. Diese endeten am 28.06.2023. Das Gesetzgebungsverfahren könnte Ende 2023 abgeschlossen werden und in einem Gesetz münden. Mit einem Inkrafttreten des Data Act wäre dann Ende 2024 zu rechnen. Sobald die EU das Gesetz verabschiedet, muss es in den Mitgliedstaaten durchgesetzt werden.
-



Data Act (DA)

- **Wer ist betroffen:** Die Hersteller, Eigentümer, Besitzer und Verwender von IoT-Geräten. Hierneben Dritte, die Daten aus IoT-Geräten nutzen wollen.
 - **Im Detail:** Der DA regelt Pflichten von Herstellern und Entwicklern von Produkten zur erleichterten Erreichbarkeit der bei der Verwendung der Produkte erzeugten Daten für den Nutzer (oder einen von ihm benannten Dritten). Damit einher gehen gewisse Transparenzpflichten. Zudem enthält der DA allgemeine Vorschriften für (faire und nicht-diskriminierende) Datenbereitstellungspflichten, spezifische Kontrollen von Vertragsklauseln und den (zwangsweise) Zugang öffentlicher Stellen auf Daten im „Besitz“ von Unternehmen in Ausnahmefällen. Letztlich finden sich im DA noch Regelungen zu IT-sicherheitsrechtlichen Anforderungen an Anbieter von Datenverarbeitungsdiensten und zu Anforderungen an die Interoperabilität von Daten.
-



eIDAS 2.0 & European Digital Identity Regulation

- **Worum geht es:** EU-Kommission möchte einen einheitlichen Identitätsnachweis
 - **Stand der Dinge:** Am 09.02.2023 hat der federführende Ausschuss seinen Bericht für die eIDAS 2.0 angenommen, der im März 2023 als Beschlussvorlage für die allgemeine Ausrichtung des EU-Parlaments im Plenum vorgelegt wurde, so dass die Trilogverhandlungen ab dem 2. Quartal 2023 beginnen werden. Voraussichtlich müssen die EU-Mitgliedstaaten ihren Bürgern ab frühestens Mitte 2025 eine digitale ID-Wallet anbieten, weil der Kompromisstext des EU-Parlaments eine Umsetzungsfrist von 18 Monaten vorsieht, der Rat aber eine Umsetzungsfrist von 30 Monaten. Bis zum Jahr 2030 soll mindestens 80 % der EU-Bevölkerung im Besitz eines digitalen Identifizierungssystems sein, mit dem sie aus der Ferne sicher mit Behörden und Unternehmen in der gesamten EU interagieren können.
-



eIDAS 2.0 & European Digital Identity Regulation

- **Wer ist betroffen:** Digitale Identitäten für Konzerne und Behörden. Mit der Reform will die EU den nationalen Flickenteppich digitaler IDs auflösen und einer europaweiten digitalen Identität zum Durchbruch verhelfen. Bislang haben nur 19 der insgesamt 27 EU-Staaten Systeme auf Basis von eIDAS eingeführt, die jedoch zueinander meist inkompatibel sind. So gibt es hierzulande etwa den digitalen Personalausweis, der aber nur innerhalb Deutschlands funktioniert. Die größte Änderung gegenüber der schon bestehenden eIDAS-Verordnung besteht darin, dass eIDAS 2.0 die Wallet-App auch für private Unternehmen öffnen soll. Sie könnten damit etwa die Identität der Nutzenden überprüfen. Sowohl Plattformen wie Facebook, Amazon und Google als auch Behörden und Banken sollen dazu verpflichtet werden, die europäische ID-Wallet zu unterstützen.
 - **Massive Bedenken** bestehen jedoch noch immer aus der Datenschutzsicht.
-

Verordnung über den europäischen Raum für Gesundheitsdaten (EHDS)



- **Worum geht es:** Die Schaffung eines europäischen Datenraums im Gesundheitssektor für einen effizienten Austausch und direkten Zugriff auf unterschiedliche Gesundheitsdaten in der Gesundheitsversorgung selbst (Primärnutzung), sowie in der Gesundheitsforschung und der Gesundheitspolitik (Sekundärnutzung).
 - **Stand der Dinge:** Die Kommission hat ihr Vorhaben am 03.05.2022 vorgestellt. Die öffentliche Konsultation dauerte bis zum 20. Juli 2022. Mit Inkrafttreten der Verordnung im Jahr 2024 oder 2025 wird der europäische Gesundheitsdatenraum unmittelbar geltendes Recht.
 - **Wer ist betroffen:** Grundsätzlich alle Patienten, Gesundheitsdienstleister, **Forschende**, Hersteller von gesundheitsbezogenen Produkten und andere Personen, die Interesse an der Nutzung von Gesundheitsdaten haben.
-



Data Governance Act (DGA)

- **Worum geht es:** Förderung der Verfügbarkeit von Daten
 - **Stand der Dinge:** Am 30. Mai 2022 verabschiedet, Geltung ab dem 24. September 2023
 - **Wer ist betroffen:** Insbesondere öffentliche Stellen, die im „Besitz“ von Daten sind, Datenvermittlungsdienste und Organisationen, welche bestimmte Ziele von allgemeinem Interesse mithilfe von „Datenaltruismus“ fördern wollen.
 - **Übersicht:** Der DGA stützt sich auf vier Säulen, um die Verfügbarkeit von Daten zu fördern: Die Weiterverwendung von geschützten Daten im „Besitz“ öffentlicher Stellen, Datenvermittlungsdienste, Datenaltruismus, die Erschaffung eines Europäischen Dateninnovationsrates. Es werden insbesondere Bedingungen für die Weiterverwendung bestimmter Daten aufgestellt; es wird ein Anmelde- und Aufsichtsrahmen für Datenvermittler statuiert und die Möglichkeit geschaffen, Privilegierungen als „anerkannte datenaltruistische Organisation“ zu erhalten.
-



Data Governance Act (DGA)

- **Im Detail:** Eine wichtige Säule der europäischen Datenstrategie bildet der Data Governance Act („DGA“). Er zielt darauf ab, die Verfügbarkeit von Daten zur wirtschaftlichen Nutzung, gemeinsamen Verwendung und nicht zuletzt für Forschungszwecke zu erhöhen, um dem europäischen Markt so einen Wettbewerbsvorteil bei datengestützten Innovationen zu verschaffen.
 - Der DGA behandelt im Schwerpunkt folgende drei zentrale Themenfelder:
 - Bereitstellung von Daten der öffentlichen Hand
 - das Konzept der Datenvermittlungsdienste
 - und den sog. „Datenaltruismus“
-



Data Governance Act (DGA)

- **Bereitstellung von Daten der öffentlichen Hand:** Im DGA werden die Voraussetzungen für die Weiterverwendung solcher Daten festgelegt, die sich im Besitz öffentlicher Stellen (z.B. auch Hochschulen) befinden und aus bestimmten Gründen geschützt sind. Hintergrund der Regelung ist die Vorstellung, dass Daten, die mithilfe öffentlicher Gelder generiert oder gesammelt wurden, auch der Gesellschaft zugutekommen sollen (ErwGr 5). Auch um die Wettbewerbsfähigkeit der europäischen Datenwirtschaft zu fördern und gleichzeitig die Rechte Dritter zu schützen, regelt der DGA Rahmenbedingungen für die (sicherere) Weitergabe geschützter Daten öffentlicher Stellen. Allerdings soll ausdrücklich kein europarechtlicher Rechtsanspruch auf Zugang zu den entsprechenden Daten geschaffen werden, Art. 1 Abs. 2 DGA. Dies obliegt weiter den Mitgliedstaaten.
-



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

- **Worum geht es:** Die Open-Data-Richtlinie verpflichtet EU-Mitgliedstaaten dazu, Dokumente der öffentlichen Hand zur Weiterverwendung freizugeben
 - Bundesrepublik Deutschland: Zweites Open-Data-Gesetz und **Datennutzungsgesetz:** Wesentliches Ziel ist es dabei, die Bereitstellung **offener Verwaltungsdaten der Bundesverwaltung** umfänglich auszuweiten und die **Nutzungsmöglichkeiten bereitgestellter öffentlich finanzierter Daten** zu vereinfachen und zu verbessern.
 - Durch den geänderten § 12a E-Government-Gesetz (EGovG) sollen erstmals die mittelbare Bundesverwaltung und **Forschungsdaten** der Bereitstellungspflicht unterliegen. Gleichzeitig sollen durch die Schaffung verbindlicher Open-Data-Koordinatoren der Bundesbehörden und eine Verordnungsermächtigung die Bereitstellungsprozesse und Datenformate verbessert und standardisiert werden.
-



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

- Mit dem neuen **Datennutzungsgesetz (DNG)** soll das Informationsweiterverwendungsgesetz (IWG) modernisiert und abgelöst werden. Zur Verbesserung der Nutzbarkeit von Daten müssen offene Daten künftig in maschinenlesbaren Formaten nutzbar gemacht werden. Darüber hinaus setzt das DNG Impulse für Open-Data-Initiativen über die Grenzen der Bundesverwaltung hinaus und etabliert analog zum ersten Open-Data-Gesetz des Bundes das Prinzip „Open by default“ auch für die **Datennutzung der Länder**, Kommunen und öffentlicher Unternehmen in den Bereichen der Wasser-, Verkehrs- und Energieversorgung. Das DNG erweitert den Anwendungsbereich auf öffentliche Unternehmen bestimmter Bereiche der Daseinsvorsorge, schärft die Grenzen der Entgeltbemessung und bestimmt die Echtzeit-Bereitstellung dynamischer Daten sowie hochwertiger Datensätze.
 - Mit dem Gesetz wurde die im Jahr 2019 neugefassten EU-Richtlinie 2019/1024 (Open-Data- und Public Sector Information-Directive) umgesetzt.
-



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

§ 1 DNG Grundsatz der offenen Daten

- (1) Daten, die in den Anwendungsbereich dieses Gesetzes fallen, sollen, soweit möglich, nach dem **Grundsatz „konzeptionell und standardmäßig offen“** erstellt werden.
 - (2) Eine Bereitstellungspflicht oder ein Anspruch auf Zugang zu Daten wird mit diesem Gesetz nicht begründet.
-



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

§ 2 DNG Anwendungsbereich

(1) Dieses Gesetz gilt für Daten von Datenbereitstellern nach Absatz 2, die

1. aufgrund eines gesetzlichen Anspruchs auf Zugang bereitgestellt werden,
2. aufgrund einer gesetzlichen Bereitstellungspflicht bereitgestellt werden oder
3. auf sonstige Weise öffentlich oder zur ausschließlichen Nutzung bereitgestellt werden.

(2) Datenbereitsteller im Sinne dieses Gesetzes sind:

1. **öffentliche Stellen;**

2. Unternehmen der Daseinsvorsorge, die den Vorschriften über die Vergabe von öffentlichen Aufträgen und Konzessionen unterfallen oder öffentliche Personenverkehrsdienste betreiben;



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

3. in **Bezug auf Forschungsdaten, die öffentlich finanziert und bereits über ein institutionelles oder thematisches Repository öffentlich bereitgestellt wurden:**

a) **Hochschulen, Forschungseinrichtungen und Forschungsfördereinrichtungen,**

b) **Forschende, wenn die Forschungsdaten nicht bereits durch andere durch dieses Gesetz verpflichtete Datenbereitsteller bereitgestellt wurden;**

dies gilt nicht, soweit berechnigte Geschäftsinteressen, Wissenstransfertätigkeiten oder bestehende Rechte Dritter an geistigem Eigentum entgegenstehen.

(3) Dieses Gesetz gilt **nicht** für

1. Daten,

a) die nicht oder nur eingeschränkt zugänglich sind, wobei eine Einschränkung auch vorliegt, wenn der Zugang nur bei Nachweis eines rechtlichen oder berechtigten Interesses besteht; nicht oder nur eingeschränkt zugänglich sind Daten insbesondere,



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

- aa) soweit der Schutz personenbezogener Daten entgegensteht,
- bb) soweit der Schutz von Geschäftsgeheimnissen entgegensteht,
- cc) soweit der Schutz der nationalen Sicherheit, der Verteidigung oder der öffentlichen Sicherheit entgegensteht,
- dd) soweit die Eigenschaft als vertrauliche Informationen über den Schutz kritischer Infrastrukturen entgegensteht oder
- ee) soweit die statistische Geheimhaltung entgegensteht,
- b) die geistiges Eigentum Dritter betreffen,
- c) die nach den Vorschriften des Bundes oder der Länder über den Zugang der Öffentlichkeit zu Umweltinformationen zugänglich sind und uneingeschränkt, kostenlos, maschinenlesbar und über eine Anwendungsprogrammierschnittstelle nutzbar sind oder
- d) deren Bereitstellung nicht unter den durch Rechtsvorschrift festgelegten öffentlichen Auftrag der öffentlichen Stelle fällt;



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

§ 3 DNG Begriffsbestimmungen

Im Sinne dieses Gesetzes

10. sind **Forschungsdaten Aufzeichnungen in digitaler Form, bei denen es sich nicht um wissenschaftliche Veröffentlichungen handelt und die im Laufe von wissenschaftlichen Forschungstätigkeiten erfasst oder erzeugt und als Nachweise im Rahmen des Forschungsprozesses verwendet werden oder die in der Forschungsgemeinschaft allgemein für die Validierung von Forschungsfeststellungen und -ergebnissen als notwendig erachtet werden,**

12. ist Anonymisierung der Prozess, in dessen Verlauf personenbezogene Daten in Daten umgewandelt werden, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder derart in Daten umgewandelt werden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

§ 4 DNG Grundsatz der uneingeschränkten Datennutzung; Zulässigkeit von Lizenzen

- (1) Daten dürfen für **jeden kommerziellen oder nichtkommerziellen Zweck** genutzt werden.
 - (2) Für Daten, an denen Bibliotheken, einschließlich **Hochschulbibliotheken**, Museen und Archive, Urheber- oder verwandte Schutzrechte oder gewerbliche Schutzrechte zustehen, und für Daten von Unternehmen der Daseinsvorsorge **gilt Absatz 1 nur, soweit die Einrichtung** oder das Unternehmen der Daseinsvorsorge **die Nutzung zugelassen hat**.
 - (3) **Nutzungsbedingungen (Lizenzen) sind zulässig**, soweit sie objektiv, verhältnismäßig, nichtdiskriminierend und durch ein im Allgemeininteresse liegendes Ziel gerechtfertigt sind. Die Lizenz darf nicht zu einer Wettbewerbsverzerrung führen und die Möglichkeiten der Nutzung nicht unnötig einschränken. Öffentliche Stellen sollen nach Möglichkeit offene Lizenzen verwenden.
-



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

§ 7 DNG Verfügbare Formate, Metadaten

(1) Der Datenbereitsteller muss die **Nutzung der Daten in allen angefragten und bei ihm vorhandenen Formaten und Sprachen** ermöglichen.

(2) Soweit möglich und sinnvoll, sind Daten **elektronisch und in nach den anerkannten Regeln der Technik offenen, maschinenlesbaren, zugänglichen, auffindbaren und interoperablen Formaten zusammen mit den zugehörigen Metadaten** bereitzustellen. Sowohl die Formate als auch die Metadaten entsprechen, soweit möglich, **förmlichen offenen Standards**.



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

§ 7 DNG Verfügbare Formate, Metadaten

(3) Die Absätze 1 und 2 verpflichten **öffentliche Stellen** und öffentliche Unternehmen nicht, Daten und Metadaten neu zu erstellen oder anzupassen oder Teile von Datensätzen zur Verfügung zu stellen, wenn dies mit unverhältnismäßigem Aufwand verbunden wäre, der über eine einfache Bearbeitung hinausgeht. **Öffentliche Stellen** und Unternehmen der Daseinsvorsorge sind außerdem nicht verpflichtet, die Erstellung und Speicherung bestimmter Arten von Daten im Hinblick auf deren Nutzung durch eine Organisation des privaten oder öffentlichen Sektors fortzusetzen.

(4) Die Metadaten zu maschinenlesbaren Daten sind, soweit möglich und sinnvoll, über das **nationale Metadatenportal GovData** zur Verfügung zu stellen.



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

§ 9 DNG Hochwertige Datensätze

Öffentliche Stellen und Unternehmen der Daseinsvorsorge müssen die Nutzung hochwertiger Datensätze in maschinenlesbarem Format über geeignete Anwendungsprogrammierschnittstellen und, falls technisch erforderlich, als Massen-Download ermöglichen.



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

§ 10 DNG Grundsatz der Unentgeltlichkeit

(1) Die **Nutzung von Daten ist unentgeltlich**. Es ist jedoch zulässig, die Erstattung von verursachten Grenzkosten für die folgenden Tätigkeiten und Maßnahmen zu verlangen:

1. die Reproduktion, Bereitstellung und Verbreitung von Daten,
2. die Anonymisierung personenbezogener Daten und
3. Maßnahmen zum Schutz vertraulicher Geschäftsinformation.

(2) Abweichend von Absatz 1 Satz 1 dürfen für die Nutzung von Daten **Entgelte verlangen**:

1. **öffentliche Stellen, die ausreichende Einnahmen erzielen müssen**, um einen wesentlichen Teil ihrer Kosten im Zusammenhang mit der Erfüllung ihrer öffentlichen Aufträge zu decken;
 2. Bibliotheken, einschließlich **Hochschulbibliotheken**, Museen und Archive;
 - ~~3. Unternehmen der Daseinsvorsorge.~~
-



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

§ 10 DNG Grundsatz der Unentgeltlichkeit

(3) Absatz 1 Satz 2 und Absatz 2 Nummer 1 und 3 gelten nicht für hochwertige Datensätze sowie **Forschungsdaten**.

(4) Wenn **öffentliche Stellen**, die ausreichende Einnahmen erzielen müssen, um einen wesentlichen Teil ihrer Kosten im Zusammenhang mit der Erfüllung ihres öffentlichen Auftrags zu decken, von der Anwendung des Absatzes 1 Satz 1 ausgenommen werden wollen, melden sie die Berufung auf die Ausnahme der Bundesnetzagentur. Die Bundesnetzagentur führt eine Liste der öffentlichen Stellen, die von der Ausnahme Gebrauch machen, und macht die Liste auf ihrer Internetseite zugänglich.

(5) Für **öffentliche Stellen**, die Einnahmen erzielen müssen, um einen wesentlichen Teil ihrer Kosten bei der Erfüllung ihres öffentlichen Auftrags zu decken, und bei denen sich die unentgeltliche Nutzung hochwertiger Datensätze wesentlich auf ihren Haushalt auswirkt, gilt die Unentgeltlichkeit der Nutzung hochwertiger Datensätze spätestens zwölf Monate ~~nach dem 23. Juli 2021.~~



Open-Data-Richtlinie & Datennutzungsgesetz (DNG)

§ 12 DNG Transparenz von Entgelten

(1) Wurden für die Nutzung von Daten Entgelte festgelegt, die für die Allgemeinheit gelten (**Standardentgelte**), sind die Bedingungen und die tatsächliche Höhe der Standardentgelte einschließlich ihrer Berechnungsgrundlage im Internet öffentlich zugänglich zu machen.

(2) Wurden für die Nutzung keine Standardentgelte festgelegt, sind die **Faktoren, die bei der Berechnung der Entgelte berücksichtigt werden**, anzugeben. Auf Anfrage wird auch die Berechnungsweise dieser Entgelte in Bezug auf einen spezifischen Antrag auf Nutzung angegeben.

§ 13 DNG Rechtsweg

Für Streitigkeiten nach diesem Gesetz ist der **Verwaltungsrechtsweg** gegeben.

Verordnung zur Festlegung harmonisierter Vorschriften über künstliche Intelligenz (AI-Act)



- **Nun endlich zum AI-Act = KI-Verordnung & KI-Richtlinie (Entwürfe)!**



Verordnung zur Festlegung harmonisierter Vorschriften über künstliche Intelligenz (AI-Act)



- **Worum geht es:** Die KI-Verordnung (noch nicht in Kraft!) soll den regulatorischen Rahmen (**Verantwortung**) für den Einsatz von KI setzen und steht im Zusammenspiel mit der Richtlinie über KI-Haftung. Diese Richtlinie (noch nicht in Kraft!) soll einen harmonisierten Rechtsrahmen auf Unionsebene schaffen und die durch den technischen Fortschritt bei Systemen mit künstlicher Intelligenz verursachten **Haftungslücken** füllen.
 - **Stand der Dinge:** Das EU-Parlament hat sich am 14.06.2023 auf eine Position zur Regulierung von Künstlicher Intelligenz geeinigt. Es verbietet Anwendungen, die mit hohen Risiken für die Sicherheit verbunden sind - etwa Gesichtserkennung. Nachdem sich das Parlament auf eine Position geeinigt hat, können nun die Verhandlungen mit den EU-Mitgliedsstaaten und der Kommission über den endgültigen Wortlaut des Gesetzes beginnen. Sollte dabei eine Einigung vor der Europawahl im kommenden Jahr gelingen, könnte die KI-Verordnung aber voraussichtlich erst im Jahr 2026 anwendbar sein, denn das Gesetz sieht Übergangsfristen von bis zu zwei Jahren vor.
-

Verordnung zur Festlegung harmonisierter Vorschriften über künstliche Intelligenz (AI-Act)



- **Wer ist betroffen:** Auch **Hochschulen** können betroffen sein, **dazu gleich mehr!**
 - **Vorab folgender Hinweis:** Schwerpunkt der Regulierung (und dieses Workshops) durch den sog. AI-Act ist die sog. „Hochrisiko-KI“, **nicht** jede KI, z.B. mit geringem bzw. minimalem Risiko (dann bestehen nur geringfügige Transparenzpflichten), und **verbotene KI-Praktiken sind verboten!**
-



Hinweis auf Workshop-Dokumentation

Der **Online-Workshop "KI-Generatoren in der Hochschul(lehr)e – Potenziale und rechtliche Implikationen von ChatGPT, DALL-E & Co."** fand am 14. März 2023 statt:

- Potenziale und Anwendungsmöglichkeiten von KI-Generatoren in Hochschul(lehre) (Prof. Dr. Christian Spannagel, PH Heidelberg)
- Haftungs- und urheberrechtliche Herausforderungen bei der Verwendung von KI-Generatoren
 - Verantwortlichkeit der Anbietenden von KI-Generatoren (Jens O. Brelle, MMKH)
 - Urheberrecht: Input & Trainingsdaten (Jens O. Brelle, MMKH)
 - Weiterverwendung des Outputs (Dr. Janine Horn, ELAN e.V.)
- Herausforderungen für das Prüfungsrecht an Hochschulen (Prof. Dr. Dirk Heckmann, TUM)

<https://www.mmkh.de/digitale-lehre/netzwerk-landesinitiativen/ki-generatoren-in-der-hochschullehre.html>

KI-GENERATOREN IN DER HOCHSCHUL[LEHR]E

Potenziale und rechtliche Implikationen
von ChatGPT, DALL-E & Co.

ONLINE-VERANSTALTUNG

14. März 2023, 10:00 – 12:30 via Zoom

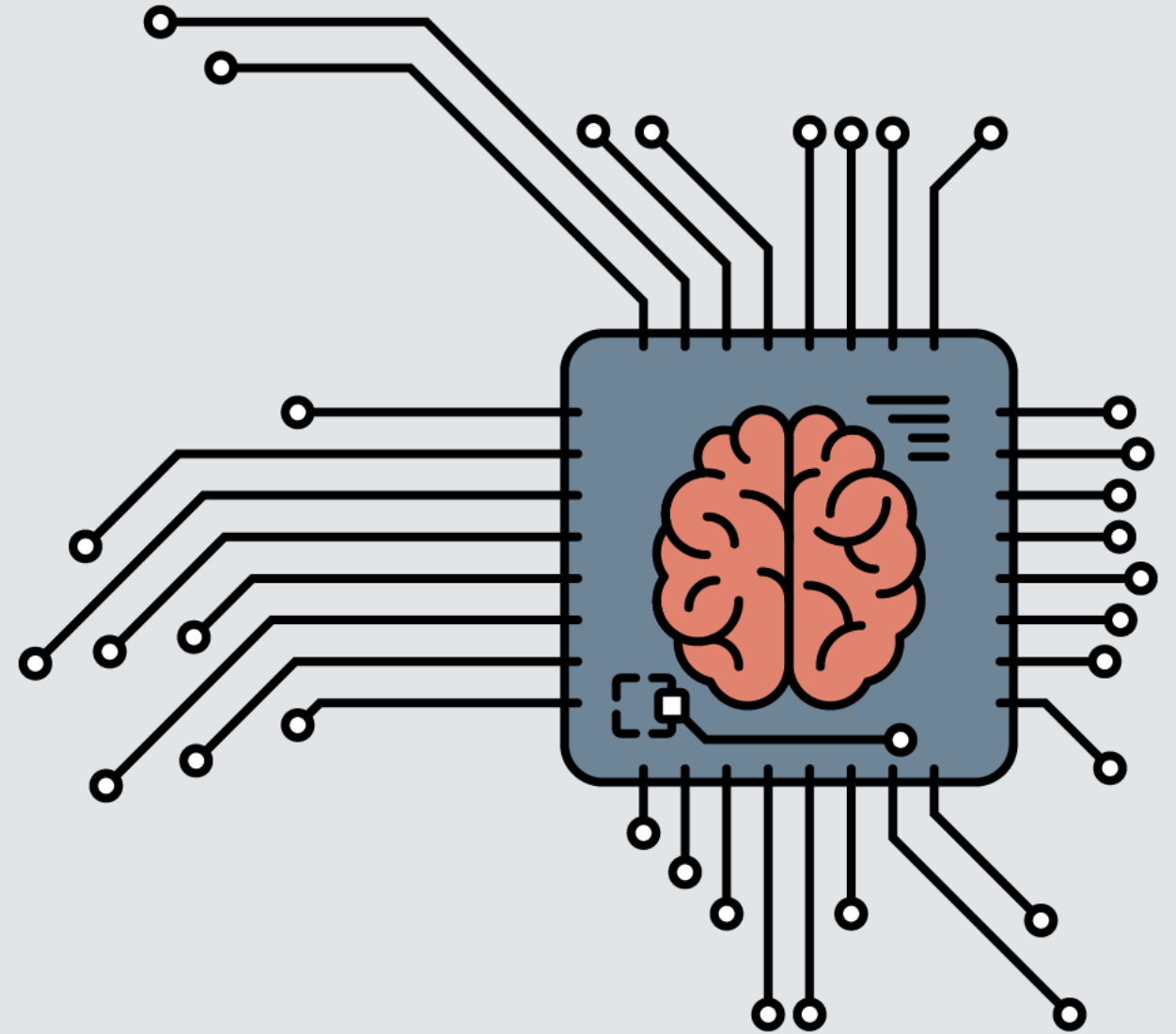
VORTRAGENDE

Prof. Dr. Christian Spannagel, PH Heidelberg

Prof. Dr. Dirk Heckmann, TUM

Jens O. Brelle, MMKH

Dr. Janine Horn, ELAN e.V.



MMKH.DE



Das Ende von ChatGPT und das Ende dieses Workshops?

GRÜNDERSZENE MAGAZIN PLUS PODCAST JOBBÖRSE EVENTS MEHR Abonnement

HOME > GRÜNDERSZENE > BUSINESS > CHATGPT: DROHT IN EUROPA BALD DAS AUS?

65+ NEUE GESETZE

Droht ChatGPT in Europa bald das Aus?

Stefan Beutelsbacher und Benedikt Fuest (Die Welt)
07 Mrz 2023

[f](#) [t](#) [in](#) [w](#) [m](#) [v](#) [s](#)

ChatGPT bringt in der EU einiges durcheinander. Auf Hauruk müssen neue Gesetze geschrieben werden - und wie es aussieht, könnte der Super-Bot sogar verboten werden.



home24
WOW²
15 %
RABATT AUF
TOPSELLER*
Jede Woche
neue
Produkte
Bis zum 14. März
9 Uhr
Jetzt sparen
*Mehr Infos auf home24.de

Generative AI

Zum Beenden des Vollbildmodus Esc drücken

Generative AI Hintergrund Ratgeber Bilder Video News

ChatGPT hat weniger Besucher

OpenAI verzeichnet rückläufigen Web-Traffic

10.07.2023

Von  [Martin Bayer \(Stellv. Chefredakteur\)](#) [FOLGEN](#)

ChatGPT katapultierte die Website von OpenAI innerhalb weniger Monate auf über 1,5 Milliarden Visits pro Monat. Doch nach dem Boom scheint das Interesse nun etwas zu erlahmen.

-  Empfehlen
-  Drucken
-  PDF
-  URL
-  Xing
-  LinkedIn
-  Twitter
-  Facebook
-  Feedback



Nachdem viele Millionen Menschen rund um den Globus ChatGPT ausprobiert



aruba
a Hewlett Packard
Enterprise company

63 % der Unternehmen
fehlt Transparenz und die
Kontrolle darüber, was in
ihrem Netzwerk vorgeht

BERICHT HERUNTERLADEN →

MEHR ZUM THEMA

-  KI-Technik für Azure und Office: Microsoft investiert Milliarden in OpenAI

AKTUELLE JOBANGEBOTE

SAP Inhouse Consultant (m/w/d) MD/MDG für die Abteilung Informationstechnologie
ifm-Unternehmensgruppe

Für eine Welt,
in der
Innovationen
reibungslos
verlaufen.

Workday.
For a changing world.™

Mehr Erfahren



workday





BRANDBRIEF

Aufschrei der Wirtschaft – Die Angst vor dem KI-Gesetz

Brüssel steht kurz vor der Verabschiedung eines KI-Gesetzes. Führende Wirtschaftsvertreter sehen darin eine Gefahr – und drängen darauf, zwei Punkte zu ändern.



Christoph Herwartz



Larissa Holzki



Christof Kerkmann

29.06.2023 - 19:20 Uhr • [Jetzt teilen](#)





MEDIZIN

Wie KI die Biotech-Branche revolutioniert

Aufbruchstimmung in der Biotech-Forschung. Mit KI wollen Wissenschaftler Krankheiten wie Krebs besiegen. Doch mit der neuen Technik steigen auch die Gefahren wie durch künstliche Erreger.



Felix Holtermann

19.06.2023 - 08:18 Uhr • [4 x geteilt](#)





Worum geht es? Zum Beispiel: netartgenerator.de

Gibt es bereits seit Anfang der 2000´er & verwende ich in meinem urheberrechtlichen Vorlesungen:

.:: NAG :: Net.Art Generator

<https://nag.iap.de>

NET.ART GENERATOR

SMART
ARTIST
MAKES
THE
MACHINE
DO
THE
WORK

create



anonymous_warhol-flowers, solo exhibition This is not by me, Kunstverein
Hildesheim, 2006 1 / 35

nag_home
about
exhibitions
projects
nag@zkm
net.art generators
publications
contact




Welcome to NAG

The net.art generator automatically produces net.art on demand.

nag_05-this version of the net.art generator creates images. The resulting image emerges as a collage of a number of images which have been collected on the WWW in relation to the 'title' you have chosen. The original material is processed in 12-14 randomly chosen and combined steps. For finding the images, nag_05 draws on Google search; that is the delicate part as Google limits access to their search results for all non-paying clients including net.art projects like this one.

The technical base of the net.art generator is a PERL script, old but reliable technology. The original version was programmed by Panos Galanis from IAP GmbH, Hamburg, in 2003 after an idea by net.artist Cornelia Sollfrank. With Winnie Soon, the net.art generator has found a skillful new master of creative coding in 2017.

We need your feedback to develop the project further! Please tell us about your experiences related to the nag. We would like to know what is happening on the other end! Also, if you are facing problems regarding the functionality, please contact [nag\[at\]artwarez.org](mailto:nag[at]artwarez.org).

If you would like to support the ongoing development and search requests of _nag, you can  [Flattr this us!](#)

Have fun and become a net.artist!

For more information, please visit net.art-generator.com, the home of all net.art.generators!

Many thanks to the generous support by IAP GmbH, in particular Gerrit Ché Boelz for his enthusiasm and dedication.

Screenshot



Info

The generation of your piece of net.art takes 1-2 minutes. Please have a little patience. If nothing has happenend after 2 minutes, please click the 'stop'-button and try again.

Query

Artist	Title	Compose
<input type="text" value="anonymous"/>	<input type="text" value="Multimedia Kontor Hamburg"/>	<input type="text" value="4 Images"/>
Max Width	Extension	<input type="button" value="Create"/>
<input type="text" value="600 px"/>	<input type="text" value="JPEG :: Jpeg Image"/>	

Searching the Net for *Multimedia Kontor Hamburg* :: Powered by [Google](#)

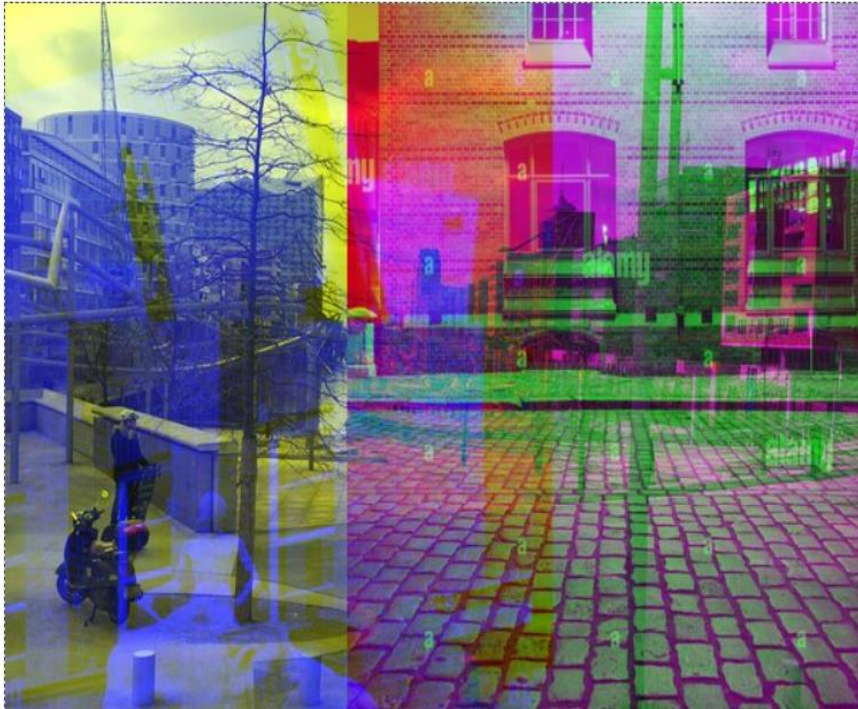
Choosing : 4 / 10

- <https://dynamic-media-cdn.tripadvisor.com/media/photo-o/0a/93/41/70/photo6jpg.jpg?w=1200&h=900&s=1> :: [view](#)
- <https://c8.alamy.com/comp/G56BEP/hamburg-germany-20th-june-2016-a-woman-holds-up-a-ticket-for-the-elbe-G56BEP.jpg> :: [view](#)
- <https://c8.alamy.com/comp/H4942C/kontor-house-architecture-alter-wandrahm-speicherstadt-city-of-warehouses-H4942C.jpg> :: [view](#)
- <https://c8.alamy.com/comp/EGK23Y/faade-detail-of-brahms-kontor-historic-office-and-commercial-building-EGK23Y.jpg> :: [view](#)

Generator Usage

Composition 4 :: New 4 :: Cached 0

Show



Info

The generation of your piece of net.art takes 1-2 minutes. Please have a little patience. If nothing has happenend after 2 minutes, please click the 'stop'-button and try again.

Query

Artist	Title	Compose
<input type="text" value="anonymous"/>	<input type="text" value="Multimedia Kontor Hamburg"/>	<input type="text" value="8 Images"/> ▼
Max Width	Extension	<input type="button" value="Create"/>
<input type="text" value="600 px"/> ▼	<input type="text" value="JPEG :: Jpeg Image"/> ▼	

Searching the Net for *Multimedia Kontor Hamburg* :: Powered by [Google](#)

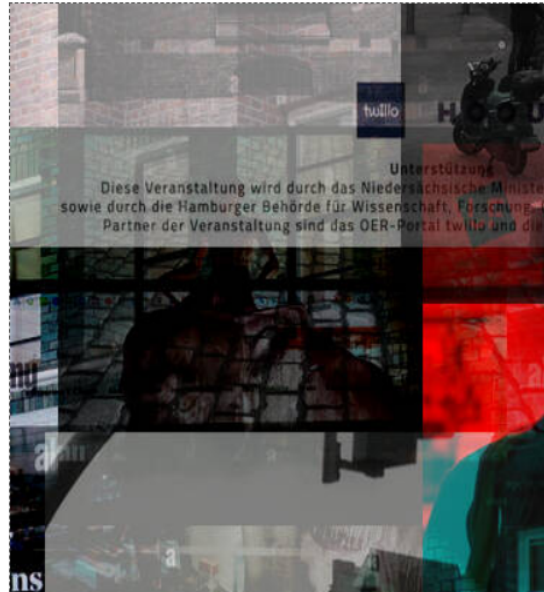
Choosing : 8 / 10

- <https://c8.alamy.com/comp/EGK23Y/faade-detail-of-brahms-kontor-historic-office-and-commercial-building-EGK23Y.jpg> :: [view](#)
- <https://pbs.twimg.com/media/FmlK9nOX0AEfd4X.jpg> :: [view](#)
- <https://c8.alamy.com/comp/2FWR1G3/new-york-usa-1-may-2021-hamburg-commercial-bank-hcob-company-website-on-screen-illustrative-editorial-2FWR1G3.jpg> :: [view](#)
- <https://c8.alamy.com/comp/H4942C/kontor-house-architecture-alter-wandrahm-speicherstadt-city-of-warehouses-H4942C.jpg> :: [view](#)
- <https://dynamic-media-cdn.tripadvisor.com/media/photo-o/0f/25/a6/00/ingang-zur-speicherstadt.jpg?w=1200&h=900&s=1> :: [view](#)
- <https://pbs.twimg.com/media/Fo6qQ1jXoAAeHsj.jpg> :: [view](#)
- https://pbs.twimg.com/ext_tw_video_thumb/1433315839080534017/pu/img/sA423WBMpPf_thWW.jpg :: [view](#)
- <https://dynamic-media-cdn.tripadvisor.com/media/photo-o/0a/93/41/70/photo6jpg.jpg?w=1200&h=900&s=1> :: [view](#)

Generator Usage

Composition 8 :: New 8 :: Cached 0

Show





Rechtliche Herausforderungen bei der Verwendung von KI-Generatoren

Verantwortlichkeit & Haftung der Anbietenden von KI-Generatoren

- Entwürfe Europäische KI-Verordnung & KI-Haftungsrichtlinie: Verantwortung & Haftung
 - Datenschutz & Persönlichkeitsrechte
 - Urheberrechtliche Bezüge
-



Verantwortlichkeit von Anbietenden von KI-Generatoren

Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Die KI-Verordnung (noch nicht in Kraft!) soll den regulatorischen Rahmen (**Verantwortung!**) für den Einsatz von KI setzen und steht im Zusammenspiel mit der Richtlinie über KI-Haftung.



Haftung von Anbietenden von KI-Generatoren

Entwurf Richtlinie über KI-Haftung = Richtlinie zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstlicher Intelligenz

Diese Richtlinie (noch nicht in Kraft!) soll einen harmonisierten Rechtsrahmen auf Unionsebene schaffen und die durch den technischen Fortschritt bei Systemen mit künstlicher Intelligenz verursachten **Haftungslücken** füllen.

Die Einführung, Verbreitung und Weiterentwicklung von KI-Systemen soll in der Europäischen Union gefördert werden, indem rechtliche Fragmentierung vermieden wird, da bei unionsweit einheitlichen Haftungsvorschriften Unternehmen ihr Haftungsrisiko besser bewerten und versichern können.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Inkrafttreten der KI-Verordnung

Die KI-Verordnung ist noch im Entwurfsstadium der EU-Gesetzgebungsorgane im sog. „Trilog“ vor: Entwurfstext im EU-Parlament und im EU-Ministerrat in der Diskussion. Der Ministerrat stellte unter zuletzt im Oktober 2022 einen vollständigen Kompromissvorschlag vor. Im Parlament haben am ersten Juni 2022 die Verhandlungen begonnen und Kompromisse werden entworfen; verschiedene Ausschüsse arbeiten derzeit noch an ihren Empfehlungen. Die Abstimmung im Plenum war für Oktober 2022 angesetzt, wurde jedoch zunächst auf November 2022 verschoben und war nunmehr für das erste Quartal 2023 geplant und fand in den Sitzungstagen Mitte März 2023 statt, **am 14.06.2023 stimmte das EU-Parlament dem Entwurf zu**, so dass die Verhandlungen mit den EU-Mitgliedsstaaten und der Kommission über den endgültigen Wortlaut des Gesetzes begonnen haben.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Inkrafttreten der KI-Verordnung

Wann die Verordnung tatsächlich in Kraft treten wird, ist momentan nicht sicher abzusehen. Ein Inkrafttreten erschien zunächst schon 2023 denkbar, wahrscheinlich wird dies nunmehr jedoch **ab 2024** geschehen. Danach wird es für Unternehmen eine **zwei- bis dreijährige Umsetzungsfrist bis zur tatsächlichen Anwendbarkeit der KI-Verordnung** geben. Die Mitgliedstaaten haben binnen eines Jahres nationale notifizierende Behörden einzurichten, die für die Durchführung von Konformitätsverfahren zuständig sind.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Sachlicher Anwendungsbereich

Der KI-VO-E definiert den Begriff „System der künstlichen Intelligenz“ in Art. 3 Abs. 1 wie folgt: „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.**“



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Sachlicher Anwendungsbereich: Aber Achtung!

Die Definition ist noch immer nicht final und noch immer umstritten (Stand: 14.06.2023). Sie wurde in dieser Form erst im letzten Kompromissvorschlag vom EU-Ministerrat in den Verordnungstext aufgenommen. In dem ursprünglich vorgelegten Entwurf war die Definition für KI-Systeme noch wesentlich weiter angelegt.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Sachlicher Anwendungsbereich: Aber Achtung!

Eine alte Definition lautete z.B.: „Ein System, das so konzipiert ist, dass es mit einem bestimmten **Grad an Autonomie** arbeitet, und das auf der **Grundlage von maschinellen und/oder menschlichen Daten** und **Eingaben mithilfe von maschinellem Lernen** und/oder **logik- und wissensbasierten Ansätzen** ableitet, wie eine bestimmte Reihe von vom **Menschen definierten Ziele erreicht** werden kann, und das **systemgenerierte Ergebnisse wie Inhalte** (generative KI-Systeme), Vorhersagen, Empfehlungen oder Entscheidungen **erzeugt, die die Umgebung beeinflussen**, mit der das KI-System interagiert.“



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Persönlicher Anwendungsbereich

Der persönliche Geltungsbereich der geplanten Verordnung ist sehr weit.

Auch **Hochschulen** können betroffen sein.

Die Verordnung richtet sich an nahezu alle Akteure in der KI-Wertschöpfungskette. Insbesondere wird sie gem. Art. 2 KI-VO-E „Anbieter“ und „Nutzer“ von KI-Systemen adressieren. Beide Begriffe werden in Art. 3 KI-VO-E legaldefiniert.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Persönlicher Anwendungsbereich

„Anbietender“ ist eine **natürliche oder juristische Person, Behörde, Einrichtung** oder sonstige Stelle, die ein **KI-System entwickelt oder entwickeln lässt**, um es unter ihrem eigenen Namen oder ihrer eigenen Marke – entgeltlich oder unentgeltlich – in **Verkehr zu bringen oder in Betrieb zu nehmen**.

„Nutzender“ ist eine **natürliche oder juristische Person, Behörde, Einrichtung** oder sonstige Stelle, die ein **KI-System in eigener Verantwortung verwendet**, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Persönlicher Anwendungsbereich

- „**Einführer**“ eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Marke einer außerhalb der Union ansässigen oder niedergelassenen natürlichen oder juristischen Person trägt, in der Union in Verkehr bringt oder in Betrieb nimmt;
 - „**Bevollmächtigter**“ eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems schriftlich dazu bevollmächtigt wurde, in seinem Namen die in dieser Verordnung **festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen**;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Räumlicher Anwendungsbereich

Auch in räumlicher Hinsicht geht die KI-VO weit. So sollen alle **Anbietenden** von KI verpflichtet werden, die **Systeme auf dem EU-Markt bereitzustellen**, unabhängig davon, ob sie in der EU niedergelassen sind oder in einem Drittland. Für **Nutzende von KI-Systemen** gilt die Verordnung dann, wenn **sie in der EU niedergelassen oder „physisch anwesend“ sind**. Zudem richtet sich die KI-VO an Anbietende und Nutzende von KI, die zwar außerhalb der EU niedergelassen sind oder sich dort befinden, deren **Systeme aber Ergebnisse hervorbringen, die in der Union verwendet werden**. Zum Beispiel sollen Entwickelnde von KI-Systemen mit Sitz in den USA unter die Verordnung fallen, wenn sie diese Systeme Unternehmen in der EU zur Verwendung bereitstellen. Die KI-VO folgt damit dem Marktortprinzip aus der DSGVO, so soll eine Umgehung von EU-Recht verhindert werden.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Begriffsbestimmungen

- „**Trainingsdaten**“ Daten, die zum Trainieren eines KI-Systems verwendet werden, wobei dessen lernbare Parameter und die Gewichte eines neuronalen Netzes angepasst werden;
 - „**Validierungsdaten**“ Daten, die zum Bewerten des trainierten KI-Systems und zum Abstimmen seiner nicht lernbaren Parameter und seines Lernprozesses verwendet werden, um unter anderem eine Überanpassung zu vermeiden; der Validierungsdatensatz kann ein separater Datensatz oder Teil des Trainingsdatensatzes mit fester oder variabler Aufteilung sein;
 - „**Testdaten**“ Daten, die für eine unabhängige Bewertung des trainierten und validierten KI-Systems verwendet werden, um die erwartete Leistung dieses Systems vor dessen Inverkehrbringen oder Inbetriebnahme zu bestätigen;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Begriffsbestimmungen

- „**Eingabedaten**“ die in ein KI-System eingespeisten oder von diesem direkt erfassten Daten, auf deren Grundlage das System ein Ergebnis (Ausgabe) hervorbringt;
 - „**biometrische Daten**“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Regelungssystematik der KI-VO - risikobasierter Ansatz

Die KI-VO verfolgt einen risikobasierten Ansatz. Das heißt, je höher die Risiken, die von einem KI-System für die Grundrechte von EU-Angehörigen oder andere sensible Rechtsgüter ausgehen, desto strenger die regulatorischen Anforderungen. Dort, wo keine Risiken gesehen werden, soll es im Gegenzug keine rechtlichen Belastungen geben. Die geplante Verordnung sieht **vier Risikoklassen** vor.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Vier Risikoklassen

- **Verbotene KI-Praktiken (Art. 5 KI-VO)** bei nicht hinnehmbaren Risiken für die Grundrechte und Werte der Union.
 - **Hochrisiko-KI (Art. 6ff. KI-VO):** Systeme, von denen eine besonders hohe Gefahr für die Gesundheit und Sicherheit oder die Grundrechte von EU-Angehörigen befürchtet wird, z.B. Bereich „Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit“ bzw. Bereich „Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen.“
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Vier Risikoklassen

- **Geringes Risiko:** KI-Systeme mit geringem Risiko sind solche, die für die Interaktion mit Menschen bestimmt sind und nicht unter die Gruppe der verbotenen KI oder der Hochrisiko-KI fallen. Von solchen Algorithmen sollen potenziell lediglich gewisse Manipulationsrisiken ausgehen. Darunter fallen beispielsweise Chatbots, die den Anschein menschlicher Kommunikation erwecken können. Daher müssen Unternehmen, die derartige Systeme entwickeln oder verwenden, vor allem gewisse Transparenzpflichten erfüllen.
 - **Minimales Risiko:** Umfasst sind Systeme, von denen keine expliziten Risiken ausgehen sollen. Für den Umgang mit diesen sieht der KI-VO-E dementsprechend auch keine besonderen Verpflichtungen vor. Die Kommission und die Mitgliedstaaten wollen jedoch gem. Art. 69 KI-VO-E fördern, dass Anbieter solcher KI-Systeme Verhaltenskodizes aufstellen.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Vier Risikoklassen ausreichend?

Aktuell (Stand: 14.06.2023) wird um die Ergänzung einer weiteren Gruppe, nämlich „Allgemeine KI-Systeme“ diskutiert...



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

(Schwierige) Begriffsbestimmung „Risiko“

Aus der Gesetzesbegründung (Punkt 3.1):

- Die Interessenträger forderten mehrheitlich eine enge, klare und genaue Begriffsbestimmung künstlicher Intelligenz. Neben einer Klärung des Begriffs der KI unterstrichen sie auch die Notwendigkeit, die Begriffe „Risiko“, „hohes Risiko“, „niedriges Risiko“, „biometrische Fernidentifizierung“ und „Schaden“ zu definieren.
 - Die meisten Teilnehmer befürworteten ausdrücklich den risikobasierten Ansatz. Ein Ansatz, der sich auf die Risiken stützt, wurde im Vergleich zu einer undifferenzierten Regulierung aller KI-Systeme als die bessere Option betrachtet. Die Festlegung der Art der Risiken und Gefahren sollte von den jeweiligen Sektoren und vom Einzelfall abhängig gemacht werden. Bei der Bewertung der Risiken sollte auch deren rechtliche und sicherheitsrelevante Auswirkung berücksichtigt werden.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

M.E. wichtig zum Gesamtverständnis des AI-Act:

Aus der Gesetzesbegründung (Punkt 3.5):

- Durch ihre besonderen Merkmale (z. B. Undurchsichtigkeit, Komplexität, Datenabhängigkeit, autonomes Verhalten) kann die Verwendung von KI dazu führen, dass einige der in der EU-Grundrechtecharta (im Folgenden die „Charta“) verankerten Grundrechte verletzt werden. **Der Vorschlag zielt darauf ab, diese Grundrechte in hohem Maße zu schützen und durch einen klar festgelegten risikobasierten Ansatz verschiedene Ursachen für Risiken anzugehen. Alle an der Wertschöpfungskette Beteiligten unterliegen einer Reihe von Anforderungen an vertrauenswürdige KI und verhältnismäßigen Pflichten, damit die durch die Charta geschützten Rechte noch stärker geschützt werden:** die Würde des Menschen (Artikel 1), die Achtung des Privatlebens und der Schutz personenbezogener Daten (Artikel 7 und 8), die Nichtdiskriminierung (Artikel 21) und die Gleichheit von Frauen und Männern (Artikel 23).
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

M.E. wichtig zum Gesamtverständnis des AI-Act:

Aus der Gesetzesbegründung (Punkt 3.5):

- Mit dem Vorschlag soll verhindert werden, dass Menschen davor zurückschrecken, ihr Recht auf Meinungsfreiheit (Artikel 11) und auf Versammlungs- und Vereinigungsfreiheit (Artikel 12) auszuüben, und sichergestellt werden, dass das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht und die Unschuldsvermutung und Verteidigungsrechte (Artikel 47 und 48) sowie der **allgemeine Grundsatz guter Verwaltung gewahrt** werden. Zudem wird sich der Vorschlag in bestimmten Bereichen positiv auf einige gruppenspezifische Rechte auswirken, beispielsweise auf das Recht der Arbeitnehmer auf gerechte und angemessene Arbeitsbedingungen (Artikel 31), den Verbraucherschutz (Artikel 28), die Rechte des Kindes (Artikel 24) und die Integration von Menschen mit Behinderung (Artikel 26). Darüber hinaus geht es um das Recht auf ein hohes Umweltschutzniveau und die Verbesserung der Umweltqualität (Artikel 37), auch in Bezug auf die Gesundheit und Sicherheit von Menschen.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

M.E. wichtig zum Gesamtverständnis des AI-Act:

Aus der Gesetzesbegründung (Punkt 3.5):

- Die Verpflichtung zu Vorabtests, Risikomanagement und menschlicher Aufsicht werden die Achtung auch anderer Grundrechte erleichtern, da sich so das **Risiko, in kritischen Bereichen wie Bildung, Ausbildung**, Beschäftigung, wichtige Dienste, Strafverfolgung und Justiz **mithilfe der KI falsche oder verzerrte Entscheidungen zu treffen, verringern lässt**. Sollten Grundrechte trotzdem noch verletzt werden, werden die betroffenen Personen die Möglichkeit haben, wirksame Rechtsmittel einzulegen, da für Transparenz und Rückverfolgbarkeit der KI-Systeme im Verbund mit starken Ex-post-Kontrollen gesorgt ist.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Hochrisiko-KI-Systeme gem. Artikel 6 Abs. 2 KI-VO (Anhang III):

Als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2 gelten die in folgenden Bereichen aufgeführten KI-Systeme:

1. Biometrische Identifizierung und Kategorisierung natürlicher Personen:

a) KI-Systeme, die bestimmungsgemäß für die biometrische Echtzeit-Fernidentifizierung und nachträgliche biometrische Fernidentifizierung natürlicher Personen verwendet werden sollen;

2. Verwaltung und Betrieb kritischer Infrastrukturen:

a) KI-Systeme, die bestimmungsgemäß als Sicherheitskomponenten in der Verwaltung und im Betrieb des Straßenverkehrs sowie in der Wasser-, Gas-, Wärme- und Stromversorgung verwendet werden sollen



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Hochrisiko-KI-Systeme gem. Artikel 6 Abs. 2 KI-VO (Anhang III):

3. Allgemeine und berufliche Bildung:

- a) KI-Systeme, die bestimmungsgemäß für Entscheidungen über den Zugang oder die Zuweisung natürlicher Personen zu **Einrichtungen der allgemeinen und beruflichen Bildung** verwendet werden sollen;
 - b) KI-Systeme, die bestimmungsgemäß für die Bewertung von Schülern in **Einrichtungen der allgemeinen und beruflichen Bildung** und für die Bewertung der Teilnehmer an üblicherweise für die **Zulassung zu Bildungseinrichtungen** erforderlichen Tests verwendet werden sollen;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Hochrisiko-KI-Systeme gem. Artikel 6 Abs. 2 KI-VO (Anhang III):

4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit:

- a) KI-Systeme, die bestimmungsgemäß für die **Einstellung oder Auswahl natürlicher Personen** verwendet werden sollen, insbesondere für die Bekanntmachung freier Stellen, das Sichten oder Filtern von Bewerbungen und das Bewerten von Bewerbern in Vorstellungsgesprächen oder Tests;
 - b) KI-Systeme, die bestimmungsgemäß für **Entscheidungen über Beförderungen und über Kündigungen von Arbeitsvertragsverhältnissen**, für die **Aufgabenzuweisung** sowie für die **Überwachung und Bewertung der Leistung und des Verhaltens von Personen** in solchen Beschäftigungsverhältnissen verwendet werden sollen;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Hochrisiko-KI-Systeme gem. Artikel 6 Abs. 2 KI-VO (Anhang III):

5. Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen:

- a) KI-Systeme, die bestimmungsgemäß **von Behörden** oder im Namen von Behörden verwendet werden sollen, um zu beurteilen, ob **natürliche Personen Anspruch auf öffentliche Unterstützungsleistungen und -dienste haben** und ob **solche Leistungen und Dienste zu gewähren, einzuschränken, zu widerrufen oder zurückzufordern** sind;
 - b) KI-Systeme, die bestimmungsgemäß für die Kreditwürdigkeitsprüfung und Kreditpunktebewertung natürlicher Personen verwendet werden sollen, mit Ausnahme von KI-Systemen, die von Kleinanbietern für den Eigengebrauch in Betrieb genommen werden;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Hochrisiko-KI-Systeme gem. Artikel 6 Abs. 2 KI-VO (Anhang III):

c) KI-Systeme, die bestimmungsgemäß für die Entsendung oder Priorisierung des Einsatzes von Not- und Rettungsdiensten, einschließlich Feuerwehr und medizinischer Nothilfe, verwendet werden sollen;

6. Strafverfolgung:

a) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden für individuelle Risikobewertungen natürlicher Personen verwendet werden sollen, um das Risiko abzuschätzen, dass eine natürliche Person Straftaten begeht oder erneut begeht oder dass eine Person zum Opfer möglicher Straftaten wird;

b) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden als Lügendetektoren und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustands einer natürlichen Person verwendet werden sollen;



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Hochrisiko-KI-Systeme gem. Artikel 6 Abs. 2 KI-VO (Anhang III):

- c) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden zur Aufdeckung von Deepfakes gemäß Artikel 52 Absatz 3 verwendet werden sollen;
 - d) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden zur Bewertung der Verlässlichkeit von Beweismitteln im Zuge der Ermittlung oder Verfolgung von Straftaten verwendet werden sollen;
 - e) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden zur Vorhersage des Auftretens oder erneuten Auftretens einer tatsächlichen oder potenziellen Straftat auf der Grundlage des Profils natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 oder zur Bewertung von Persönlichkeitsmerkmalen und Eigenschaften oder vergangenen kriminellen Verhaltens natürlicher Personen oder von Gruppen verwendet werden sollen;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Hochrisiko-KI-Systeme gem. Artikel 6 Abs. 2 KI-VO (Anhang III):

f) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden zur Erstellung von Profilen natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 im Zuge der Aufdeckung, Ermittlung oder Verfolgung von Straftaten verwendet werden sollen;

g) KI-Systeme, die bestimmungsgemäß zur Kriminalanalyse natürlicher Personen eingesetzt werden sollen und es den Strafverfolgungsbehörden ermöglichen, große komplexe verknüpfte und unverknüpfte Datensätze aus verschiedenen Datenquellen oder in verschiedenen Datenformaten zu durchsuchen, um unbekannte Muster zu erkennen oder verdeckte Beziehungen in den Daten aufzudecken;



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Hochrisiko-KI-Systeme gem. Artikel 6 Abs. 2 KI-VO (Anhang III):

7. Migration, Asyl und Grenzkontrolle:

- a) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden als Lügendetektoren und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustands einer natürlichen Person verwendet werden sollen;
 - b) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden zur Bewertung eines Risikos verwendet werden sollen, einschließlich eines Sicherheitsrisikos, eines Risikos der irregulären Einwanderung oder eines Gesundheitsrisikos, das von einer natürlichen Person ausgeht, die in das Hoheitsgebiet eines Mitgliedstaats einzureisen beabsichtigt oder eingereist ist;
 - c) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden zur Überprüfung der Echtheit von Reisedokumenten und Nachweisunterlagen natürlicher Personen und zur Erkennung unechter Dokumente durch Prüfung ihrer Sicherheitsmerkmale verwendet werden sollen;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Hochrisiko-KI-Systeme gem. Artikel 6 Abs. 2 KI-VO (Anhang III):

d) KI-Systeme, die bestimmungsgemäß zuständige Behörden bei der Prüfung von Asyl- und Visumanträgen sowie Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick auf die Feststellung der Berechtigung der den Antrag stellenden natürlichen Personen unterstützen sollen;

8. Rechtspflege und demokratische Prozesse:

KI-Systeme, die bestimmungsgemäß Justizbehörden bei der Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften und bei der Anwendung des Rechts auf konkrete Sachverhalte unterstützen sollen.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Anforderungen an Hochrisiko-KI



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Anforderungen an Hochrisiko-KI

- Risikomanagementsystem
 - Daten und Daten-Governance
 - Technische Dokumentation
 - Aufzeichnungspflichten
 - Transparenz und Bereitstellung von Informationen für die Nutzer
 - Menschliche Aufsicht
 - Genauigkeit, Robustheit und Cybersicherheit
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Anforderungen an Hochrisiko-KI: Risikomanagementsystem

- Das Risikomanagementsystem versteht sich als ein kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus eines KI-Systems, der eine regelmäßige systematische Aktualisierung erfordert. Es umfasst folgende Schritte:
 - Ermittlung und Analyse der bekannten und vorhersehbaren Risiken, die von jedem Hochrisiko-KI-System ausgehen;
 - Abschätzung und Bewertung der Risiken, die entstehen können, wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird;
 - Bewertung anderer möglicherweise auftretender Risiken auf der Grundlage der Auswertung der Daten aus dem in Artikel 61 genannten System zur Beobachtung nach dem Inverkehrbringen;
 - Ergreifung geeigneter Risikomanagementmaßnahmen gemäß den Bestimmungen der folgenden Absätze.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Anforderungen an Hochrisiko-KI: Daten und Daten-Governance

- Für Trainings-, Validierungs- und Testdatensätze gelten geeignete Daten-Governance- und Datenverwaltungsverfahren. Diese Verfahren betreffen insbesondere
 - die einschlägigen konzeptionellen Entscheidungen,
 - die Datenerfassung,
 - relevante Datenaufbereitungsvorgänge wie Kommentierung, Kennzeichnung, Bereinigung, Anreicherung und Aggregation,
 - die Aufstellung relevanter Annahmen, insbesondere in Bezug auf die Informationen, die mit den Daten erfasst und dargestellt werden sollen,
 - eine vorherige Bewertung der Verfügbarkeit, Menge und Eignung der benötigten Datensätze
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Anforderungen an Hochrisiko-KI: Daten und Daten-Governance

- Die Trainings-, Validierungs- und Testdatensätze müssen, soweit dies für die Zweckbestimmung erforderlich ist, den Merkmalen oder Elementen entsprechen, die für die besonderen geografischen, verhaltensbezogenen oder funktionalen Rahmenbedingungen, unter denen das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, typisch sind.
- Soweit dies für die Beobachtung, Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist, dürfen die Anbieter solcher Systeme besondere Kategorien personenbezogener Daten ... verarbeiten, wobei sie angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen müssen, wozu auch technische Beschränkungen einer Weiterverwendung und modernste Sicherheits- und Datenschutzmaßnahmen wie Pseudonymisierung oder Verschlüsselung gehören, wenn der verfolgte Zweck durch eine Anonymisierung erheblich beeinträchtigt würde.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Anforderungen an Hochrisiko-KI: Technische Dokumentation

- Die technische Dokumentation eines Hochrisiko-KI-Systems wird erstellt, bevor dieses System in Verkehr gebracht oder in Betrieb genommen wird, und ist stets auf dem neuesten Stand zu halten.
 - Die technische Dokumentation wird so erstellt, dass aus ihr der Nachweis hervorgeht, wie das Hochrisiko-KI-System die Anforderungen dieses Kapitels erfüllt, und dass den zuständigen nationalen Behörden und den notifizierten Stellen alle Informationen zur Verfügung stehen, die erforderlich sind, um zu beurteilen, ob das KI-System diese Anforderungen erfüllt. Sie enthält zumindest die in Anhang IV genannten Angaben.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Anforderungen an Hochrisiko-KI: Aufzeichnungspflichten

- Hochrisiko-KI-Systeme werden mit Funktionsmerkmalen konzipiert und entwickelt, die eine automatische Aufzeichnung von Vorgängen und Ereignissen („Protokollierung“) während des Betriebs der Hochrisiko-KI-Systeme ermöglichen. Diese Protokollierung muss anerkannten Normen oder gemeinsamen Spezifikationen entsprechen.
 - Die Protokollierung gewährleistet, dass das Funktionieren des KI-Systems während seines gesamten Lebenszyklus in einem der Zweckbestimmung des Systems angemessenen Maße rückverfolgbar ist.
 - Die Protokollierung ermöglicht insbesondere die Überwachung des Betriebs des Hochrisiko-KI-Systems im Hinblick auf das Auftreten von Situationen, die dazu führen können, dass das KI-System ein Risiko im Sinne des Artikels 65 Absatz 1 birgt, oder die zu einer wesentlichen Änderung führen, und erleichtert so die Beobachtung nach dem Inverkehrbringen gemäß Artikel 61.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Anforderungen an Hochrisiko-KI: Aufzeichnungspflichten

- Die Protokollierungsfunktionen der in Anhang III Absatz 1 Buchstabe a genannten Hochrisiko-KI-Systeme müssen zumindest Folgendes umfassen:
 - Aufzeichnung jedes Zeitraums der Verwendung des Systems (Datum und Uhrzeit des Beginns und des Endes jeder Verwendung);
 - die Referenzdatenbank, mit der das System die Eingabedaten abgleicht;
 - die Eingabedaten, mit denen die Abfrage zu einer Übereinstimmung geführt hat;
 - die Identität der gemäß Artikel 14 Absatz 5 an der Überprüfung der Ergebnisse beteiligten natürlichen Personen.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Anforderungen an Hochrisiko-KI: Transparenz und Bereitstellung von Informationen für die Nutzer

- Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass ihr Betrieb hinreichend transparent ist, damit die Nutzer die Ergebnisse des Systems angemessen interpretieren und verwenden können. Die Transparenz wird auf eine geeignete Art und in einem angemessenen Maß gewährleistet, damit die Nutzer und Anbieter ihre in Kapitel 3 dieses Titels festgelegten einschlägigen Pflichten erfüllen können.
 - Hochrisiko-KI-Systeme werden mit Gebrauchsanweisungen in einem geeigneten digitalen Format bereitgestellt oder auf andere Weise mit Gebrauchsanweisungen versehen, die präzise, vollständige, korrekte und eindeutige Informationen in einer für die Nutzer relevanten, barrierefrei zugänglichen und verständlichen Form enthalten.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Anforderungen an Hochrisiko-KI: Menschliche Aufsicht

- Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie während der Dauer der Verwendung des KI-Systems – auch mit geeigneten Werkzeugen einer Mensch-Maschine-Schnittstelle – von natürlichen Personen wirksam beaufsichtigt werden können.
 - Die menschliche Aufsicht dient der Verhinderung oder Minimierung der Risiken für die Gesundheit, die Sicherheit oder die Grundrechte, die entstehen können, wenn ein Hochrisiko-KI-System bestimmungsgemäß oder unter im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird, insbesondere wenn solche Risiken trotz der Einhaltung anderer Anforderungen dieses Kapitels fortbestehen.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Anforderungen an Hochrisiko-KI: Genauigkeit, Robustheit und Cybersicherheit

- Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie im Hinblick auf ihre Zweckbestimmung ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren.
 - Die Genauigkeitsgrade und die relevanten Genauigkeitskennzahlen von Hochrisiko-KI-Systemen werden in der ihnen beigefügten Gebrauchsanweisung angegeben.
 - Hochrisiko-KI-Systeme müssen widerstandsfähig gegenüber Fehlern, Störungen oder Unstimmigkeiten sein, die innerhalb des Systems oder der Umgebung, in der das System betrieben wird, insbesondere wegen seiner Interaktion mit natürlichen Personen oder anderen Systemen auftreten können.
 - Die Robustheit von Hochrisiko-KI-Systemen kann durch technische Redundanz erreicht werden, was auch Sicherungs- oder Störungssicherheitspläne umfassen kann.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Pflichten der Anbietenden von Hochrisiko-KI (Art. 16 KI-VO)



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Pflichten der Anbietenden von Hochrisiko-KI (Art. 16 KI-VO)

Anbieter von Hochrisiko-KI-Systemen müssen

- sicherstellen, dass ihre Hochrisiko-KI-Systeme die Anforderungen in Kapitel 2 dieses Titels erfüllen;
 - über ein Qualitätsmanagementsystem verfügen, das dem Artikel 17 entspricht;
 - die technische Dokumentation des Hochrisiko-KI-Systems erstellen;
 - die von ihren Hochrisiko-KI-Systemen automatisch erzeugten Protokolle aufbewahren, wenn dies ihrer Kontrolle unterliegt;
 - sicherstellen, dass das Hochrisiko-KI-System dem betreffenden Konformitätsbewertungsverfahren unterzogen wird, bevor es in Verkehr gebracht oder in Betrieb genommen wird;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Pflichten der Anbietenden von Hochrisiko-KI (Art. 16 KI-VO)

Anbieter von Hochrisiko-KI-Systemen müssen

- den in Artikel 51 genannten Registrierungspflichten nachkommen;
 - die erforderlichen Korrekturmaßnahmen ergreifen, wenn das Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels nicht erfüllt;
 - die zuständigen nationalen Behörden der Mitgliedstaaten, in denen sie das System bereitgestellt oder in Betrieb genommen haben, und gegebenenfalls die notifizierte Stelle über die Nichtkonformität und bereits ergriffene Korrekturmaßnahmen informieren;
 - die CE-Kennzeichnung an ihren Hochrisiko-KI-Systemen anbringen, um die Konformität mit dieser Verordnung gemäß Artikel 49 anzuzeigen;
 - auf Anfrage einer zuständigen nationalen Behörde nachweisen, dass das Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels erfüllt.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Plichten der Anbietenden von Hochrisiko-KI: Qualitätsmanagementsystem

Anbieter von Hochrisiko-KI-Systemen richten ein Qualitätsmanagementsystem ein, das die Einhaltung dieser Verordnung gewährleistet. Dieses System wird systematisch und ordnungsgemäß in Form schriftlicher Regeln, Verfahren und Anweisungen dokumentiert und umfasst mindestens folgende Aspekte:

- ein Konzept zur Einhaltung der Regulierungsvorschriften, was die Einhaltung der Konformitätsbewertungsverfahren und der Verfahren für das Management von Änderungen an den Hochrisiko-KI-Systemen miteinschließt;
 - Techniken, Verfahren und systematische Maßnahmen für den Entwurf, die Entwurfskontrolle und die Entwurfsprüfung des Hochrisiko-KI-Systems;
 - Techniken, Verfahren und systematische Maßnahmen für die Entwicklung, Qualitätskontrolle und Qualitätssicherung des Hochrisiko-KI-Systems;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Plichten der Anbietenden von Hochrisiko-KI: Qualitätsmanagementsystem

- Untersuchungs-, Test- und Validierungsverfahren, die vor, während und nach der Entwicklung des Hochrisiko-KI-Systems durchzuführen sind, und die Häufigkeit der Durchführung;
 - die technischen Spezifikationen und Normen, die anzuwenden sind, falls die einschlägigen harmonisierten Normen nicht vollständig angewandt werden, sowie die Mittel, mit denen gewährleistet werden soll, dass das Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels erfüllt;
 - Systeme und Verfahren für das Datenmanagement, einschließlich Datenerfassung, Datenanalyse, Datenkennzeichnung, Datenspeicherung, Datenfilterung, Datenauswertung, Datenaggregation, Vorratsdatenspeicherung und sonstiger Vorgänge in Bezug auf die Daten, die im Vorfeld und für die Zwecke des Inverkehrbringens oder der Inbetriebnahme von Hochrisiko-KI-Systemen durchgeführt werden;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Plichten der Anbietenden von Hochrisiko-KI: Qualitätsmanagementsystem

- das in Artikel 9 genannte Risikomanagementsystem;
- Einrichtung, Anwendung und Aufrechterhaltung eines Systems zur Beobachtung nach dem Inverkehrbringen gemäß Artikel 61; Verfahren zur Meldung schwerwiegender Vorfälle und Fehlfunktionen gemäß Artikel 62;
- Kommunikation mit zuständigen nationalen Behörden, zuständigen Behörden, auch sektoralen Behörden, die den Zugang zu Daten gewähren oder erleichtern, sowie mit notifizierten Stellen, anderen Akteuren, Kunden oder sonstigen interessierten Kreisen;
- Systeme und Verfahren für die Aufzeichnung aller einschlägigen Unterlagen und Informationen;
- Ressourcenmanagement, einschließlich Maßnahmen im Hinblick auf die Versorgungssicherheit;
- einen Rechenschaftsrahmen, der die Verantwortlichkeiten der Leitung und des sonstigen Personals in Bezug auf alle in diesem Absatz aufgeführten Aspekte regelt.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Plichten der Anbietenden von Hochrisiko-KI: technische Dokumentation des Hochrisiko-KI-Systems

Anbieter von Hochrisiko-KI-Systemen erstellen die in Artikel 11 genannte technische Dokumentation gemäß Anhang IV.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Plichten der Anbietenden von Hochrisiko-KI: Konformitätsbewertung

Die Anbieter von Hochrisiko-KI-Systemen stellen sicher, dass ihre Systeme vor dem Inverkehrbringen oder der Inbetriebnahme dem betreffenden Konformitätsbewertungsverfahren gemäß Artikel 43 unterzogen werden.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Pflichten der Anbietenden von Hochrisiko-KI: Bevollmächtigte

- Anbieter, die außerhalb der Union niedergelassen sind, benennen vor der Bereitstellung ihrer Systeme in der Union schriftlich einen in der Union niedergelassenen Bevollmächtigten, wenn kein Einführer festgestellt werden kann.
 - Der Bevollmächtigte nimmt die Aufgaben wahr, die in seinem vom Anbieter erhaltenen Auftrag festgelegt sind. Der Auftrag ermächtigt den Bevollmächtigten zumindest zur Wahrnehmung folgender Aufgaben:
 - Bereithaltung eines Exemplars der EU-Konformitätserklärung und der technischen Dokumentation für die zuständigen nationalen Behörden und die in Artikel 63 Absatz 7 genannten nationalen Behörden;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Pflichten der Anbietenden von Hochrisiko-KI: Bevollmächtigte

- Übermittlung aller Informationen und Unterlagen, die erforderlich sind, um die Konformität eines Hochrisiko-KI-Systems mit den Anforderungen in Kapitel 2 dieses Titels nachzuweisen, an eine zuständige nationale Behörde auf deren begründetes Verlangen, einschließlich der Gewährung des Zugangs zu den vom Hochrisiko-KI-System automatisch erzeugten Protokollen, soweit diese Protokolle aufgrund einer vertraglichen Vereinbarung mit dem Nutzer oder auf gesetzlicher Grundlage der Kontrolle des Anbieters unterliegen;
 - Zusammenarbeit mit den zuständigen nationalen Behörden auf deren begründetes Verlangen bei allen Maßnahmen, die Letztere im Zusammenhang mit dem Hochrisiko-KI-System ergreifen.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Pflichten der Anbietenden von Hochrisiko-KI: Einführende

Bevor sie ein Hochrisiko-KI-System in Verkehr bringen, stellen die Einführende solcher Systeme sicher, dass

- der Anbieter des KI-Systems das betreffende Konformitätsbewertungsverfahren durchgeführt hat;
 - der Anbieter die technische Dokumentation gemäß Anhang IV erstellt hat;
 - das System mit der erforderlichen Konformitätskennzeichnung versehen ist und ihm die erforderlichen Unterlagen und Gebrauchsanweisungen beigelegt sind.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Pflichten der Händler, Einführer, Nutzer oder sonstiger Dritter von Hochrisiko-KI



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Pflichten der Händler, Einführer, Nutzer oder sonstiger Dritter von Hochrisiko-KI

In den folgenden Fällen gelten Händler, Einführer, Nutzer oder sonstige Dritte als Anbieter für die Zwecke dieser Verordnung und unterliegen den Anbieterpflichten gemäß Artikel 16 (s. oben):

- wenn sie ein Hochrisiko-KI-System unter ihrem Namen oder ihrer Marke in Verkehr bringen oder in Betrieb nehmen;
 - wenn sie die Zweckbestimmung eines bereits im Verkehr befindlichen oder in Betrieb genommenen Hochrisiko-KI-Systems verändern;
 - wenn sie eine wesentliche Änderung an dem Hochrisiko-KI-System vornehmen.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Pflichten der Nutzer von Hochrisiko-KI (Artikel 29 KI-VO)



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Pflichten der Nutzer von Hochrisiko-KI

Die Nutzer von Hochrisiko-KI-Systemen verwenden solche Systeme entsprechend der den Systemen beigefügten Gebrauchsanweisung und gemäß den Absätzen 2 und 5.

Die Pflichten nach Absatz 1 lassen sonstige Pflichten der Nutzer nach Unionsrecht oder nationalem Recht sowie das Ermessen der Nutzer bei der Organisation ihrer eigenen Ressourcen und Tätigkeiten zur Wahrnehmung der vom Anbieter angegebenen Maßnahmen der menschlichen Aufsicht unberührt.

Unbeschadet des Absatzes 1 und soweit die Eingabedaten seiner Kontrolle unterliegen, sorgen die Nutzer dafür, dass die Eingabedaten der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Pflichten der Nutzer von Hochrisiko-KI

Die Nutzer überwachen den Betrieb des Hochrisiko-KI-Systems anhand der Gebrauchsanweisung. Haben sie Grund zu der Annahme, dass die Verwendung gemäß der Gebrauchsanweisung dazu führen kann, dass das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 65 Absatz 1 birgt, so informieren sie den Anbieter oder Händler und setzen die Verwendung des Systems aus. Sie informieren den Anbieter oder Händler auch, wenn sie einen schwerwiegenden Vorfall oder eine Fehlfunktion im Sinne des Artikels 62 festgestellt haben, und unterbrechen die Verwendung des KI-Systems. Kann der Nutzer den Anbieter nicht erreichen, so gilt Artikel 62 entsprechend.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Pflichten der Nutzer von Hochrisiko-KI

Nutzer von Hochrisiko-KI-Systemen bewahren die von ihrem Hochrisiko-KI-System automatisch erzeugten Protokolle auf, soweit diese Protokolle ihrer Kontrolle unterliegen. Die Protokolle werden für einen Zeitraum aufbewahrt, der der Zweckbestimmung des Hochrisiko-KI-Systems und den geltenden rechtlichen Verpflichtungen nach Unionsrecht oder nationalem Recht angemessen ist.

Die Nutzer von Hochrisiko-KI-Systemen verwenden die gemäß Artikel 13 bereitgestellten Informationen, um gegebenenfalls ihrer Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Artikel 35 der Verordnung (EU) 2016/679 oder Artikel 27 der Richtlinie (EU) 2016/680 nachzukommen.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Notifizierende Behörden & Konformitätsbewertungsstellen & Konformitätsbewertung

Jeder Mitgliedstaat sorgt für die Benennung oder Schaffung einer notifizierenden Behörde, die für die Einrichtung und Durchführung der erforderlichen Verfahren zur Bewertung, Benennung und Notifizierung von Konformitätsbewertungsstellen und für deren Überwachung zuständig ist.

Konformitätsbewertungsstellen beantragen ihre Notifizierung bei der notifizierenden Behörde des Mitgliedstaats, in dem sie ansässig sind.

Die Konformitätsbewertung wird in Art. 43 KI-VO geregelt, ist aber recht kompliziert...



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

EU-Konformitätserklärung & CE-Konformitätskennzeichnung

Der Anbieter stellt für jedes KI-System eine schriftliche EU-Konformitätserklärung aus und hält sie für einen Zeitraum von 10 Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des KI-Systems für die zuständigen nationalen Behörden bereit. Aus der EU-Konformitätserklärung geht hervor, für welches KI-System sie ausgestellt wurde. Ein Exemplar der EU-Konformitätserklärung wird den zuständigen nationalen Behörden auf Anfrage zur Verfügung gestellt.

Die CE-Kennzeichnung wird gut sichtbar, leserlich und dauerhaft an Hochrisiko-KI-Systemen angebracht. Falls die Art des Hochrisiko-KI-Systems dies nicht zulässt oder nicht rechtfertigt, wird sie auf der Verpackung oder gegebenenfalls den Begleitunterlagen angebracht....



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Transparenzpflichten für „bestimmte“ KI-Systeme (mit geringem bzw. minimalem Risiko)



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Transparenzpflichten für „bestimmte“ KI-Systeme (mit geringem bzw. minimalem Risiko)

- Die Anbieter stellen sicher, dass KI-Systeme, **die für die Interaktion mit natürlichen Personen bestimmt sind**, so konzipiert und entwickelt werden, dass natürlichen Personen mitgeteilt wird, dass sie es mit einem KI-System zu tun haben, es sei denn, dies ist aufgrund der Umstände und des Kontexts der Nutzung offensichtlich. Diese Vorgabe gilt nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten zugelassene KI-Systeme, es sei denn, diese Systeme stehen der Öffentlichkeit zur Anzeige einer Straftat zur Verfügung.
 - Die Verwender eines **Emotionserkennungssystems** oder eines Systems zur biometrischen Kategorisierung informieren die davon betroffenen natürlichen Personen über den Betrieb des Systems. Diese Vorgabe gilt **nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten zugelassene KI-Systeme**, die zur biometrischen Kategorisierung verwendet werden.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Transparenzpflichten für „bestimmte“ KI-Systeme (mit geringem bzw. minimalem Risiko)

- Nutzer eines **KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert**, die wirklichen Personen, Gegenständen, Orten oder anderen Einrichtungen oder Ereignissen merklich ähneln und einer Person fälschlicherweise als echt oder wahrhaftig erscheinen würden („Deepfake“), **müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden.**
 - Unterabsatz 1 gilt jedoch **nicht**, wenn die **Verwendung zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten gesetzlich zugelassen** oder für die Ausübung der durch die Charta der Grundrechte der Europäischen Union **garantierten Rechte auf freie Meinungsäußerung und auf Freiheit der Kunst und Wissenschaft erforderlich** ist und **geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter** bestehen.
-

Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz



KI-Reallabore



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

KI-Reallabore

- KI-Reallabore, die von den zuständigen Behörden eines oder mehrerer Mitgliedstaaten oder vom Europäischen Datenschutzbeauftragten eingerichtet werden, bieten eine **kontrollierte Umgebung, um die Entwicklung, Erprobung und Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme nach einem spezifischen Plan zu erleichtern**. Dies geschieht unter direkter Aufsicht und Anleitung der zuständigen Behörden, um die Einhaltung der Anforderungen dieser Verordnung und gegebenenfalls anderer Rechtsvorschriften der Union und der Mitgliedstaaten, die innerhalb des Reallabors beaufsichtigt wird, sicherzustellen.
- Soweit die **innovativen KI-Systeme personenbezogene Daten verarbeiten** oder anderweitig der Aufsicht anderer nationaler Behörden oder zuständiger Behörden unterstehen, die den Zugang zu Daten gewähren oder unterstützen, sorgen die Mitgliedstaaten dafür, dass die **nationalen Datenschutzbehörden und diese anderen nationalen Behörden in den Betrieb des KI-Reallabors einbezogen** werden.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

KI-Reallabore

- Die KI-Reallabore lassen die Aufsichts- und Abhilfebefugnisse der zuständigen Behörden unberührt. Alle erheblichen Risiken für die Gesundheit und Sicherheit und die Grundrechte, die bei der Entwicklung und Erprobung solcher Systeme festgestellt werden, führen zur sofortigen Risikominderung oder, falls dies nicht möglich ist, zur Aussetzung des Entwicklungs- und Erprobungsprozesses bis eine solche Risikominderung erfolgt ist.
 - Die am KI-Reallabor Beteiligten bleiben nach geltendem Recht der Union und der Mitgliedstaaten für Schäden haftbar, die Dritten infolge der Erprobung im Reallabor entstehen.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Weiterverarbeitung personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im KI-Reallabore

- Im KI-Reallabor dürfen personenbezogene Daten, die rechtmäßig für andere Zwecke erhoben wurden, zur Entwicklung und Erprobung bestimmter innovativer KI-Systeme im Reallabor unter folgenden Bedingungen verarbeitet werden:
 - die innovativen KI-Systeme werden entwickelt, um ein erhebliches öffentliches Interesse in einem oder mehreren der folgenden Bereiche zu wahren:
 - Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten ...
 - öffentliche Sicherheit und öffentliche Gesundheit, einschließlich Verhütung, Bekämpfung und Behandlung von Krankheiten,
 - hohes Umweltschutzniveau und Verbesserung der Umweltqualität;
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Beobachtung nach dem Inverkehrbringen durch die Anbieter und Plan für die Beobachtung nach dem Inverkehrbringen für Hochrisiko-KI-Systeme

- Anbieter müssen ein System zur Beobachtung nach dem Inverkehrbringen einrichten und dokumentieren, das im Verhältnis zur Art der KI-Technik und zu den Risiken des Hochrisiko-KI-Systems steht.
 - Mit dem System zur Beobachtung nach dem Inverkehrbringen müssen sich die einschlägigen von den Nutzern bereitgestellten oder aus anderen Quellen gesammelten Daten zur Leistung der Hochrisiko-KI-Systeme über deren gesamte Lebensdauer hinweg aktiv und systematisch erfassen, dokumentieren und analysieren lassen, und der Anbieter muss damit die fortdauernde Einhaltung der in Titel III Kapitel 2 genannten Anforderungen an die KI-Systeme bewerten können.
-




Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

EU-Datenbank für eigenständige Hochrisiko-KI-Systeme

- Die Kommission errichtet und pflegt in Zusammenarbeit mit den Mitgliedstaaten eine EU-Datenbank mit den in Absatz 2 genannten Informationen über Hochrisiko-KI-Systeme nach Artikel 6 Absatz 2, die gemäß Artikel 51 registriert werden.
 - Die in Anhang VIII aufgeführten Daten werden von den Anbietern in die EU-Datenbank eingegeben. Die Kommission leistet ihnen dabei technische und administrative Unterstützung.
 - Die in der EU-Datenbank gespeicherten Daten sind öffentlich zugänglich.
-

Übereinstimmung der großen Sprachmodelle mit EU AI Act

	 OpenAI	 cohere	 stability.ai	 ANTHROPIC	 Google	 BigScience	 Meta	 AI21 labs	 ALEPH ALPHA	 ELEutherAI	Totals
Draft AI Act Requirements	GPT-4	Cohere Command	Stable Diffusion v2	Claude	PaLM 2	BLOOM	LLaMA	Jurassic-2	Luminous	GPT-NeoX	
Data sources	● ○ ○ ○ ○	● ● ● ○ ○	● ● ● ● ●	○ ○ ○ ○ ○	● ● ● ○ ○	● ● ● ● ●	● ● ● ● ●	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ● ● ●	22
Data governance	● ● ○ ○ ○	● ● ● ○ ○	● ● ○ ○ ○	○ ○ ○ ○ ○	● ● ● ○ ○	● ● ● ● ●	● ● ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ● ○ ○	19
Copyrighted data	○ ○ ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ● ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ● ● ●	7
Compute	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ● ● ●	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ● ● ●	● ● ● ● ●	○ ○ ○ ○ ○	● ○ ○ ○ ○	● ● ● ● ●	17
Energy	○ ○ ○ ○ ○	● ○ ○ ○ ○	● ● ● ● ●	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ● ● ●	● ● ● ● ●	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ● ● ●	16
Capabilities & limitations	● ● ● ● ●	● ● ● ● ○	● ● ● ● ●	● ○ ○ ○ ○	● ● ● ● ●	● ● ● ● ○	● ● ○ ○ ○	● ● ○ ○ ○	● ○ ○ ○ ○	● ● ● ● ○	27
Risks & mitigations	● ● ● ○ ○	● ● ● ○ ○	● ○ ○ ○ ○	● ○ ○ ○ ○	● ● ● ○ ○	● ● ○ ○ ○	● ○ ○ ○ ○	● ● ○ ○ ○	○ ○ ○ ○ ○	● ○ ○ ○ ○	16
Evaluations	● ● ● ● ●	● ● ● ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ● ○ ○	● ● ● ● ○	● ● ○ ○ ○	○ ○ ○ ○ ○	● ○ ○ ○ ○	● ○ ○ ○ ○	15
Testing	● ● ● ○ ○	● ● ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ● ○ ○	● ● ○ ○ ○	○ ○ ○ ○ ○	● ○ ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	10
Machine-generated content	● ● ● ○ ○	● ● ● ○ ○	○ ○ ○ ○ ○	● ● ● ○ ○	● ● ● ○ ○	● ● ● ○ ○	○ ○ ○ ○ ○	● ● ● ○ ○	● ○ ○ ○ ○	● ● ○ ○ ○	21
Member states	● ● ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ○ ○ ○	● ● ● ● ●	○ ○ ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ○ ○ ○ ○	○ ○ ○ ○ ○	9
Downstream documentation	● ● ● ○ ○	● ● ● ● ●	● ● ● ● ●	○ ○ ○ ○ ○	● ● ● ● ●	● ● ● ● ●	● ● ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	● ● ● ○ ○	24
Totals	25 / 48	23 / 48	22 / 48	7 / 48	27 / 48	36 / 48	21 / 48	8 / 48	5 / 48	29 / 48	

Deutsche Unternehmen sehen ChatGPT skeptisch



Stimmungen zu

11 Aussagen zur ChatGPT

Stimmungen





Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

EU-AI-Act Übersicht Anforderungen KI



Dr. Holger Schmidt – Netzökonom

Live-Session "Digitale Transformation, Plattformökonomie & KI" am 04. Juli 2023

<https://www.youtube.com/watch?v=GdmTbBRCZoM&t=1451s>



Netzökonom Dr. Holger Schmidt

Dr. Holger Schmidt ist Experte für digitale Ökonomie. Seine Kernthemen sind Plattform-Ökonomie, digitale Geschäftsmodelle und künstliche Intelligenz. Der Volkswirt lehrt digitale Transformation an der TU Darmstadt, schreibt Bücher und ist Co-Host eines F.A.Z.-Podcasts zur Künstlichen Intelligenz. Mit der Plattformökonomie beschäftigt er sich seit rund zehn Jahren, vor allem mit deren Bedeutung als digitales Geschäftsmodell und den ökonomischen Effekten auf gesamtwirtschaftlicher Ebene.

[> Unverbindliche Buchungsanfrage](#)

Vorträge zu künstlicher Intelligenz / ChatGPT

Bei seinen Reden und Vorträgen rund um Künstliche Intelligenz / ChatGPT richtet sich Holger Schmidt gerne nach Ihren Schwerpunkten. Seine Vorträge richten sich an Unternehmen, die

- die ökonomischen Effekte der KI einschätzen wollen.
- auf Basis der künstliche Intelligenz neue digitale Geschäftsmodelle aufbauen wollen,
- ihre Belegschaft auf die Anforderungen des KI-Zeitalters vorbereiten wollen.

Newsletter Digitale Transformation

Mein Newsletter mit relevanten Nachrichten und Forschungsergebnissen zur **Digitalen Transformation & Plattformökonomie**
14-tägig | Kostenlos abonnieren

Mit der Anmeldung zum Newsletter akzeptiere ich die [Datenschutzbestimmungen](#)

[Kostenlos anmelden](#)



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Fazit: Guijarro Santos „Nicht besser als nichts“ (ZfDR 2023, 23)

- Aus der Perspektive der EU ist KI ein Wirtschaftsgut, das Grundrechtsrisiken birgt. KI-Regulierung ist Geopolitik. Entsprechend ist der Anwendungsbereich des KI-Verordnungsentwurfs einerseits territorial, personell und sachlich denkbar weit. Andererseits werden aufgrund des sog. risikobasierten Regulierungsansatzes KI-Systeme auf dem EU-Binnenmarkt effektiv kaum beschränkt. Daten und datenbasierte Technologien – wie KI-Systeme – sollen im digitalen Binnenmarkt fließen.
 - Die Qualitätsanforderungen an sog. Hochrisiko-KI-Systeme verfehlen den anvisierten Grundrechtsschutz. Sie denken die Entwicklung und Nutzung von KI-Systemen losgelöst von gesellschaftlichen Machtverhältnissen, die aber (mit)ursächlich für die anvisierten Grundrechtsrisiken sind.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Fazit: Guijarro Santos „Nicht besser als nichts“ (ZfDR 2023, 23)

- Die EU gibt die Konkretisierung von Begriffen wie „statistische Genauigkeit“ und „Bias“ an privat organisierte Normierungsbehörden ab. Damit suggeriert die EU, dass es sich um technisch eindeutige Begriffe handeln würde. Mit ihrer Konkretisierung werden aber politische, grundrechtsrelevante Entscheidungen getroffen. Damit entdemokratisiert der KI-Verordnungsentwurf den Grundrechtsschutz.
 - Die Einhaltung der Qualitätsanforderungen wird stark relativiert. Aufgrund des risikobasierten Regulierungsansatzes müssen nur ausgewählte KI-Systeme die Anforderungen erfüllen. Kleine KI-Unternehmen sind zu weniger verpflichtet als größere KI-Unternehmen, obwohl sie gleichermaßen grundrechtsriskante KI-Systeme auf dem Markt platzieren können. Insbesondere jedoch behandelt der KI-Verordnungsentwurf KI-Anbieter:innen als „vertrauenswürdige Partei“, setzt auf Selbst- statt externer Kontrolle und räumt den KI-Anbieter:innen damit einen enormen Ermessensspielraum ein.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Fazit: Guijarro Santos „Nicht besser als nichts“ (ZfDR 2023, 23)

- Die Aufgrund des risikobasierten Regulierungsansatzes ist ein normorientiertes Vorgehen bei der Bestimmung des Gestaltungsspielraums der Mitgliedsstaaten schwierig. Es ist ungewiss, ob und wenn ja, inwiefern die Mitgliedstaaten neben die KI-Verordnung eigene KI-Regulierungen erlassen dürfen.
 - KI-Regulierung kann auch aus der Perspektive sozial marginalisierter Personengruppenerfolgen und dann auch die gesellschaftlichen Machtverhältnisse mit in den Blick nehmen, in denen ein KI-System entwickelt und genutzt werden soll. Statt einer Dachregulierung erscheint ein sektoraler, kontextgebundener Regulierungsansatz grundrechtswirksamer, der die epistemischen Grenzen von KI-Systemen und das Zusammenwirken mit gesellschaftlichen Machtverhältnissen ernst nimmt sowie auf demokratische Partizipation beider Regelbildung von Datenregimes angelegt ist.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Verbesserungsvorschläge: Becker „Der Kommissionsentwurf für eine KI-Verordnung – Gefahr für die Wissenschaftsfreiheit?“ ZfDR 2023, 164

- Der Entwurf der KI-VOE ist mit einigen Eingriffen in die Wissenschaftsfreiheit aus Art. 13 GRC verbunden. Dabei ist das Groß der Eingriffe als rechtfertigbar zu qualifizieren, während indes bei einzelnen sowohl die Erforderlichkeit als auch die Angemessenheit in Frage gestellt werden kann. Ziel der KI-VOE ist es einen Ausgleich zwischen Risiken und Chancen von KI-Systemen zu wahren und den Schutz der Grundrechte und Grundfreiheiten zu gewährleisten. Dies ist in Bezug auf die Wissenschaftsfreiheit nicht an allen Stellen des KI-VOE gelungen.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Verbesserungsvorschläge: Becker „Der Kommissionsentwurf für eine KI-Verordnung – Gefahr für die Wissenschaftsfreiheit?“ ZfDR 2023, 164

- Verbesserungswürdig ist zunächst die zentrale Definition des Anbieters nach Art. 3 Nr. 2 KI-VOE. Zwar ist die Einbeziehung von Forschenden unter die Definition nicht zwingend, aber durch eine Klarstellung, dass das Publizieren von Forschungsergebnissen nicht erfasst ist, kann Rechtssicherheit gewonnen werden. Da es sich bei der Einordnung der Publikation von Forschungsergebnissen um eine Auslegungsfrage handelt, wäre diesbezüglich eine Klarstellung im Rahmen der Erwägungsgründe als ausreichend zu bewerten. In der Folge würden die Eingriffe in die Wissenschaftsfreiheit, wie sie sich aus der Regulierung von Hochrisiko-KI-Systemen ergeben würden, weitgehend entfallen. Soweit Forschende dennoch als Anbieter zu qualifizieren sind, weil sie tatsächlich KI-Systeme in den Verkehr bringen oder in Betrieb nehmen, wäre jedenfalls das Eingriffsniveau gesenkt und die Gleichbehandlung mit anderen Marktteilnehmern einfacher zurechtfertigen.



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Verbesserungsvorschläge: Becker „Der Kommissionsentwurf für eine KI-Verordnung – Gefahr für die Wissenschaftsfreiheit?“ ZfDR 2023, 164

- Verbleibend wären Wissenschaftler weiterhin den Regelungen des KI-VOE für Nutzer von Hochrisiko-KI-Systemen unterworfen, dies allerdings auch nur dann, wenn deren Handlungen auch tatsächlich mit dem angepeilten Adressatenkreis vergleichbar sind.
 - Im Rahmen der nach Art. 5 KI-VOE verbotenen Technologien sollte ebenfalls eine allgemeine Forschungsprivilegierung verankert werden. Die Forschung kann dabei auf geschützte Umgebungen, wie sie der KI-VOE richtiggehend in KI-Reallaboren erkennt, gesehen werden.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Verbesserungsvorschläge: Becker „Der Kommissionsentwurf für eine KI-Verordnung – Gefahr für die Wissenschaftsfreiheit?“ ZfDR 2023, 164

- Um Rechtssicherheit zu schaffen, liegt es nahe erforderliche Forschungsausnahmen im unmittelbar bindenden Teil der Verordnung zu verankern, z.B. wie folgt:
 - Diese Verordnung gilt nicht für KI-Systeme und deren Ergebnisse, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden.
 - Diese Verordnung gilt nicht für Forschungs- und Entwicklungsaktivitäten zu KI-Systemen.
 - Auch sollte hinsichtlich der Forschung in öffentlichen Einrichtungen, wie Universitäten, auf der einen Seite und privaten Unternehmen auf der anderen Seite differenziert werden.
-



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Übersicht

TITEL I – ALLGEMEINE BESTIMMUNGEN

TITEL II – VERBOTENE PRAKTIKEN IM BEREICH DER KÜNSTLICHEN INTELLIGENZ

TITEL III – HOCHRISIKO-KI-SYSTEME

TITEL IV – TRANSPARENZPFLICHTEN FÜR BESTIMMTE KI-SYSTEME

TITEL V – MAßNAHMEN ZUR INNOVATIONSFÖRDERUNG

TITEL VI – LEITUNGSSTRUKTUR



Entwurf KI-Verordnung = Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Übersicht

TITEL VII – EU-DATENBANK FÜR EIGENSTÄNDIGE HOCHRISIKO-KI-SYSTEME

TITEL VIII – BEOBACHTUNG NACH DEM INVERKEHRBRINGEN,
INFORMATIONSAUSTAUSCH, MARKTÜBERWACHUNG

Titel IX – VERHALTENSKODIZES

Titel X – VERTRAULICHKEIT UND SANKTIONEN

<https://lexparency.de/eu/52021PC0206/>



Haftung von Anbietenden von KI-Generatoren

Entwurf Richtlinie über KI-Haftung = Richtlinie zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstlicher Intelligenz



Haftung von Anbietenden von KI-Generatoren

Entwurf Richtlinie über KI-Haftung = Richtlinie zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstlicher Intelligenz

Diese Richtlinie (noch nicht in Kraft!) soll einen harmonisierten Rechtsrahmen auf Unionsebene schaffen und die durch den technischen Fortschritt bei Systemen mit künstlicher Intelligenz verursachten **Haftungslücken** füllen.

Die Einführung, Verbreitung und Weiterentwicklung von KI-Systemen soll in der Europäischen Union gefördert werden, indem rechtliche Fragmentierung vermieden wird, da bei unionsweit einheitlichen Haftungsvorschriften Unternehmen ihr Haftungsrisiko besser bewerten und versichern können.



Haftung von Anbietenden von KI-Generatoren

Anwendungsbereich (Artikel 1)

Die Richtlinie gälte für nichtvertragliche Ansprüche auf Ersatz von Schäden, die durch ein KI-System verursacht wurden, wenn solche Ansprüche im Rahmen nationaler verschuldensabhängiger Haftungsregelungen geltend gemacht werden. **Unberührt** bleiben laut dem Vorschlag aber die Bereiche öffentlicher Verkehr, das **Produkthaftungsrecht**, die **Haftungsfreistellungen gemäß dem Gesetz über digitale Märkte (Digital Markets Act)** und Regelungen zur strafrechtlichen Verantwortlichkeit.



Haftung von Anbietenden von KI-Generatoren

Begriffsbestimmungen (Artikel 2)

Die Begriffsbestimmungen folgen denjenigen des von der Kommission präsentierten Entwurfs der KI-VO, um Kohärenz zu gewährleisten. Daneben werden weitere, für die Anwendung der Richtlinie wichtige Begriffe definiert, wie „Anspruchsteller“ und „potenzieller Anspruchsteller“



Haftung von Anbietenden von KI-Generatoren

Offenlegung von Beweismitteln und widerlegbare Vermutung eines Verstoßes (Artikel 3)

Der Zugang zu Beweismitteln über KI-Systeme, die eventuell an einem Schadensereignis mitgewirkt haben, sind für den potentiell Geschädigten relevant hinsichtlich der **Feststellung, ob ein Anspruch auf Entschädigung besteht**, sowie zur **Begründung** eines solchen Anspruchs.

Daher soll die Richtlinie einem potentiellen Geschädigten ermöglichen, die **Offenbarung von relevanten Beweismitteln vorgerichtlich geltend zu machen oder gerichtlich anordnen** zu lassen. Ebenso können **Maßnahmen zur Sicherung der Beweismittel** beantragt werden. Voraussetzung ist aber, wenn noch keine Klage anhängig ist, dass der potenzielle Anspruchsteller erfolglos um die Herausgabe der Informationen gebeten hat und ausreichend Tatsachen und Beweise vorlegt, um die Plausibilität eines Schadensersatzanspruchs zu belegen.



Haftung von Anbietenden von KI-Generatoren

Offenlegung von Beweismitteln und widerlegbare Vermutung eines Verstoßes (Artikel 3)

Die Beweismittel bezüglich derer der Offenbarungsanspruch besteht sind nicht abschließend aufgezählt. Dazu zählen dürften in der Regel aber **Datensätze, die zur Entwicklung des KI-Systems verwendet** wurden, **technische Unterlagen, Protokolle**, das **Qualitätsmanagementsystem** und alle **Korrekturmaßnahmen**.

Adressat der Offenbarungspflicht sind Anbieter oder ihnen gleichgestellte Händler, Einführer, Nutzer oder sonstige Dritte von Hochrisiko KI-Systemen (zu letztgenannten Gruppe gehören alle, die die KI unter eigenem Namen, nach einer Zweckänderung oder einer Änderung an der KI verwenden) sowie Nutzer, die derartige Systeme verwenden.



Haftung von Anbietenden von KI-Generatoren

Offenlegung von Beweismitteln und widerlegbare Vermutung eines Verstoßes (Artikel 3)

Die Offenbarungspflicht ist dahingehend **begrenzt**, dass sie erforderlich und verhältnismäßig für den Schadensersatzanspruch ist.

Eine Nichteinhaltung der Offenbarungsanordnung führt im Rahmen einer Klage zu der **widerleglichen Vermutung derjenigen Sorgfaltspflichtverletzung**, die die angeforderten Beweise für den betreffenden Schadensersatzanspruch belegen sollte.

Weiter soll sich im Zusammenhang mit einem Schadensersatzanspruch die **Offenbarungspflicht grundsätzlich auf den Beklagten** beschränken; es sei denn, der Kläger hat die Beweismittel trotz angemessener Anstrengungen von diesem nicht erlangen können.



Haftung von Anbietenden von KI-Generatoren

Widerlegbare Vermutung eines ursächlichen Zusammenhangs im Fall eines Verschuldens (Artikel 4)

Ziel der Richtlinie ist es, Geschädigte von Kausalitätsfragen bei der Geltendmachung von Schadensersatzansprüchen insbesondere im Zusammenhang mit der Nichteinhaltung der KI-VO zu entlasten. Unter bestimmten Voraussetzungen bestünde daher eine **widerlegliche Vermutung**, dass ein **ursächlicher Zusammenhang – die Kausalität** – zwischen einem **Verschulden** bezüglich der Nichteinhaltung einer Pflicht nach der KI-VO und dem durch das KI-Ergebnis herbeigeführten **Schaden** besteht. Diese Vermutung ist für den Anspruchsteller deshalb so wichtig, da der Beweis des Kausalzusammenhangs oft nur durch ein „Nachvollziehen“ der „Entscheidung“ der KI geführt werden könnte und – wenn dies nicht möglich ist – der fehlende Beweis der Kausalität zu Lasten des Geschädigten ginge.



Haftung von Anbietenden von KI-Generatoren

Widerlegbare Vermutung eines ursächlichen Zusammenhangs im Fall eines Verschuldens (Artikel 4)

Der Richtlinienentwurf zählt in Artikel 4 Abs. 1 **sieben Varianten der Vermutungsregeln** für die Gerichte auf, auf deren Aufzählung wir hier aus Zeitgründen verzichten...



USA

Entwurf für eine "Bill of Rights" (Oktober 2022)

Die US-Regierung will Künstliche Intelligenz (KI) ebenfalls vertrauenswürdig machen. Das Büro für Wissenschafts- und Technologiepolitik des Weißen Hauses hat dazu im Oktober 2022 einen Entwurf für eine "Bill of Rights" für das KI-Zeitalter veröffentlicht. Die Grundrechtecharta stellt **fünf Grundsätze** auf, die die Entwicklung, die Nutzung und den Einsatz automatisierter Systeme leiten sollen. Ziel ist es, die Öffentlichkeit vor negativen Auswirkungen von KI-Systemen zu bewahren und Risiken der Schlüsseltechnik von vornherein zu entschärfen.

USA



Entwurf für eine "Bill of Rights" (Oktober 2022)

Die Prinzipien besagen, dass algorithmische Systeme nachweislich sicher und effektiv sein müssen und keine "ungerechtfertigte" Diskriminierung verursachen dürfen. Datenschutz soll direkt in die Technik eingebaut werden (Privacy by Design), auch von Datensparsamkeit ist die Rede.

Betroffenen soll die Kontrolle über ihre personenbezogenen Informationen gegeben werden: Sie sollten wissen, dass ein automatisiertes System verwendet wird und verstehen, wie und warum es zu welchen Ergebnissen beiträgt. Entwickler und Hersteller müssten dafür aussagekräftige Hinweise und Erklärungen in einfacher Sprache bereitstellen.



Datenschutz

Keine «neuen» Regeln (s. Workshoptitel), sondern bestehendes Recht!

Trotzdem ein paar Anwendungshinweise...





Datenschutz

KI-VO und die DSGVO

KI arbeitet in vielen Fällen mit enormen Datenmengen. Deshalb sind bei der Entwicklung, aber auch im Umgang mit KI-Systemen häufig datenschutzrechtliche Anforderungen zu beachten. Insbesondere im Rahmen des maschinellen Lernens (Machine Learning) werden KI-Algorithmen mit einer Vielzahl an Datensätzen trainiert. Beim Machine Learning lernt die Software autonom, indem sie auf Basis der Korrelation von alten und neuen Datenmustern, Arbeitsergebnisse produziert. Je nach Input und Anwendungsfeld kommt es dabei auch zur **Verarbeitung von personenbezogenen Daten**.

In diesen Fällen sind daher die zahlreichen **Vorgaben aus der DSGVO einzuhalten**.



Datenschutz

KI-VO und die DSGVO

Die KI-VO wird ebenfalls datenschutzrechtliche Regelungen enthalten.

Die Ziele des Datenschutzes werden jedoch nicht den Fokus der Verordnung darstellen. Vielmehr soll **bestehendes Datenschutzrecht von der Verordnung unberührt** bleiben und durch diese **ergänzt** werden. Bei der Entwicklung und Nutzung von KI wird es also zu vielen Wechselwirkungen und gegebenenfalls zu „Doppelverpflichtungen“ aus den beiden Verordnungen kommen. Die beiden Regelungsmaterien liegen inhaltlich nah beieinander, zudem ähnelt sich die Natur der Verpflichtungen und Regelungsansätze aus KI-VO-E und DSGVO an vielen Stellen.



Datenschutz

DFN-Infobrief „Recht“ März 2023, Zitat:

„Die Datenschutz-Grundverordnung (DSGVO) hat ebenfalls erhebliche Auswirkungen auf den Einsatz von KI-Software. Sie legt strenge **Regeln für die Erhebung, Speicherung und Verwendung personenbezogener Daten** fest und gilt für **jede Person oder Einrichtung, die personenbezogene Daten von EU-Bürgern verarbeitet**.

Eine der wichtigsten Auswirkungen der DSGVO besteht darin, dass **Verantwortliche transparent darlegen müssen, wie sie personenbezogene Daten erheben und verwenden und dass sie gegebenenfalls die ausdrückliche Zustimmung von betroffenen Personen für die Verarbeitung ihrer Daten einholen müssen**. Im Falle von KI-Software bedeutet dies, dass Unternehmen erklären müssen, **wie und zu welchem Zweck die personenbezogenen Daten bei dieser Software verwendet** werden und **falls erforderlich die Zustimmung einholen**.“



Datenschutz

DFN-Infobrief „Recht“ März 2023, Zitat:

„Die DSGVO verlangt darüber hinaus, dass **Verantwortliche sicherstellen, dass die von ihnen erhobenen personenbezogenen Daten richtig und aktuell sind** und dass sie gelöscht oder anonymisiert werden, wenn sie nicht mehr benötigt werden. **Für KI-Software bedeutet dies, dass die Daten, die zum Trainieren von Modellen verwendet werden, regelmäßig überprüft und aktualisiert werden müssen und dass die Software keine personenbezogenen Daten länger aufbewahrt, als sie benötigt werden.**

Schließlich ist das **Recht auf nicht automatisierte Entscheidung (Art. 22 DSGVO)** ein wichtiger Aspekt, das der betroffenen Person das Recht einräumt, **keiner Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruht, wenn diese rechtliche Folgen für sie hat oder sie in ähnlicher Weise erheblich beeinträchtigt.**“



Datenschutz

Garante per la protezione dei dati personali – Italienische Datenschutzbehörde (GPDP)

Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori...

Künstliche Intelligenz: Die **italienische Datenschutzbehörde blockierte ChatGPT im März 2023**. Illegale Erhebung personenbezogener Daten. Fehlen von Systemen zur Überprüfung des Alters von Minderjährigen...

Seit Ende April 2023 darf ChatGPT in Italien wieder genutzt werden, nachdem OpenAI Änderungen vorgenommen hat, um mehr Transparenz und Nutzerrechte zu gewährleisten.



Datenschutz

Garante per la protezione dei dati personali – Italienische Datenschutzbehörde

Die Entscheidung der GPDP, die Anwendung ChatGPT zu sperren, wurde nur acht Wochen nach der Sperrung von „Replika“, am 30.03.2023, verkündet (GPDP vom 30.03.2023). Nach dem seit November 2022 anhaltenden Hype um die KI-gestützte Chat-Anwendung erfuhr die Nachricht eine große Medienaufmerksamkeit. Zwar hatte die GPDP zuvor schon die App Replika in die Schranken gewiesen, jedoch war ChatGPT weitaus bekannter, sodass die Entscheidung europaweit für viel Aufsehen sorgte (vgl. tagesschau.de vom 31.03.2023; BBC vom 01.04.2023).

In der Begründung der Maßnahme nach Art. 58 Abs. 2 lit. f DS-GVO bemängelte die italienische Datenschutzbehörde, dass **keine wirksame Grundlage für die Datenverarbeitung** vorliege und **keine geeigneten Mechanismen zum Schutz Minderjähriger vorhanden** seien.



Datenschutz

Garante per la protezione dei dati personali – Italienische Datenschutzbehörde

Bemängelt wurde vor allem die **fehlende Rechtsgrundlage für die Datenverarbeitung**. So sei nicht erkennbar, wie OpenAI **die massenhafte Verarbeitung von personenbezogenen Daten italienischer Nutzer** rechtfertige. Dadurch werde die **Informationspflicht der betroffenen Personen (Art. 13 Abs. 1 lit. c DS-GVO) verletzt**. Außerdem sei festgestellt worden, dass **zahlreiche personenbezogene Daten unzutreffend** waren. Ähnlich wie im Fall „Replika“ **monierte** die GPDP zudem den **Minderjährigenschutz**. So gebe es bei ChatGPT **keine Altersüberprüfung, die verifiziere**, dass die Nutzenden mindestens 13 Jahre alt seien. Dies führe dazu, dass nicht altersgerechte Antworten von dem Chatbot ausgegeben würden (GPDP vom 30.03.2023).



Datenschutz

Garante per la protezione dei dati personali – Italienische Datenschutzbehörde

Binnen einer Woche wurde ein Treffen zwischen ranghohen Mitarbeitenden von OpenAI und der GPDP vereinbart. Dabei wurden die Datenschutzverstöße thematisiert, die in einem Forderungskatalog der GPDP mündeten, den die Behörde am 11.04.2023 veröffentlichte. Darin stellte die Behörde dem US-Unternehmen konkrete Fristen für die Erfüllung der geforderten Maßnahmen. Sollte OpenAI den Hauptforderungen bis zum 30.04.2023 nachkommen, würde die **Sperre der Chat-Anwendung in Italien aufgehoben** werden (GPDP vom 11.04.2023).



Datenschutz

Garante per la protezione dei dati personali – Italienische Datenschutzbehörde

Forderungskatalog GPDP vom 11.04.2023:

Konkret umfasst der Katalog neun Forderungen, von denen die ersten sieben zum 30.04.2023 fällig waren, während die letzten beiden Forderungen spätere Fristen enthalten (GPDP vom 11.04.2023):

1. OpenAI informiert auf ihrer Website über die Grundlage der Datenverarbeitung und die Rechte der betroffenen Personen (gut sichtbar und vor der Registrierung).
 2. OpenAI stellt ein Tool zur Geltendmachung der Betroffenenrechte auf der Website zur Verfügung, womit u. a. der Datenverarbeitung für Trainingszwecke widersprochen werden kann.
-



Datenschutz

Garante per la protezione dei dati personali – Italienische Datenschutzbehörde

3. OpenAI stellt ein Tool zur Richtigstellung von unrichtigen personenbezogenen Daten auf der Website zur Verfügung, notfalls auch zur Datenlöschung.
 4. OpenAI fügt im Registrierungsprozess für ChatGPT oder bei Wiederanmeldung einen Link zu den Nutzungsbedingungen ein, der zwingend von den Registrierenden gesehen werden muss.
 5. OpenAI ändert die Rechtsgrundlage für die Verarbeitung zu Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO) oder berechnete Interessen (Art. 6 Abs. 1 lit. f DS-GVO) und entfernt jegliche Erwähnung der vertraglichen Rechtsgrundlage (Art. 6 Abs. 1 lit. b DS-GVO).
 6. OpenAI stellt ein Tool zur Verfügung, mit dem Nutzende der Verarbeitung ihrer personenbezogenen Daten widersprechen können, wenn die Rechtsgrundlage Art. 6 Abs. 1 lit. f DS-GVO ist.
-



Datenschutz

Garante per la protezione dei dati personali – Italienische Datenschutzbehörde

7. OpenAI fügt eine Altersabfrage in den Registrierungs- und Anmeldeprozess ein, der auf der Eingabe der Nutzenden beruht.

8. OpenAI legt einen Plan für eine qualifizierte Altersüberprüfung vor, durch die Minderjährige unter 13 Jahren gar keinen Zugang und Minderjährige zwischen 13 und 18 Jahren nur mit Einwilligung der gesetzlichen Vertreter Zugang zu ChatGPT erlangen. Dieser Plan soll bis zum 31.05.2023 vorgelegt werden und spätestens ab 30.09.2023 umgesetzt werden.

9. OpenAI startet eine nicht werbliche Informationskampagne in allen italienischen Massenmedien (Radio, Fernsehen, Presse, Internet) bis 15.05.2023. Der Inhalt wird mit der GPDP abgestimmt und informiert darüber, dass personenbezogene Daten von italienischen Bürgerinnen und Bürgern wahrscheinlich verarbeitet wurden und dass weitere Informationen auf der Webseite zum Abruf bereitstehen.



Datenschutz

Garante per la protezione dei dati personali – Italienische Datenschutzbehörde

9. Zudem soll darauf hingewiesen werden, dass auf der Webseite ein Tool zur Verfügung steht, mit dem die betroffenen Personen die Datenlöschung ihrer personenbezogenen Daten veranlassen können.

Mit Mitteilung vom **28.04.2023** hat die GPDP verkündet, dass die **Untersagung für die Bereitstellung von ChatGPT in Italien aufgehoben** wird. OpenAI habe in einem Schreiben an die Behörde erklärt, dass sie die **geforderten Maßnahmen umgesetzt** habe und einen **ausreichenden Schutz der personenbezogenen Daten gewährleisten** könne (GPDP vom 28.04.2023). In dem Brief erwähnt OpenAI auch, dass sie zwar ein Tool zur Datenlöschung eingerichtet hat, allerdings sei es **nach derzeitigem technischen Stand nicht möglich, Datenberichtigungen** vorzunehmen (GPDP vom 28.04.2023).



Datenschutz

Garante per la protezione dei dati personali – Italienische Datenschutzbehörde

Thöne: „Italien - Datenschutzbehörde hebt ChatGPT-Sperre auf“, ZD-Aktuell 2023, 01254:

„Besonders hervorzuheben ist die Forderung nach der Änderung der Rechtsgrundlage. Die GPDP ordnete an, dass ein **vermeintlich geschlossener Vertrag als Rechtsgrundlage vor dem Hintergrund der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO nicht genüge** und deshalb jegliche Erwähnung zu entfernen sei. In Betracht komme lediglich eine **Einwilligung (deren Informiertheit zuvor nicht gegeben war)** oder die **Verarbeitung auf Grund berechtigter Interessen**. Hiermit setzt die GPDP ein klares Zeichen und mahnt Digitalunternehmen zur Einhaltung der Grundsätze der DS-GVO. Das **gekünstelte Vertragskonstrukt**, nach dem die Nutzenden unbewusst mit OpenAI einen Nutzungsvertrag schließen, deren Gegenleistung in der Bereitstellung von personenbezogenen Daten bestehe, **entspreche nicht dem, was die Nutzenden erklären**. Einen **Nachweis über einen Vertragsschluss** nach italienischem (und auch deutschem) Zivilrecht **kann OpenAI somit nicht erbringen.**“



Datenschutz

Spanische Datenschutzbehörde

Auch Spaniens Datenschutzbehörde sagt, dass sie ChatGPT untersucht...



Datenschutz

Deutschland...

Der Digitalausschuss des Bundestags hat in einer öffentlichen Sitzung am Mittwoch, 29.03.2023, über den Stand der Verhandlungen zur gesetzlichen Regulierung von generativer Künstlicher Intelligenz (KI) auf EU-Ebene debattiert...

<https://www.bundestag.de/dokumente/textarchiv/2023/kw13-pa-digitales-ki-938580>



Datenschutz

BaWü: LfDI informiert sich bei OpenAI, wie ChatGPT datenschutzrechtlich funktioniert

LfDI fordert ChatGPT-Betreiber **OpenAI zur Stellungnahme** auf.

LfDI wirkt im Europäischen Datenschutz-Ausschuss auf **einheitliches europäisches Vorgehen** hin.

Hintergrund lt. Pressemitteilung LfDI v. 24.04.2023: „Anwendungen müssen auf Grundlage unseres europäischen Rechtsrahmens und unserer europäischen Werte erfolgen. Wir sprechen nun mit dem Betreiber von ChatGPT, danach nehmen wir eine Bewertung vor. Bürgerinnen müssen dem technischen Fortschritt vertrauen können. Das wird nur möglich, wenn eingesetzte Techniken die Bürgerrechte auch im Digitalen wahren.“



Datenschutz

BaWü: LfDI informiert sich bei OpenAI, wie ChatGPT datenschutzrechtlich funktioniert

Nach der Datenschutz-Grundverordnung muss ein Anbieter von Leistungen, bei denen personenbezogene Daten verarbeitet werden, unter anderem **erklären können, welche Daten wie und zu welchem Zweck verarbeitet** werden.

Auch muss er **angemessene technische und organisatorische Maßnahmen** treffen, um diese **personenbezogenen Daten zu sichern** und dabei **besondere Regelungen treffen, wenn er sensible Daten verarbeiten** will – wie etwa **Informationen zu Gesundheitszustand, zur sexuellen Identität, zur Weltanschauung oder zur familiären und auch finanziellen Situation**.

Zudem muss der Anbieter die **Rechte von Betroffenen** wahren, wie etwa das **Recht auf Berichtigung oder Auskunft**.



Datenschutz

BaWü: LfDI informiert sich bei OpenAI, wie ChatGPT datenschutzrechtlich funktioniert

Der Landesbeauftragte lässt sich nun in einem **datenschutzrechtlichen Aufsichtsverfahren die Verarbeitung von personenbezogenen Daten im Rahmen von ChatGPT erklären**. Die Aufsichtsbehörden der Länder haben die Fragen, die an OpenAI gerichtet sind, miteinander abgestimmt. Zugleich wirkt der Landesbeauftragte auf europäischer Ebene auf ein einheitliches Vorgehen bei der Betrachtung von ChatGPT hin und beteiligt sich dafür intensiv an einer entsprechenden Arbeitsgruppe des Europäischen Datenschutz-Ausschusses.

Die **Zuständigkeit des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg**, auf die Firma OpenAI mit Sitz in San Francisco zuzugehen, ergibt sich aufgrund von Artikel 55 Absatz 1 DS-GVO in Verbindung mit § 40 BDSG, soweit eine Niederlassung in Europa nicht benannt ist.



Datenschutz

BaWü: LfdI informiert sich bei OpenAI, wie ChatGPT datenschutzrechtlich funktioniert

In seinem Tätigkeitsbericht hat der Landesbeauftragte über Künstliche Intelligenz ausführlich berichtet (Kap. 1.5., Seite 23 ff): https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2023/02/TB_38_Datenschutz-2022_V1-.pdf

Pressemitteilung vom 24.04.2023

<https://www.baden-wuerttemberg.datenschutz.de/lfdi-informiert-sich-bei-openai-wie-chatgpt-datenschutzrechtlich-funktioniert/>



Datenschutz

BaWü: LfDI informiert sich bei OpenAI, wie ChatGPT datenschutzrechtlich funktioniert

Weitere Ergebnisse der Prüfung sind (hier) bisher nicht bekannt...



Datenschutz

KI & Datenschutz – Checkliste für den Einsatz künstlicher Intelligenz

[Dr. Thomas Schwenke vom 06.04.2023](#)



Datenschutz

Verarbeitung personenbezogener Daten und DSGVO-Relevanz

Datenschutzrechtlich ist der Einsatz von KI relevant, wenn dabei personenbezogene Daten verarbeitet werden. Darunter fallen Daten, die es ermöglichen, eine lebende Person zu identifizieren (Art. 4 DSGVO), wie Namen, Adressen und Telefonnummern, aber auch alle mit diesen Daten verbundenen Informationen (z.B. Schriftstücke)..

Keine DSGVO-Relevanz, da kein Personenbezug: Generierung von Code, Bildern oder Marketingtexten.

DSGVO-Relevanz, da Personenbezug: Einspeisen von Schriftstücken mit Angaben zu Personen, Hochladen von Bildern fremder Personen als Vorlage, KI über eine Schnittstelle mit einem E-Mail-Programm verbinden oder Datensätze mit Nutzer- oder Kundendaten auswerten, Nutzung durch Mitarbeiter mit personenbezogenen Accountdaten (z.B. max.mueller@unternehmen-xyz.de).



Datenschutz

Verarbeitung personenbezogener Daten und DSGVO-Relevanz

Im Ergebnis ist es sinnvoll, **Daten vor dem Einsatz im Rahmen der KI zu anonymisieren**. Dieser Grundsatz der Datenminimierung gilt generell, insbesondere wenn die DSGVO zur Anwendung kommt.

Privatpersonen: Die DSGVO ist nicht anwendbar, wenn die Verarbeitung nur persönlicher und familiärer Natur ist. Diese Grenze ist jedoch überschritten, wenn fremde personenbezogene Daten im Internet veröffentlicht werden. Die Verbreitung von Bildaufnahmen von Personen außerhalb des persönlichen Bereichs ist grundsätzlich untersagt. Ob die KI eher einem Cloud-Dienst gleichkommt, der der Privatsphäre zugeordnet wird, oder eher einem öffentlichen Facebook-Profil, ist unklar und kann beidseitig argumentiert werden. Bei Eingaben von Personennamen oder ähnlichen Einzeldaten sind hier eher keine Probleme zu erwarten. Wer jedoch Bilder fremder Personen hochlädt, sollte ~~diese Personen zur Sicherheit vorab um Erlaubnis fragen.~~



Datenschutz

Zulässigkeit und Rechtsgrundlage des Einsatzes der KI

Ein explizites KI-Verbot existiert zwar (noch) nicht. Aber die DSGVO ist so aufgebaut, dass **jede Verarbeitung von personenbezogenen Daten zuerst verboten und gesondert gerechtfertigt** werden muss.

Die DSGVO **erlaubt die Verarbeitung in den folgenden Fällen:**

Erforderlich zur **Erfüllung von Vertragspflichten**: Diese Rechtsgrundlage kommt vor allem dann zur Anwendung, wenn die KI als Arbeitsmittel eingesetzt wird (Art. 6 Abs. 1 lit. b) DSGVO). Beispielsweise, wenn eine Agentur ihren Kunden den Einsatz von KI als Arbeitsmittel anpreist, ist es eindeutig erforderlich, diese KI einzusetzen. Aber je stärker die KI in den Alltag integriert wird, desto eher kann sie als erforderlich angesehen werden.



Datenschutz

Zulässigkeit und Rechtsgrundlage des Einsatzes der KI

Berechtigte Interessen: Praktisch alle nicht verbotenen Interessen sind erlaubt, so insbesondere betriebswirtschaftliche Interessen (Art. 6 Abs. 1 lit. f) DSGVO). Allerdings dürfen die Schutzinteressen der betroffenen Personen nicht überwiegen. Hier besteht ein Problem darin, dass bei vielen Diensten unklar ist, wie sie Daten verarbeiten (sog. "Blackbox"-Problem). Sie sind aber nachweispflichtig sind, dass die Verarbeitung datenschutzkonform erfolgt.

Einwilligung: Die Einwilligung ist eine Ausweichnorm, die dann in Frage kommt, wenn sonst keine Erlaubnis greift (Art. 6 Abs. 1 lit. a) DSGVO). Sie hat den Nachteil, dass sie jederzeit widerrufen werden kann und z.B. bei Minderjährigen erst ab einem bestimmten Alter anwendbar ist (z.B. Deutschland ab 16 Jahren, Österreich ab 14 Jahren). Ferner ist eine Einwilligung nur dann wirksam, wenn die betroffene Person hinreichend über die Verarbeitungsprozesse und Risiken informiert wurde, was einen gewissen Erläuterungsaufwand erfordert.



Datenschutz

Privacy by Design

Der in Art. 25 DSGVO als “**Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**” bezeichnete Grundsatz verlangt, dass Sie sich vor dem Einsatz von KI-Software folgende Überlegungen machen:

Warum eine KI-Software eingesetzt werden muss: Bevor Verantwortliche personenbezogene Daten einer KI übermitteln, sollten diese **begründen, warum der geplante Zweck der KI-Nutzung nicht auf anderen datenschutzfreundlicheren Wegen erreicht** werden könnte.

Warum es diese eine KI-Software sein muss: Bevor Verantwortliche sich für ein System entscheiden, sollten diese **prüfen, ob es datenschutzfreundlichere Alternativen** gibt (andere Anbieter, Einsatz von KI auf eigenem Server, etc.).



Datenschutz

Grundsätzliches Verbot automatisierter Entscheidungen im Einzelfall

Die DSGVO **verbietet –grundsätzlich- automatische Entscheidungen, von denen der Abschluss von Verträgen oder sonstige erhebliche Entscheidungen abhängen** (Art. 22 DSGVO). Typische Beispiele sind z.B. eine automatische Bonitätsprüfung mit folgendem Ausschluss von Kunden im Hinblick auf z.B. den Rechnungskauf oder **automatische Bewerberauswahl**.

In solchen Fällen wird daher eine **Einwilligung der betroffenen Personen, strenge Erforderlichkeit oder eine menschliche Endprüfung der maschinellen Entscheidung** notwendig.

In jedem Fall müssen die betroffenen Personen darüber **informiert** werden, wenn sie von automatisierten Entscheidungen im Einzelfall betroffen sind.



Datenschutz

Verantwortlichkeit und Auftragsverarbeitung beim Einsatz von KI

Ein wesentlicher Aspekt der DSGVO ist die Feststellung der datenschutzrechtlichen **Verantwortlichkeit für die Verarbeitungsprozesse**. Danach bestimmt sich z.B. welche Arten von Verträgen geschlossen werden müssen und wer für etwaige Rechtsverstöße haftet. Als mögliche Konstellationen kommen in Frage:

Alleinverantwortung: KI-Anbieter ist alleine für die Verarbeitung im KI-System verantwortlich. Sie sind nur für die Eingabe verantwortlich.

Auftragsverarbeitung: KI-Anbieter ist Ihr weisungsgebundener Auftragsverarbeiter und Sie sind für die Verarbeitungsprozesse bei dem Anbieter verantwortlich.

Gemeinsame Verantwortlichkeit: KI-Anbieter und Sie sind gemeinsam verantwortlich, weil Sie die Daten zuführen und wie der Anbieter ein Interesse an dem Verbessern der KI haben



Datenschutz

Verantwortlichkeit und Auftragsverarbeitung beim Einsatz von KI

Welche dieser **Konstellationen zutrifft, ist derzeit nicht klar** und wird von der Art des verwendeten Systems und dessen Einsatzes abhängen.

OpenAI, der Anbieter von ChatGPT, sieht sich z.B. als Auftragsverarbeiter im Hinblick auf die Nutzung via Schnittstelle (API) und stellt einen entsprechenden Auftragsverarbeitungsvertrag zur Verfügung. Ob diese Einschätzung zutreffend ist, kann derzeit nicht gesagt werden, aber immerhin ist so die Nutzung der API ein Stück "rechtssicherer".

Information der Auftraggeber: Wenn Unternehmen personenbezogene Daten im Auftrag von Kunden verarbeiten und dabei eine KI einsetzen wollen, dann müssen die Unternehmen dies den Kunden mitteilen. Je nach Vereinbarung im Auftragsverarbeitungsvertrag kann eine Genehmigung der Kunden erforderlich sein.



Datenschutz

EU-US-Datentransfers

Mit der datenschutzrechtlichen Verantwortlichkeit geht auch die Verantwortung für Datenübertragungen außerhalb der EU, bei KI-Diensten vornehmlich in die USA, einher (Art. 44 DSGVO).

Wenn personenbezogene Daten außerhalb der EU, z.B. in den USA, verarbeitet werden, müssen die Verarbeitenden als datenschutzrechtlich Verantwortlicher auch die Zulässigkeit dieser Datenübertragungen prüfen. Zum Beispiel sollte man die Anbietenden fragen, ob sie sogenannte Standardvertragsklauseln bereitstellen können.

Zum sog. „**EU/US-Data Privacy Framework**“ s. oben...



Datenschutz

Auskunfts- und Löschungsrechte

Mit der datenschutzrechtlichen Verantwortlichkeit geht auch die Verpflichtung zur Erfüllung der Rechte betroffener Personen einher (§ 15 bis 21 DSGVO). Das heißt, die Verantwortlichen sollten auf Anfragen dieser Art vorbereitet sein:

“Bitte teilen Sie mir mit, welche personenbezogenen Daten von mir Sie im Rahmen von KI-Verfahren verarbeiten, übermitteln mir eine Kopie dieser Daten und löschen diese anschließend, da ich deren Verarbeitung widerspreche.”

Diese Anfrage müssen die Verantwortlichen immer, auch wenn negativ, unverzüglich beantworten. Wenn ein Fall der Auftragsverarbeitung oder gemeinsamer Verantwortlichkeit vorliegt und tatsächlich personenbezogene Daten in die KI eingespeist wurden, dann könnte die Auskunft problematisch werden. Umso mehr hilft es, wenn die Verantwortlichen darauf verweisen können, dass personenbezogene Daten gelöscht werden.



Datenschutz

Auskunfts- und Löschungsrechte

Zwar bietet z.B. OpenAI ein Opt-Out-Formular an. Ob und in welchem Umfang es effektiv ist, kann hier nicht verifiziert werden.



Datenschutz

Datenschutz-Folgenabschätzung

Im Fall besonders risikobehafteter Verarbeitungen, was vor allem beim Einsatz neuer Technologien, Verarbeitung von personenbezogenen Daten im großen Umfang oder besonderer Kategorien von Daten (z.B. Gesundheitsdaten) der Fall ist, muss eine sogenannte Datenschutz-Folgenabschätzung durchgeführt werden (Art. 35 DSGVO).

Das bedeutet, die Verantwortlichen müssen zuerst prüfen, ob eine solche Risikosituation vorliegt und falls ja, die entsprechende Datenschutz-Folgenabschätzung durchführen.



Datenschutz

Rechenschaftspflichten

Bei allen Prüfungspunkten sollten die Verantwortlichen immer davon ausgehen, dass die Beweislast für den rechtmäßigen Einsatz bei ihnen liegt. Das bedeutet, dass die Verantwortlichen die Voraussetzungen der zulässigen Nutzung nachweisen müssen

In der Praxis bedeutet dies, dass die Verantwortlichen alle Aspekte der Nutzung, angefangen bei der Prüfung der Zulässigkeit, protokollieren sollten.



Datenschutz

Verzeichnis von Verarbeitungstätigkeiten

Das Datenschutzmanagement erfordert ein internes Verzeichnis von Verarbeitungsprozessen (Art. 30 DSGVO).

In diesem Verzeichnis muss auch der Einsatz der KI und der eingesetzten Anbieter unter Nennung der Zwecke, der Rechtsgrundlagen und der verarbeiteten Daten eingetragen werden.



Datenschutz

Datenschutzhinweise

Im Rahmen des Datenschutz-Generators hat Dr. Thomas Schwenke die bekanntesten Diensteanbieter von KI und Tools, wie z.B. OpenAI, Chat-GPT oder Midjourney als Module aufgenommen. D.h. die Nutzenden dieses Tools können ihre Datenschutzhinweise oder Auftragsverarbeitungsverträge (dort OpenAI als Subunternehmer) entsprechend ergänzen.

Das zum internen Verzeichnis von Verarbeitungstätigkeiten gesagte gilt auch für die Datenschutzhinweise. Setzen Verantwortliche z.B. im Rahmen des Supports ChatGPT ein, dann sollten diese die Angaben zur Verarbeitung von Kundendaten im Rahmen des Service um Angaben zu dem Diensteanbieter OpenAI als Datenempfänger aufnehmen.



Datenschutz

Setzen Sie Chatbots oder Chatfunktionen zu Kommunikationszwecken ein?

(Erläuterungen anzeigen)

ja

nein

Bitte wählen Sie die eingesetzten Anbieter aus:

ChatGPT



OpenAI (Nutzung via
API)



Bing KI



Intercom





Datenschutz

Geschäftsgeheimnisse

Beim Einsatz von KI sollten die Nutzenden auch die eigenen und fremden Geschäftsgeheimnisse beachten, und zwar unabhängig von Problemen bei der Nachweisfragen eines möglichen Verstoßes.

Eigene Geschäftsgeheimnisse: Wenn Nutzende z.B. eigene Geschäftsgeheimnisse gegenüber der KI preisgeben (s. dazu einen Vorfall bei Samsung) und sie so anderen zugänglich werden, verlieren Sie den Geschäftsgeheimnisschutz mangels angemessener Schutzmaßnahmen, s. § 2 Nr. 1 b) GeschGehG.

Fremde Geschäftsgeheimnisse: Wenn Nutzende wiederum fremde Geschäftsgeheimnisse, z.B. im Rahmen der Auswertung der Geschäftskorrespondenz preisgeben, dann liegt ein Verstoß gegen vertragliche Schutzpflichten und u.U. gegen ein mit einer Vertragsstrafe bewehrtes NDA vor.



Datenschutz

DSGVO-Checkliste für den Einsatz von KI in Hochschulen

- Verarbeitung personenbezogener Daten und DSGVO-Relevanz
 - Zulässigkeit und Rechtsgrundlage für den Einsatz von KI
 - Privacy by Design
 - Verbot automatisierter Entscheidungen im Einzelfall
 - Verantwortlichkeit und Auftragsverarbeitung bei KI-Nutzung
 - EU-US-Datentransfers
 - Auskunfts- und Löschungsrechte
 - Datenschutz-Folgenabschätzung
-



Datenschutz

DSGVO-Checkliste für den Einsatz von KI in Hochschulen

- Rechenschaftspflichten
- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutzhinweise
- Geschäftsgeheimnisse

Quelle: Dr. Thomas Schwenke vom 06.04.2023

<https://datenschutz-generator.de/ki-datenschutz/>



Datenschutz

Online-Diskussion statt: Unter dem Titel "ChatGPT und der Datenschutz"

Auf Einladung des Instituts für Rechtsinformatik der Universität des Saarlandes findet am **Mittwoch, 12. Juli, von 18 bis 20 Uhr**, eine Online-Diskussion statt: Unter dem Titel "ChatGPT und der Datenschutz" diskutieren im Podium unter anderem der Leiter der KI-Taskforce der deutschen Datenschutzbehörden, Professor Dieter Kugelmann, der ehemalige Datenschutzbeauftragte von Baden-Württemberg, Dr. Stefan Brink, und der Rechtsanwalt und Partner der Londoner Rechtsanwaltskanzlei Ashurst LLP, Dr. Alexander Duisberg. Moderator ist der Direktor des Instituts für Rechtsinformatik, Professor Georg Borges. Interessierte sind herzlich eingeladen mitzudiskutieren. **Eine Anmeldung ist nicht erforderlich.** Unter folgendem Link ist am 12. Juli ab 18 Uhr die öffentliche Online-Live-Diskussion erreichbar: <https://www.rechtsinformatik.saarland>

oder direkt unter: <https://www.rechtsinformatik.saarland/de/aktuelles/770-gpt-dsgvo>



Persönlichkeitsrechte

DFN-Infobrief „Recht“ März 2023, Zitat:

„Auch im Bereich der Persönlichkeitsrechte wirft die Verwendung von KI Bedenken auf. Ein zentraler Diskussionspunkt ist die **Diskriminierung**. Denn KI-Systeme, die auf der Grundlage voreingenommener Daten trainiert werden, können bei ihrer Entscheidungsfindung eine Diskriminierung aufrechterhalten und sogar verstärken. Dies kann insbesondere in Bereichen wie **Beschäftigung, Wohnungswesen und Kreditvergabe** zu Problemen führen.

Fehlerhafte Trainingsdaten können außerdem dazu führen, dass ein KI-System **falsche Informationen über Personen**, z. B. einen Politiker liefert. Dies kann zu Desinformation und Misstrauen im politischen Prozess führen und möglicherweise den demokratischen Prozess beeinträchtigen.“




Datenschutz & Urheberrecht

MONEYWATCH >

ChatGPT maker OpenAI sued for allegedly using "stolen private information"

MONEY WATCH BY MEGAN CERULLO
JUNE 30, 2023 / 3:14 PM / MONEYWATCH

f t q



Industry leaders warn of AI risks
00:23

Cookies Verwalten

<https://www.cbsnews.com/news/chatgpt-open-ai-lawuit-stolen-private-information/>



Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 | F: (213) 788-4070 | clarksonlawfirm.com

1 **CLARKSON LAW FIRM, P.C.**
Ryan J. Clarkson (CA SBN 257074)
2 *rclarkson@clarksonlawfirm.com*
Yana Hart (CA SBN 306499)
3 *yhart@clarksonlawfirm.com*
Tiara Avanes (CA SBN 343928)
4 *tavanes@clarksonlawfirm.com*
Valter Malkhasyan (CA SBN 348491)
5 *vmalkhasyan@clarksonlawfirm.com*
22525 Pacific Coast Highway
6 Malibu, CA 90265
Tel: (213) 788-4050

7 **CLARKSON LAW FIRM, P.C.**
Tracey Cowan (CA SBN 250053)
8 *tcowan@clarksonlawfirm.com*
9 95 3rd St., 2nd Floor
San Francisco, CA 94103
10 Tel: (213) 788-4050

11 **CLARKSON LAW FIRM, P.C.**
Timothy K. Giordano (NY SBN 4091260)
12 *(PHV Application Forthcoming)*
tgiordano@clarksonlawfirm.com
13 590 Madison Ave., 21st Floor
New York, NY 10022pr
14 Tel: (213) 788-4050

15 *Counsel for Plaintiffs and the Proposed Classes*

16 **UNITED STATES DISTRICT COURT**
17 **NORTHERN DISTRICT OF CALIFORNIA**

18 PLAINTIFFS P.M., K.S., B.B., S.J., N.G., C.B.,
19 S.N., J.P., S.A., L.M., D.C., C.L., C.G, R.F., N.J.,
20 and R.R., individually, and on behalf of all others
similarly situated,

21 Plaintiffs,

22 vs.

23 OPENAI LP, OPENAI INCORPORATED,
OPENAI GP, LLC, OPENAI STARTUP FUND
24 I, LP, OPENAI STARTUP FUND GP I, LLC,
OPENAI STARTUP FUND MANAGEMENT
25 LLC, MICROSOFT CORPORATION and DOES
26 1 through 20, inclusive,

27 Defendants.

Case No.:

CLASS ACTION COMPLAINT

1. VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §§ 2510, *et seq.*
2. VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030
3. VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA"), CAL. PENAL CODE § 631
4. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, BUSINESS AND PROFESSIONS CODE §§ 17200, *et seq.*



Urheberrecht

Unzulässiges Machine-Learning: Klage gegen Stability AI

Das Unternehmen Stability AI sieht sich derzeit von Klagen überhäuft. Ihr KI Bildgenerator Stable Diffusion soll anhand von Daten trainiert worden sein, die urheberrechtlich geschützt sind. KI muss anhand von Datensets trainiert werden. Um also z.B. zu wissen, wie ein Apfel aussieht, muss der Bildgenerator vorher anhand von genügend Bildern von Äpfeln trainiert worden sein. Konkret für das Stable Diffusion wurde in letzter Zeit jedoch immer deutlicher, dass die dafür verwendeten Trainingsbilder nicht hätten genutzt werden dürfen. Die Plattform Getty Images bietet auf ihrem Portal sog. Stockfotos an, die gegen Abschluss eines Lizenzvertrages genutzt werden dürfen.



Urheberrecht

Unzulässiges Machine-Learning: Klage gegen Stability AI

Stability AI hat keine derartigen Vereinbarungen mit Getty Images getroffen, deren KI versucht aber ganz offensichtlich, das bekannte Wasserzeichen von Getty nachzuahmen – eine Folge des übermäßigen Trainings mit Bildern, die eben dieses Zeichen enthielten. Bereits Mitte Januar 2023 hatte Getty Images in Großbritannien Klage erhoben. Nun folgte die Klage auch in den USA. Getty Images betonte dabei jedoch deutlich, dass das Unternehmen nicht per se gegen die Verwendung der Bilder zu KI-Trainingszwecken vorgehen wolle. Es müsse lediglich eine vernünftige Vergütungsvereinbarung für die betreffenden Urheber getroffen werden. Die Bildagentur ist allerdings nicht die einzige Rechteinhaberin, die sich gegen Stabilität AI wendet. Bereits im Vorfeld hatten drei Kunstschaffende Klage gegen die KI-Entwickler erhoben.



Urheberrecht

Ralph Oliver Graef Rechtsanwalt, Managing Partner at GRAEF Rechtsanwälte

“Under German law any AI software crawling German websites et al. was legally trained due to § 44 b section 3 UrhG. **The mistake of the German legislator, if we may call it a mistake, was to make this paragraph an opt-out rather than an opt-in rule.** By the time creators and producers realized that their works were used to train the AI it was too late.

However, I expect European Parliament to address the copyright issues and I personally think that three things will happen soon: (1) **creators and producers will opt out with effect to the future** and not allow AI software to be trained with their works, (2) **platforms will not publish a book/film/game if the producer cannot guarantee that it was created without artificial intelligence** and (3) **works created with AI will have to be labeled „AI works“** just like with product placement in films and audiovisual works.

Will that stop generative AI to blow up the media markets? No. Unless the EU and the US legislators act together.”



Urheberrecht

- **1. Teil: Input & Trainingsdaten**
 - **2. Teil: Weiterverwendung des Outputs**
-



Urheberrecht

Input & Trainingsdaten

Wenn Bilder, Texte oder Programmcode lediglich **zum Training eines neuronalen Netzes verwendet** werden, ist zunächst auch nur dafür eine urheberrechtliche Erlaubnis erforderlich. Wer urheberrechtlich geschützte Bilder kopiert, braucht eine Erlaubnis. Entweder durch eine Lizenz (wie CC-lizenzierte Bilder) oder gesetzlich. Gesetzlich ist der **§ 44b UrhG** die Erlaubnis – die gerade deswegen eingeführt wurde, weil Big Data Analysen von urheberrechtlich geschützten Inhalten sonst faktisch nicht möglich sind.



Urheberrecht

Input & Trainingsdaten

These: Der eigentliche Analyseprozess im Rahmen von Data Mining ist grundsätzlich **keine urheberrechtlich relevante Handlung**, da die Information für sich genommen kein urheberrechtlicher Schutzgegenstand ist.

Entsprechendes Trainingsmaterial darf also erhoben werden, es sei denn, dass der jeweilige **Rechteinhaber seinen Vorbehalt gegen ein solches Data Mining in maschinenlesbarer Form erklärt** hat. Rechteinhaber, die ein Mining „ihrer“ Daten verhindern wollen, sollten also einen entsprechenden Vorbehalt auf den eigenen Webpräsenzen erklären.



Urheberrecht

§ 44b UrhG: Text und Data Mining

(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.

https://www.gesetze-im-internet.de/urhg/__44b.html



Urheberrecht

§ 60d Text und Data Mining für Zwecke der wissenschaftlichen Forschung

(1) Vervielfältigungen für Text und Data Mining (§ 44b Absatz 1 und 2 Satz 1) sind für Zwecke der **wissenschaftlichen Forschung** nach Maßgabe der nachfolgenden Bestimmungen zulässig.

(2) Zu Vervielfältigungen berechtigt sind **Forschungsorganisationen**. **Forschungsorganisationen sind Hochschulen, Forschungsinstitute oder sonstige Einrichtungen, die wissenschaftliche Forschung betreiben**, sofern sie

1. **nicht kommerzielle** Zwecke verfolgen,
 2. **sämtliche Gewinne in die wissenschaftliche Forschung reinvestieren** oder
 3. im **Rahmen eines staatlich anerkannten Auftrags im öffentlichen Interesse** tätig sind.
-



Urheberrecht

§ 60d Text und Data Mining für Zwecke der wissenschaftlichen Forschung

Nicht nach Satz 1 berechtigt sind **Forschungsorganisationen, die mit einem privaten Unternehmen zusammenarbeiten**, das einen bestimmenden Einfluss auf die Forschungsorganisation und einen bevorzugten Zugang zu den Ergebnissen der wissenschaftlichen Forschung hat.

(3) Zu **Vervielfältigungen** berechtigt sind ferner

1. Bibliotheken und Museen, sofern sie öffentlich zugänglich sind, sowie Archive und Einrichtungen im Bereich des Film- oder Tonerbes (**Kulturerbe-Einrichtungen**),
 2. **einzelne Forscher, sofern sie nicht kommerzielle Zwecke** verfolgen.
-



Urheberrecht

§ 60d Text und Data Mining für Zwecke der wissenschaftlichen Forschung

(4) Berechtigte nach den Absätzen 2 und 3, die nicht kommerzielle Zwecke verfolgen, **dürfen Vervielfältigungen nach Absatz 1 folgenden Personen öffentlich zugänglich machen:**

1. einem **bestimmt abgegrenzten Kreis von Personen für deren gemeinsame wissenschaftliche Forschung** sowie
2. einzelnen **Dritten zur Überprüfung der Qualität wissenschaftlicher Forschung.**

Sobald die gemeinsame wissenschaftliche Forschung oder die Überprüfung der Qualität wissenschaftlicher Forschung abgeschlossen ist, ist die öffentliche Zugänglichmachung zu beenden.



Urheberrecht

§ 60d Text und Data Mining für Zwecke der wissenschaftlichen Forschung

(5) Berechtigte nach den Absätzen 2 und 3 Nummer 1 dürfen **Vervielfältigungen nach Absatz 1 mit angemessenen Sicherheitsvorkehrungen gegen unbefugte Benutzung aufbewahren**, solange sie für Zwecke der wissenschaftlichen Forschung oder zur Überprüfung wissenschaftlicher Erkenntnisse erforderlich sind.

(6) Rechtsinhaber sind befugt, erforderliche Maßnahmen zu ergreifen, um zu verhindern, dass die Sicherheit und Integrität ihrer Netze und Datenbanken durch Vervielfältigungen nach Absatz 1 gefährdet werden.



Urheberrecht

Weiterverwendung des Outputs

Beitrag zur Online-Veranstaltung "KI-Generatoren in der Hochschul(lehr)e – Potenziale und rechtliche Implikationen von ChatGPT, DALL-E & Co." am 14. März 2023 zum Thema **„Weiterverwendung des Outputs“** von **Dr. Janine Horn** (Stiftung Innovation Hochschullehre, Souver@n & ELAN e.V.)

https://www.mmkh.de/fileadmin/veranstaltungen/netzwerk_landesinitiativen/KI-Generatoren/2023-03-14_KI-Generatoren_UrhR_Horn.pdf



Urheberrecht

Weiterverwendung des Outputs

- Urheberrechtlicher Werkschutz für KI-generierte Inhalte
- Urheberrechtlicher Leistungsschutz für KI-generierte Inhalte
- Rechte von dritten Urhebern an KI-generierten Inhalten
- Gesetzliche Nutzungserlaubnisse für Lehrende
- Einräumung von Nutzungsrechten durch Anbieter des KI-Generators
- Kennzeichnungspflicht von KI-generierten Inhalten
- Zusammenfassung



Urheberrecht

Urheberrechtlicher Werkschutz für KI-generierte Inhalte

- Werkbegriff im deutschen Urheberrecht
 - Nur persönliche geistige Schöpfung eines Menschen, §1 UrhG, §2 Abs. 2, §7 UrhG
 - Computergenerierte Werke nur, wenn Computersystem im schöpferischen Prozess wie untergeordnete Werkzeuge zur Umsetzung von menschlichen Gestaltungsspielraum genutzt werden
- Werkbegriff im EU-Recht
 - Werk muss eine eigene geistige Schöpfung seines Urhebers darstellen
 - Urheber muss tatsächlich frei hinreichende kreative Entscheidungen treffen können, EuGH, Urt. v. 29.7.2019 –C-469/17 Afghanistan Papiere



Urheberrecht

Urheberrechtlicher Werkschutz für KI-generierte Inhalte

- Werkbegriff im EU-Recht
 - Unterscheidung zwischen KI-gestützten menschlichen (schutzfähigen) Schöpfungen und KI-erzeugten (zurzeit nicht schutzfähigen) Schöpfungen, Entschließung des Europäischen Parlaments vom 20. Oktober 2020 zu den Rechten des geistigen Eigentums bei der Entwicklung von KI-Technologien (2020/2015(INI), Nr. 14
 - Das irische Urheberrecht sieht für computer-generierte Werke eine rechtliche Fiktion vor, durch die das Urheberrecht einer Person zusteht, die kein Urheber im Sinne eines persönlichen Schöpfers ist, S. 21 lit. f Copyright and Related Rights Act 2000



Urheberrecht

Urheberrechtlicher Werkschutz für KI-generierte Inhalte

- Auch nach britischem Urheberrecht sind computer-generierte Werke zu Gunsten des Arrangeurs geschützt, wenn sie allein von einem Computer geschaffen wurden, S. 9 (3) Copyright, Designs and Patent Act 1988
- US-amerikanische Urheberrecht verlangt ein Mindestmaß an Kreativität und damit eine menschliche Geistesäußerung
 - Bei KI-Generatoren, bei denen Nutzer keinen Einfluss auf die maschinelle Durchführung der Produktion des Outputs hat, erlangen die KI-generierten Inhalte keinen Urheberrechtsschutz (kein ausreichender gestalterischer Einfluss)
 - Bei KI-Generatoren, wo der Programmierer der Software und der Verfasser des Inputs nicht gezielt zusammenarbeiten, erlangt der KI-generierte Inhalt keinen Urheberrechtsschutz (kein ausreichender gestalterischer Einfluss)



Urheberrecht

§ 69a UrhG Gegenstand des Schutzes

(1) Computerprogramme im Sinne dieses Gesetzes sind Programme in jeder Gestalt, einschließlich des Entwurfsmaterials.

(2) Der gewährte Schutz gilt für alle Ausdrucksformen eines Computerprogramms. Ideen und Grundsätze, die einem Element eines Computerprogramms zugrunde liegen, einschließlich der den Schnittstellen zugrundeliegenden Ideen und Grundsätze, sind nicht geschützt.

(3) Computerprogramme werden geschützt, wenn sie individuelle Werke in dem Sinne darstellen, dass sie das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers sind. Zur Bestimmung ihrer Schutzfähigkeit sind keine anderen Kriterien, insbesondere nicht qualitative oder ästhetische, anzuwenden.



Urheberrecht

Urheberrechtlicher Leistungsschutz für KI-generierte Inhalte?

- Keine persönliche geistige Schöpfung erforderlich, sondern Investitionsschutz
- Teilweise aber menschliches Handeln beim Entstehungsprozess erforderlich, Lichtbild- und Laufbildschutz, §§72, 95 UrhG
- Rückgriff auf Leistungsschutzrechte ist lückenhaft, denn häufig fehlen Schutzvoraussetzungen
- Tonträgerhersteller §85 UrhG: Erstfixierung der Tonaufnahmen vor Auswertung, BGH, Urteil v. 20.11.2008 -I ZR 112/06 –Sampling
- Filmhersteller §94 UrhG: Erstfixierung eines zum Vertrieb geeigneten Filmträgers vor Auswertung



Urheberrecht

Urheberrechtlicher Leistungsschutz für KI-generierte Inhalte?

- Datenbankherstellerrecht, §87a UrhG: Wesentliche Investition in die Beschaffung, Überprüfung, oder Darstellung der Daten, nicht bloße Erzeugung von Daten
- Presseverlegerrecht, §87f UrhG: Periodisch erscheinende Presseveröffentlichung
- Herausgeber wissenschaftlicher Ausgaben, §70 UrhG: Ausgaben urheberrechtlich nicht geschützter Werke oder Texte, wenn sie das Ergebnis wissenschaftlich sichtender Tätigkeit darstellen



Urheberrecht

§ 87a ff. UrhG (Leistungs)Schutz von Datenbanken

(1) Datenbank im Sinne dieses Gesetzes ist eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Eine in ihrem Inhalt nach Art oder Umfang wesentlich geänderte Datenbank gilt als neue Datenbank, sofern die Änderung eine nach Art oder Umfang wesentliche Investition erfordert.

(2) Datenbankhersteller im Sinne dieses Gesetzes ist derjenige, der die Investition im Sinne des Absatzes 1 vorgenommen hat.



Urheberrecht

Persönliche These

De lege ferenda: Leistungsschutzrecht für Diensteanbietende von KI-Generatoren?

Leistungsschutzrecht für KI-Diensteanbietende, zum Beispiel a lá Leistungsschutzrecht für Presseverlage bzw. a lá Recht der Datenbankherstellenden?

Persönliche These: Eher nein, denn argumentum e contrario aus der vergütungsfreien (!) Schranke nach § 44b UrhG „Text und Data Mining“, **aber** diese Schranke betrifft ja nur den **Input** und grds. nicht den Output, also auch eine andere Sichtweise wäre m.E. durchaus vertretbar...



Urheberrecht

Rechte von dritten Urhebern an KI-generierten Inhalten

- KI-generierte Inhalte können urheberrechtlich geschützte Werke bzw. Werkteile von dritten Urhebern enthalten
- Verwendung von KI-generierten Inhalten kann demnach zustimmungspflichtig sein
- Reproduktion
 - Nicht gemeinfreier Werke bestehen Rechte des Originalurhebers fort, §2 UrhG, §11 ff UrhG
 - Frei verwendbar sind amtliche Werke nach §5 UrhG und Werke, deren Schutzfrist abgelaufen ist, §64 ff UrhG



Urheberrecht

Rechte von dritten Urhebern an KI-generierten Inhalten

- Bearbeitungen oder Umgestaltungen
 - Dürfen nach §23 Abs. 1 UrhG nur mit Zustimmung des Urhebers des Ausgangswerkes veröffentlicht oder verwertet werden
 - Wahrt das neu geschaffene Werk (Output) einen hinreichenden Abstand zum benutzten Werk, so liegt keine Bearbeitung oder Umgestaltung vor, deren Verwendung zustimmungspflichtig ist



Urheberrecht

Rechte von dritten Urhebern an KI-generierten Inhalten

- Vorbestehende Filmszene oder Roman umschreiben
 - Fiktionale Figuren: einzelne Charaktere eines Films oder Sprachwerkes können Urheberrechtsschutz genießen
 - Übernahme des individuell gestalteten Handlungsverlaufs erforderlich, BGH, Urt. v. 29.4.1999 -I ZR 65/96 -Laras Tochter
 - Stil oder die Technik, in denen ein bestimmtes Werk geschaffen wurde, allein nicht schutzfähig
 - Die falsche Zuschreibung solcher Werke kann aber das allgemeine Persönlichkeitsrecht des Urhebers verletzen, dem die KI-generierten Inhalte zugeordnet werden, BGH, Urt. v. 8.6.1989 -I ZR 135/87 –Emil Nolde
- Bsp. Songtext im Stile von Nick Cave als ChatGPT-Output



Urheberrecht

Rechte von dritten Urhebern an KI-generierten Inhalten

- Vorbestehenden Text zusammenfassen
 - Zusammenfassung oder Verkürzung von Sprachwerken, kann eine Bearbeitung bzw. Umgestaltung sein, deren Verwendung zustimmungspflichtig ist
 - Entscheidend ist hierbei, ob eigenschöpferische Gehalt der Vorlage übernommen wird, wie wesentliche und prägende Formulierungen und Satzteile des Originalwerkes, BGH, Urt. v. 1. 12. 2010 -I ZR 12/08–Perlentaucher
 - Übernahme liegt nicht vor, wenn Zusammenfassung neu und autonom von der KI formuliert wird



Urheberrecht

Rechte von dritten Urhebern an KI-generierten Inhalten

- Fachtexte erstellen
 - Wissenschaftliche Werke sind grundsätzlich schutzfähig, §2 Abs. 1 UrhG, §2 Abs. 1 Nr. 7 UrhG
 - Aber wissenschaftliche Entdeckungen, Theorien und Ideen sind zur Vermeidung einer Monopolisierung dem Urheberrechtsschutz grundsätzlich entzogen, Art. 5 Abs. 3 GG
 - Aufgrund geringen Gestaltungsspielraums durch Vorgabe des Forschungsgegenstands und der Fachsprache häufig nur 1:1-Übernahme geschützt, LG Köln, Urt. v. 1.9.1999 -28 O 161/99 –MC-Klausuren
 - Bei Texten, deren Inhalt wesentlich durch die in ihnen erhaltenen Informationen bestimmt wird, kann schöpferische Geist des Verfassers nicht in origineller Weise zum Ausdruck kommen, EuGH, Urt. v. 29.7.2019 –C-469/17 –Afghanistan Papiere



Urheberrecht

Rechte von dritten Urhebern an KI-generierten Inhalten

- Fachtexte erstellen
 - Übernahme liegt nicht vor, wenn Fachtext nicht aus Textbausteinen oder Satzfragmenten vorbestehender Fachtexte zusammengesetzt wird, sondern neu und autonom von der KI formuliert wird



Urheberrecht

Gesetzliche Nutzungserlaubnisse für Lehrende

- Vervielfältigung, Verbreitung und öffentliche Wiedergabe eines veröffentlichten Werkes zum Zweck des Zitats, § 51 UrhG
- Vervielfältigung, die Verbreitung und die öffentliche Wiedergabe eines veröffentlichten Werkes zum Zweck der Karikatur, der Parodie und des Pastiches, §51a UrhG
- Zur Veranschaulichung der Lehre an Hochschulen dürfen zu nicht kommerziellen Zwecken für den begrenzten Kreis von Unterrichtsteilnehmern bis zu 15 Prozent eines veröffentlichten Werkes vervielfältigt, verbreitet, öffentlich zugänglich gemacht und in sonstiger Weise öffentlich wiedergegeben werden, §60a UrhG
- Vervielfältigung von wesentlichen Teilen einer Datenbank zu bestimmten Zwecken zulässig, §87 c UrhG
- Weiterverwendung von unwesentlichen Teilen einer Datenbank ist zulässig, §87b UrhG



Urheberrecht

Weiterverwendung des Outputs, eine urheberrechtliche Grauzone

Pastiche?

Auch wenn der Begriff des "Pastiche" noch keine klaren Konturen besitzt, geht es im Ergebnis um "eine Auseinandersetzung mit einem vorbestehenden Werk, das erkennbar ist, aber nicht bloß zur weiteren Verwertung kopiert wird". In den Worten der Gesetzesbegründung: "Anders als bei Parodie und Karikatur, die eine humoristische oder verspottende Komponente erfordern, kann diese beim Pastiche auch einen Ausdruck der Wertschätzung oder Ehrerbietung für das Original enthalten, etwa als Hommage." Dies dürfte zu weiteren offenen und von den Gerichten zu klärenden Auslegungsfragen führen.

Eine ausführliche Darstellung dazu findet sich bei [Kreutzer, Gutachten "Der Pastiche im Urheberrecht"](#)



Urheberrecht

§ 51a UrhG: Karikatur, Parodie und Pastiche

Zulässig ist die Vervielfältigung, die Verbreitung und die öffentliche Wiedergabe eines veröffentlichten Werkes zum Zweck der Karikatur, der Parodie und des Pastiches. Die Befugnis nach Satz 1 umfasst die Nutzung einer Abbildung oder sonstigen Vervielfältigung des genutzten Werkes, auch wenn diese selbst durch ein Urheberrecht oder ein verwandtes Schutzrecht geschützt ist.

https://www.gesetze-im-internet.de/urhg/__51a.html



Urheberrecht

Einräumung von Nutzungsrechten durch Anbieter des KI-Generators

- Anbieter von KI-Generatoren räumen den Nutzern die Nutzungsrechte am Output in ihren Nutzungsbedingungen ein
- Nutzungsrechte am Output können diese aber nur wirksam einräumen, wenn sie diese Rechte an den Inhalten (Input) selbst wirksam von den Urhebern bzw. Rechteinhabern erworben haben
- Urheber bzw. Rechteinhaber von im Output enthaltenen geschützten Inhalten können vom Nutzer Unterlassung der Verwendung mit kostenpflichtiger Abmahnung verlangen, §§ 97 ff. UrhG
- Nutzungsbedingungen enthalten i.d.R. keine Haftungsfreistellung im Fall der Geltendmachung von Rechten Dritter



Urheberrecht

Kennzeichnungspflicht von KI-generierten Inhalten (s. oben)

Art. 52 Abs. 3 KI-VO-E: „Nutzer eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die wirklichen Personen, Gegenständen, Orten oder anderen Einrichtungen oder Ereignissen merklich ähneln und einer Person fälschlicherweise als echt oder wahrhaftig erscheinen würden („Deepfake“), müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden.“

KI-generierte Texte werden nicht genannt und unterliegen somit nach KI-VO-E nicht der Kennzeichnungspflicht (argumentum e contrario aus dem Wortlaut)

Evtl. Kennzeichnungspflicht nach Nutzungsbedingungen des KI-Systems

Evtl. Kennzeichnungspflicht nach Hochschulrecht



Urheberrecht

Weitere Fragen...

„Aktiv“seite aus der Perspektive der Diensteanbieter: Können die durch KI generierten Inhalte monopolisiert werden?

- Vertragliche Normen: Nutzungsbedingungen, AGB etc.
- insbesondere: Urheberrecht, insbesondere Unterscheidung
 - Nur Mensch
 - Mensch/Maschine
 - Nur Maschine

Zur Vertiefung empfehlenswert ist der Aufsatz: „Die Schutzfähigkeit von KI-Trainingsdaten de lege lata - What would Machup find?“, s. unten.



Urheberrecht

Zukunftsmusik?

Leistungsschutzrecht für KI-Diensteanbietende, zum Beispiel a lá Leistungsschutzrecht für Presseverlage bzw. a lá Recht der Datenbankherstellenden?

De lege ferenda: Leistungsschutzrecht für Diensteanbietende von KI-Generatoren?

Persönliche These: Eher nein, denn argumentum e contrario aus der vergütungsfreien (!) Schranke nach § 44b UrhG „Text und Data Mining“, **aber** diese Schranke betrifft ja nur den **Input** und grds. nicht den Output, also auch eine andere Sichtweise wäre m.E. durchaus vertretbar...



Urheberrecht

Hoeren: „Geistiges Eigentum“ ist tot – lang lebeChatGPT (MMR 2023, 81ff.), Zitat:

„Maschinelles Lernen droht mit ihren Werkzeugen den klassischen Autoren überflüssig werden zu lassen und das Urheberrecht als Ganzes auszuhebeln. Dem stehen die Urheber und ihnen folgend die Content-Industrie hilflos gegenüber, die sich nur dadurch retten können, dass sie gesamtgesellschaftliche Umverteilungsmechanismen instrumentalisieren. Insbesondere über die Verwertungsgesellschaften mag es gelingen, noch allgemein (Pauschal-)Zahlungsströme für die Verwertung von Inhalten durch KI-Werkzeuge zu generieren. Einzelnen alt-antiquierten Urhebern mag es dann noch unbenommen sein, sich generell der Digitalisierung ihrer Werke iRv Urheberpersönlichkeitsrechten verstärkt durch DRM zu widersetzen.“



Urheberrecht

Hoeren: „Geistiges Eigentum“ ist tot – lang lebeChatGPT (MMR 2023, 81ff.), Zitat:

„Ansonsten werden GEMA und Co. zu neuen Treuhändern primärrechtlicher Nutzungsrechte (mit hoffentlich verstärkter Aufsicht durch die Kontrollbehörden). Das wird dann zu neuen Tarifen für die Verwertung durch KI-Systeme führen müssen. Und das ganze System der Leistungsschutzrechte steht auf dem Prüfstand, vor allem die Frage, ob eigentlich KI-Systeme Software iSv § 69a UrhG oder Datenbanken nach § 87a UrhG sind oder irgendetwas anderes beinhalten. Vermutlich ist das Kriterium der qualitativen oder quantitativen wesentlichen Investition besser geeignet, mit den Anforderungen der Informationsgesellschaft klarzukommen, auch wenn dann Kreativität im Urheberrecht allmählich zum Randphänomen wird.“



Sehr empfehlenswerte Linksammlung



<https://hochschulforumdigitalisierung.de/de/blog/chatgpt-im-hochschulkontext-%E2%80%93-eine-kommentierte-linksammlung>



Sehr empfehlenswerte Tutorials

dghd – Deutsche Gesellschaft für Hochschuldidaktik

„KI in der Hochschullehre“

Block I: Auswirkungen von textbasierten KI in der Lehre

- Prof. Dr. Doris Weißels (FH Kiel)

Was ist ChatGPT und wie funktioniert es? – Und welche ähnlichen Tools gibt es?

https://www.youtube.com/watch?v=cMuBo_rH15c

- Dr. Thomas Arnold (TU Darmstadt)

ChatGPT für Nicht-Informatiker*innen: Schlüssel zum Verstehen der künstlichen Intelligenz und ihrer Anwendungen in der Hochschullehre

<https://www.youtube.com/watch?v=-c8ogAwX6KI>



Sehr empfehlenswerte Tutorials

Künstliche Intelligenz: Glossar – die wichtigsten Begriffe

Klaus Meffert

Veröffentlicht am 10. Juli 2023 von Dr. DSGVO · zuletzt aktualisiert am 11. Juli 2023

<https://dr-dsgvo.de/kuenstliche-intelligenz-glossar-die-wichtigsten-begriffe/>



Workshop-Dokumentation

Die Online-Veranstaltung "KI-Generatoren in der Hochschul(lehr)e – Potenziale und rechtliche Implikationen von ChatGPT, DALL-E & Co." fand am 14. März 2023 statt:

- Potenziale und Anwendungsmöglichkeiten von KI-Generatoren in Hochschul(lehre) (Prof. Dr. Christian Spannagel, PH Heidelberg)
- Haftungs- und urheberrechtliche Herausforderungen bei der Verwendung von KI-Generatoren
 - Verantwortlichkeit der Anbietenden von KI-Generatoren (Jens O. Brelle, MMKH)
 - Urheberrecht: Input & Trainingsdaten (Jens O. Brelle, MMKH)
 - Weiterverwendung des Outputs (Dr. Janine Horn, ELAN e.V.)
- Herausforderungen für das Prüfungsrecht an Hochschulen (Prof. Dr. Dirk Heckmann, TUM)

<https://www.mmkh.de/digitale-lehre/netzwerk-landesinitiativen/ki-generatoren-in-der-hochschullehre.html>

KI-GENERATOREN IN DER HOCHSCHUL[LEHR]E

Potenziale und rechtliche Implikationen
von ChatGPT, DALL-E & Co.

ONLINE-VERANSTALTUNG

14. März 2023, 10:00 – 12:30 via Zoom

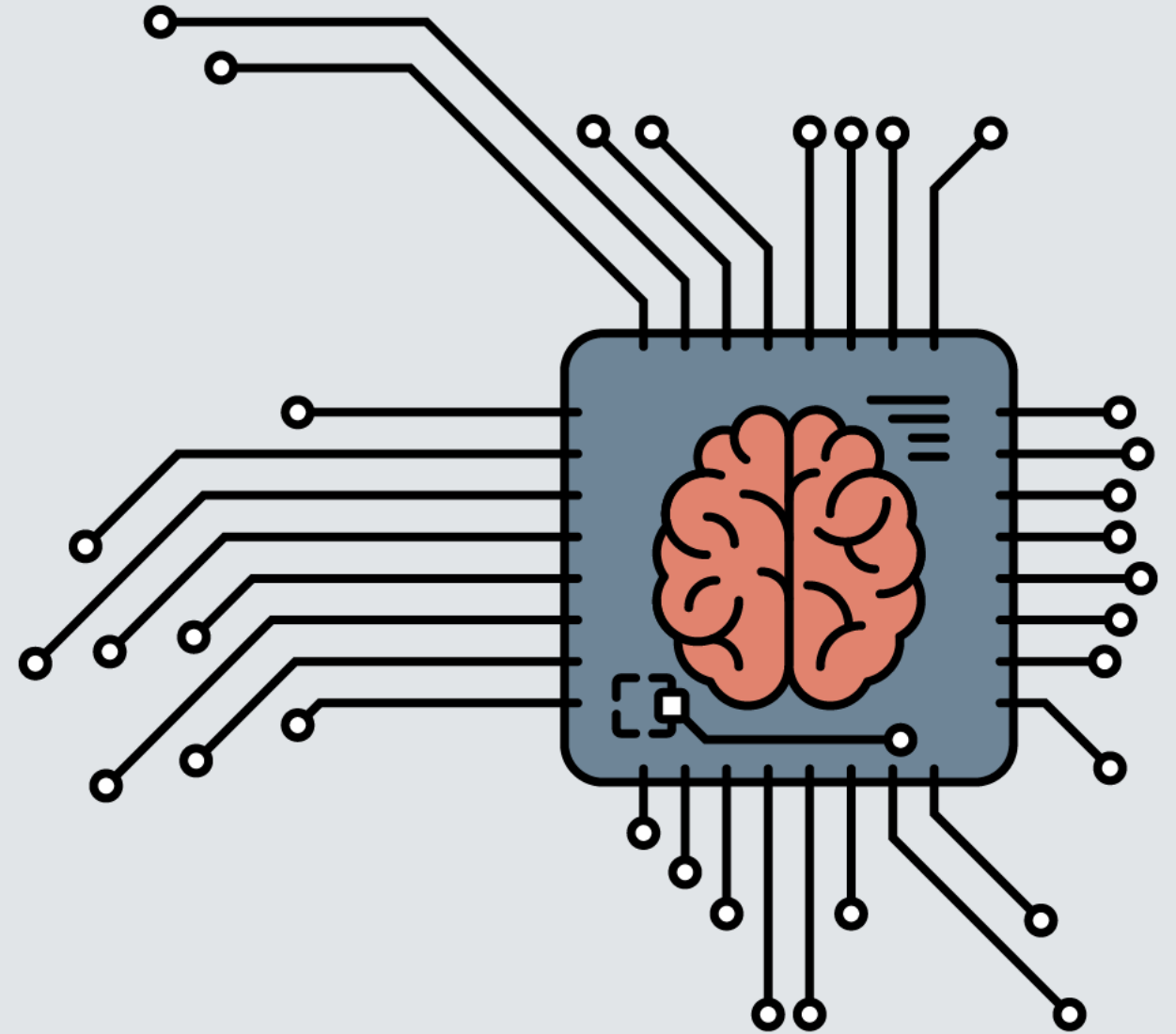
VORTRAGENDE

Prof. Dr. Christian Spannagel, PH Heidelberg

Prof. Dr. Dirk Heckmann, TUM

Jens O. Brelle, MMKH

Dr. Janine Horn, ELAN e.V.



MMKH.DE



Linksammlung & Vertiefungstipps

KI und OER: Wie gut passen sie zusammen?

Georg Fischer

Irights.info vom 23.04.2023

<https://irights.info/artikel/kuenstliche-intelligenz-und-open-educational-resources/31872>

Künstliche Intelligenz: Kampf um das Urheberrecht

Dr. Till Jaeger

Heise.de vom 17.02.2023

<https://www.heise.de/hintergrund/Kuenstliche-Intelligenz-Kampf-um-das-Urheberrecht-7518607.html>



Linksammlung & Vertiefungstipps

Beitrag zur Online-Veranstaltung "KI-Generatoren in der Hochschul(lehr)e – Potenziale und rechtliche Implikationen von ChatGPT, DALL-E & Co." am 14. März 2023 zum Thema **„Weiterverwendung des Outputs“ von Dr. Janine Horn** (Stiftung Innovation Hochschullehre, Souver@n & ELAN e.V.)

https://www.mmkh.de/fileadmin/veranstaltungen/netzwerk_landesinitiativen/KI-Generatoren/2023-03-14_KI-Generatoren_UrhR_Horn.pdf



Linksammlung & Vertiefungstipps

- **Daten-Governance-Rechtsakt**, VO (EU) 2022/868, Verkündungsblatt ausgewertet bis 16.06.2023, zukünftige Fassung - Text gilt ab 24.09.2023: https://beck-online.beck.de/?vpath=bibdata%2Fges%2FEU_VO_2022_868%2Fcont%2FEU_VO_2022_868%2eINH%2ehtm bzw. <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R0868>
 - **DIE AKTUELLE EU-GESETZGEBUNG** IM BEREICH DIGITALISIERUNG UND DATENWIRTSCHAFT – MÖGLICHE AUSWIRKUNGEN FÜR FORSCHUNGS- UND ENTWICKLUNGSPROJEKTE – EINE **ÜBERSICHT** - Erstellt im Rahmen der vom Bundesministerium für Wirtschaft und Klimaschutz beauftragten Begleitforschungen zu den Technologieprogrammen „KI-Innovationswettbewerb“ und „Smarte Datenwirtschaft“ (Stand: 23.03.2023): https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/SDW/2023_03_22_Leitfaden_Recht.pdf
 - **„Die DS-GVO bleibt unberührt“** DGA, DMA, DSA, AIA, DA, EHDS und der Datenschutz von Dr. Winfried Veil – BMI Referat DG I 4 Datenpolitik, Datenstrategie, Open Data: https://www.ihk-muenchen.de/ihk/documents/Recht-Steuer/Datenschutz/DSGVO-bleibt-unberu%CC%88hrt_Dr.-Winfried-Veil.pdf
-



Linksammlung & Vertiefungstipps

Daniel Becker: Der Kommissionsentwurf für eine KI-Verordnung – Gefahr für die Wissenschaftsfreiheit?

ZfDR 2023, 164

<https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzfd%2F2023%2Fcont%2Fzfd.2023.164.1.htm&anchor=Y-300-Z-ZFDR-B-2023-S-164-N-1>

Sarah Bußmann / Carolin Glasowski / Michael Niehaus / Sarah Stecher: Die Schutzfähigkeit von KI-Trainingsdaten de lege lata - What would Machup find?

RD 2022, 391

<https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fr%2F2022%2Fcont%2Fr.2022.391.1.htm&pos=6&hlwords=on>



Linksammlung & Vertiefungstipps

Victoria Guijarro Santos „Nicht besser als nichts - Ein Kommentar zum KI-Verordnungsentwurf“

Nicht besser als nichts

ZfDR 2023, 23

<https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzfd%2F2023%2Fcont%2Fzfd.2023.23.1.htm&anchor=Y-300-Z-ZFDR-B-2023-S-23-N-1>

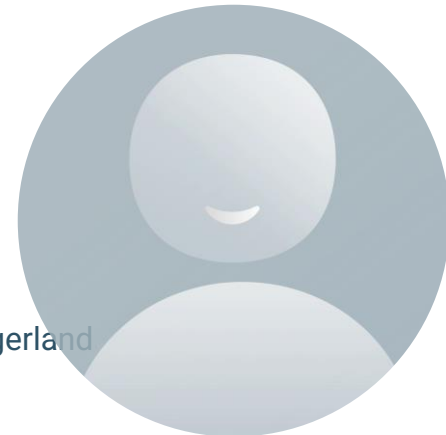
Vielen Dank für Ihre Aufmerksamkeit!



**Multimedia Kontor
Hamburg**

info@mmkh.de | www.mmkh.de | Saarlandstr. 30, 22303 Hamburg | +49 40 303 85 79-0

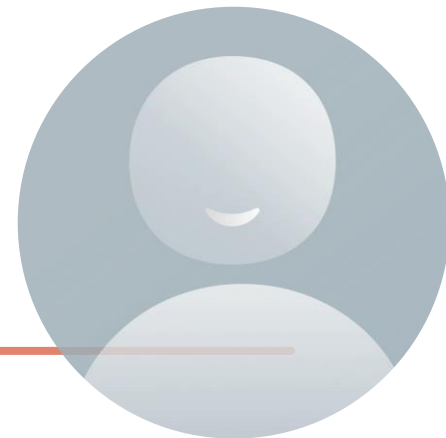
Registergericht Hamburg HRB 82237 | Geschäftsführer: Dr. Marc Göcks | Vorsitzende des Aufsichtsrats: Stephanie Egerland





Fragen?

Fragen am besten am Ende des Workshops...





Neue Regeln zur künstlichen Intelligenz (KI) - Was bedeutet das für Hochschulen?!

Inhalte der KI-Verordnung & Bezüge zu OpenData & zum
Datenschutz- & Urheberrecht



Neue Regeln zur künstlichen Intelligenz (KI) - Was bedeutet das für Hochschulen?!

Inhalte der KI-Verordnung & Bezüge zu OpenData & zum
Datenschutz- & Urheberrecht





Multimedia Kontor Hamburg

Ein Unternehmen der
Hamburger Hochschulen

