



Multimedia Kontor Hamburg

Ein Unternehmen der
Hamburger Hochschulen



KI-Detektoren und digitale Prüfungen – Möglichkeiten und prüfungsrechtliche Grenzen

Datenschutzrechtliche Fragen und (mögliche) Implikationen
des EU AI-Act für den Hochschulbereich

Jens O. Brelle (MMKH)



KI-Detektoren und digitale Prüfungen – Möglichkeiten und prüfungsrechtliche Grenzen

Datenschutzrechtliche Fragen und (mögliche) Implikationen des EU AI-Act für den Hochschulbereich

Jens O. Brelle (MMKH)



Inhaltsübersicht

- Zum Verständnis des Regelungskontextes: **Sehr kurzer Gesamtüberblick europäische Datenstrategie** & EU-Digitalgesetzgebung: von der DSGVO über DGA/DSA/DMA/DGA bis zur Open Data-Richtlinie/Datennutzungsgesetz und zur KI-Richtlinie (regelt die Haftung) und zur KI-Verordnung (sog. „AI-Act“, regelt die Verantwortung)
 - Schwerpunkt dieses Teils: **AI-Act**, d.h. die Entwürfe KI-Verordnung & KI-Richtlinie
 - Sonderfragen, aber **keine neuen Regeln**:
 - Datenschutz & Persönlichkeitsrechte (kurz)
 - Urheberrecht (sehr kurz)
-



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.
-



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) / Digitale-Dienste-Gesetz ab 17.02.2024
 - 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)
-

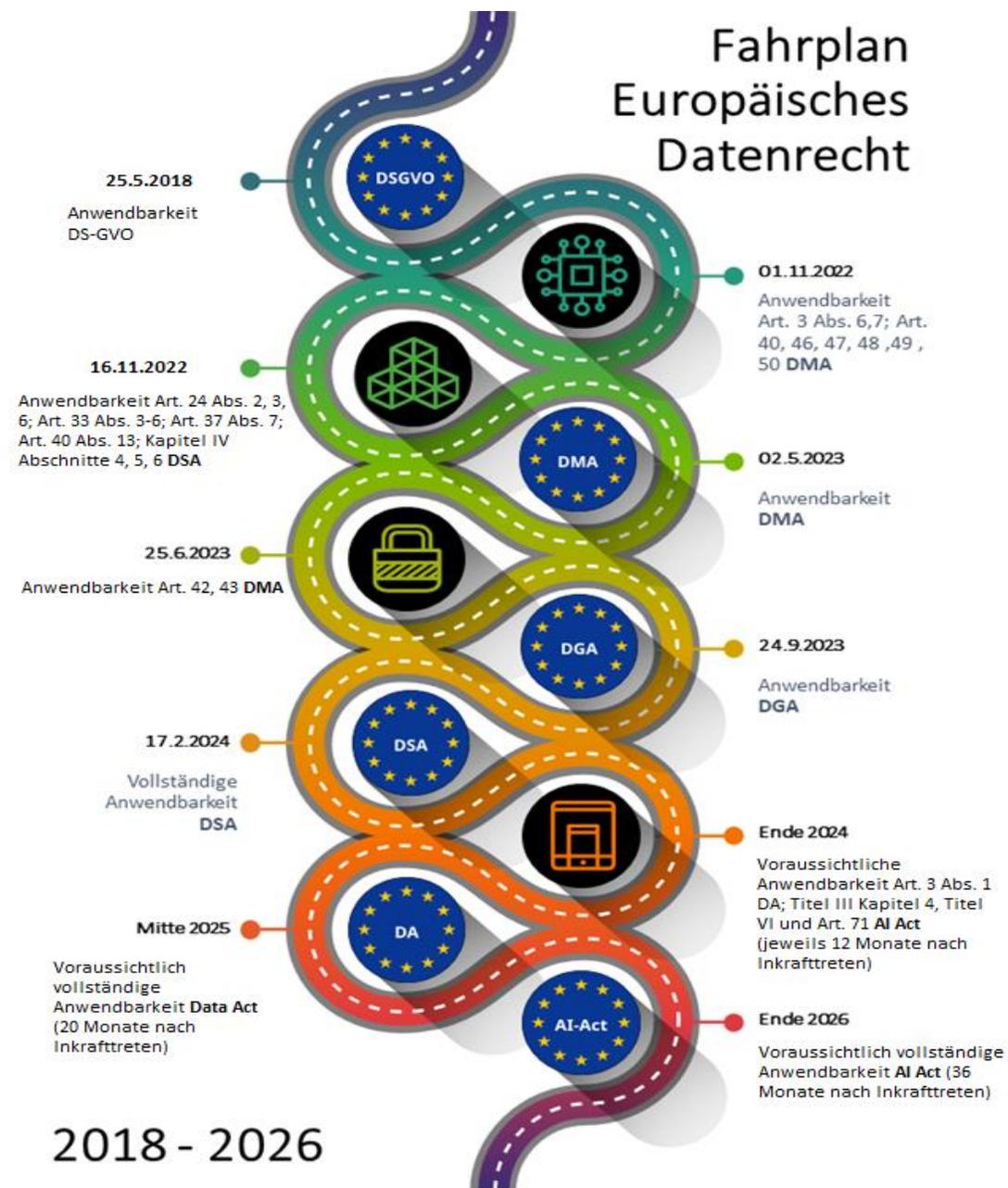


Übersicht EU-Digitalgesetzgebung

- Data Governance Act (DGA)
 - Open Data-Richtlinie / Datennutzungsgesetz (DNG)
 - KI-Verordnung (AI-Act)
 - KI-Richtlinie
-



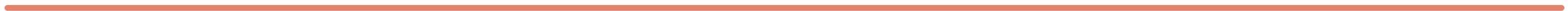
Fahrplan Europäisches Datenrecht



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



- **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 & nach den Trilog-Verhandlungen am 09.12.2023 auf eine Position zur Regulierung von Künstlicher Intelligenz geeinigt. 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 Jahr 2024 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
 - **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!**
-



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

Inkrafttreten der KI-Verordnung

Laut vorläufiger Einigung soll das KI-Gesetz – mit Ausnahme einiger spezifischer Bestimmungen – zwei Jahre nach seinem Inkrafttreten zur Anwendung kommen, also Ende 2025.

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

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 bzw. „unannehmbares“ Risiko (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?

Nach den ersten Entwürfen wurde um die Ergänzung einer weiteren Gruppe, nämlich „Allgemeine KI-Systeme“ diskutiert:

Neue Bestimmungen wurden hinzugefügt, um Situationen Rechnung zu tragen, in denen KI-Systeme für viele verschiedene Zwecke genutzt werden können (KI mit allgemeinem Verwendungszweck) und die Technologie anschließend in ein anderes System integriert wird, das als hochriskant gilt. In der vorläufigen Einigung wird auch auf den Sonderfall der KI-Systeme mit allgemeinem Verwendungszweck („general purpose artificial intelligence systems“, GPAI) eingegangen.



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

Pflichten der Nutzenden 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 Nutzenden 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 Nutzenden 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

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.
-



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...



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

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 Filmen o.ä.

DSGVO-Relevanz, da Personenbezug: Einspeisen von Schriftstücken (z.B. Prüfungsleistungen) 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@hochschule-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.



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

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

Automatisierte Entscheidungen im Einzelfall (Art. 22 DSGVO)

Gem. Art. 22 DSGVO sind **automatisierte Entscheidungen im Einzelfall grundsätzlich verboten**, außer wenn diese explizit durch eine entsprechende Rechtsgrundlage von der nationalen Gesetzgebung erlaubt sind.



Datenschutz

Automatisierte Entscheidungen im Einzelfall (Art. 22 DSGVO)

(1) Die betroffene Person hat das **Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet** oder sie in ähnlicher Weise erheblich beeinträchtigt.

(2) **Absatz 1 gilt nicht**, wenn die Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen **erforderlich** ist,

b) aufgrund von **Rechtsvorschriften** der Union oder der Mitgliedstaaten, denen der Verantwortliche **unterliegt**, zulässig ist und diese Rechtsvorschriften angemessene **Maßnahmen zur Wahrung der Rechte und Freiheiten** sowie der berechtigten Interessen der betroffenen Person enthalten oder



Datenschutz

Automatisierte Entscheidungen im Einzelfall (Art. 22 DSGVO)

c) mit **ausdrücklicher Einwilligung** der betroffenen Person erfolgt.

(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.



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

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 (sog. „EU/US-Data Privacy Framework“)

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.



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

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

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 & 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

- **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

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

Kennzeichnungspflicht von KI-generierten Inhalten

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



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



Ethische Leitlinien zur Nutzung von KI

Stellungnahme des deutschen Ethikrates

„Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz“ untersucht die Auswirkungen digitaler Technologien auf das menschliche Selbstverständnis und Miteinander. Sie fordert, dass die Künstliche Intelligenz (KI) dem Menschennutzen und nicht schaden soll, und dass die Menschenwürde, die Autonomie und die Teilhabe aller Menschen gewahrt werden müssen. Sie gibt auch ethische Leitlinien und politische Empfehlungen für den verantwortungsvollen Umgang mit KI.

<https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-menschund-maschine.pdf>



Ethische Leitlinien zur Nutzung von KI

Ethische Leitlinien der EU-Kommission zur Nutzung von künstlicher Intelligenz (KI) und Daten im Unterricht und beim Lernen für Bildungspersonal

Die Europäische Kommission hat Ethische Leitlinien zur Nutzung von künstlicher Intelligenz (KI) und Daten im Unterricht und beim Lernen für Bildungspersonal herausgegeben. Die Leitlinien sind ein wesentlicher Bestandteil des Aktionsplans für Digitale Bildung (2021-2027) der EU:

<https://education.ec.europa.eu/de/focus-topics/digital-education/action-plan>

<https://op.europa.eu/o/opportalservice/download-handler?identifier=d81a0d54-5348-11ed-92ed-01aa75ed71a1&format=pdf&language=de&productionSystem=cellar&part=>



Ethische Leitlinien zur Nutzung von KI

Empfehlung zur Ethik der Künstlichen Intelligenz der UNESCO

Im November 2021 haben die 193 UNESCO-Mitgliedsstaaten die Empfehlung zur Ethik der Künstlichen Intelligenz verabschiedet. Der Text setzt einen klaren ethischen Rahmen für aktuelle und zukünftige Anwendungen von KI in elf Handlungsfeldern, darunter Bildung, Kultur, Kommunikation, Arbeit und Gesundheit.

<https://unesdoc.unesco.org/ark:/48223/pf0000381137>



Linksammlung & Vertiefungstipps

- **Entwurf KI-VO (AI-Act):** <https://www.consilium.europa.eu/de/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/>
 - **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** (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-Steuern/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%2Frdi%2F2022%2Fcont%2Frdi.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 gern jetzt...





KI-Detektoren und digitale Prüfungen – Möglichkeiten und prüfungsrechtliche Grenzen

Datenschutzrechtliche Fragen und (mögliche) Implikationen
des EU AI-Act für den Hochschulbereich

Jens O. Brelle (MMKH)



KI-Detektoren und digitale Prüfungen – Möglichkeiten und prüfungsrechtliche Grenzen

Datenschutzrechtliche Fragen und (mögliche) Implikationen des EU AI-Act für den Hochschulbereich

Jens O. Brelle (MMKH)



Multimedia Kontor Hamburg

Ein Unternehmen der
Hamburger Hochschulen