

# Künstliche Intelligenz im gesetzlichen Rahmen nutzen - Der AI Act & seine Relevanz für NPOs

Heidi Scheichenbauer

[heidi.scheichenbauer@researchinstitute.at](mailto:heidi.scheichenbauer@researchinstitute.at)

Dezember 2024

**Research Institute AG & Co KG**  
**Digital Human Rights Center**

Florianigasse 55/10  
1080 Wien

<https://researchinstitute.at/>  
[www.networkfairdata.at](http://www.networkfairdata.at)



# Research Institute

## Digital Human Rights Center

### **RESEARCH INSTITUTE AG & CO KG– DIGITAL HUMAN RIGHTS CENTER**

Florianigasse 55/10  
1080 Wien

[www.researchinstitute.at](http://www.researchinstitute.at)

# Research Institute



## Forschung

Wissenschaftliche Forschung an der Schnittstelle von Technik, Recht, Gesellschaft. Grund- und datenschutzrechtliche Fragen sowie gesellschaftliche Folgen und ethische Aspekte neuer Technologien.



## Consulting

Fachlich kompetente sowie effiziente und lösungsorientierte Beratung im Bereich Datenschutz und IT- Compliance.



## Lehre

Seminare, Vorträge und Tagungen, akademische Lehre und Kurse in Kooperation mit führenden Expert\*innen der Branche sowie wissenschaftliche Publikationen



## Academy

Die Research Institute-Academy (RIAC) versteht sich als interdisziplinäre Plattform für Wissenstransfer und berufliche Weiterbildung in den Bereichen Technik, Recht, Verwaltung und Ethik. Die Veranstaltungen finden an unserem Standort in der Florianigasse oder als inhouse-Seminare statt und werden sowohl physisch als auch virtuell angeboten. Unsere Veranstaltungen werden von Austrian Standards als Weiterbildungsveranstaltung für die Rezertifizierung als Datenschutzbeauftragte\*r anerkannt.



## Network.fair.data

Mit dem Zweck Datenschutz – als Katalysator für alle Menschenrechte – in die Organisationskultur zu integrieren, wird mit network.fair.data ein Netzwerk von gemeinnützigen Organisationen und social entrepreneurs geschaffen, das es ermöglicht, niederschwellig und preiswert Zugang zu praxisrelevanten Informationen zum Datenschutz mit Blick auf NPOs zu bekommen.

- Juristin
- **Senior Researcher** und **Senior Consultant**, Research Institute
- Autorin von Fachbeiträgen in datenschutzrechtlichen Fachzeitschriften (Jus-IT, Datenschutz-konkret)
- Mitautorin mehrerer aktueller Bücher zur Datenschutz-Grundverordnung (jusIT Spezial: DS-GVO, Handbuch Datenschutz Verlag WEKA) Vortragstätigkeiten
- Datenschutz für Vereine (Verlag Linde)
- Der Datenschutzbeauftragte (Verlag Linde)
- **Erfahrungen** in:
  - Wissenschaft und Consulting (RI, KMU Forschung Austria)
  - Interessenvertretung und Rechtsberatung (Fundraising Verband Austria)
- **Forschungsschwerpunkte:**
  - Datenschutzrecht für gem. Organisationen



# UNSER NPO-PROJEKT: NETWORK.FAIR.DATA

network.fair.data

Home | Deutsch | network.fair.data

## DATENSCHUTZ, DER VERBINDET

Compliance im Bereich Datenschutz, insbesondere die laufende Umsetzung der DSGVO, benötigt oft eine fundierte Beratung, die zu kostenintensiv für gemeinnützige Organisationen sein kann.

Mit dem Zweck Datenschutz – als Katalysator für alle Menschenrechte – in die Organisationskultur zu integrieren, wird mit network.fair.data ein **Netzwerk von gemeinnützigen Organisationen und social entrepreneurs** geschaffen, das es ermöglicht, niederschwellig und preiswert Zugang zu praxisrelevanten Informationen zum Datenschutz mit Blick auf NPOs zubekommen.

Damit wird Mitgliedern eine Möglichkeit geboten, von der jahrelangen Expertise des Research Institute zu profitieren und durch den Austausch und das Zusammenwirken zwischen den Netzwerkorganisationen zu den – oftmals ähnlich gelagerten – Fragestellungen einen Mehrwert im Bereich Datenschutz zu schaffen.



<https://researchinstitute.at/network-fair-data/>

# WAS WIRD DERZEIT BEREITS GEMACHT- KI-EINSATZ IN NGOs/NPOs



# WAS WIRD DERZEIT BEREITS GEMACHT- KI-EINSATZ IN NGOs/NPOs



## Fundraising

- Konversation überprüfen
- Personalisierte Informationsfeeds
- Ideen für Aktionen finden
- Grafiken und Bilder erstellen
- (Erklär-)Videos erstellen



## SEO Inhalte

- Keywords zu Bildern finden
- Redaktionsplanung
- Newsletter erstellen
- Text in leichte Sprache bringen
- Transkriptionen, Untertitel
- Eindruck über eine Website erhalten



## Projekte

- Übersetzungen
- PDF Inhalte extrahieren
- Reiseplanungen



## Personal

- Stellenausschreibungen



## Verwaltung

- Protokolle schneller schreiben
- Transkriptionen
- PDF Inhalte extrahieren

Mitarbeiter\*innen Ebene

# KI BEDARFSERHEBUNG -Wo soll KI EINGESETZT WERDEN?

## ○ Beispiele

- Darstellung von Textbausteinen zu Themen
- Vergleichen und Abstimmen von Dokumenten in Feedbackprozessen
- Rechtschreibprüfung von Texten vor Veröffentlichung
- Check von PA-/PK-Texten/Stellungnahmen (etc), ob Aussagen widersprüchlich zu früher veröffentlichten Forderungen/Haltungen sind
- Screening von Dokumenten zu gewähltem Thema bzw. Kurzfassung dieser
- Protokollierung von Meetings und/oder Pressekonferenzen und auf die wesentlichen Punkte zusammenfassen
- Übersetzung von Mailtexten
- Auf Knopfdruck Erstellung von aktuellen „Pressespiegeln“ zu gewissen Themen - aktuelle Zitate (etc.) - finden
- Erstellung von Infoflyern, Broschüren
- Themenzuweisung nach Protokollen, Briefings,
- Zusammenfassen von Berichten, Publikationen, Studien etc. (Förderrichtlinien etc.)
- Erstellen von Präsentation (Bsp.: Bitte erstelle eine PPT. Die Grundlage dafür ist folgende Kurzstudie)
- Erstellen von Infographiken
- Tools zum Umformulieren von Texten / Übersetzungen
- Unterstützung bei der Formulierung von Emails, insbesondere Mails die an große Verteiler gehen
- Kalender: Terminfindungsassistenten. (Brauche einen Termin zw. 08:00 – 12:00 mit XY, XY & XY bitte sage mir das nächste mögliche Zeitfenster etc.)

- Regulierung künstlicher Intelligenz im Kontext der Digitalisierungsinitiative der EU
- Datenschutz/Menschenrechte
- Urheberrecht
- KI-Richtlinien/Haftung

# **Regulierung künstlicher Intelligenz im Kontext der Digitalisierungsinitiative der EU**

# PROBLEME

- Risiken für Sicherheit, Gesundheit, Grundrechte und Demokratie
- Unzureichender legislativer Rahmen, fehlende Standardisierung, kein Monitoring
- Rechtsunsicherheit bezüglich Anwendbarkeit bestehender Regelungen
- Nationalen und europäischen Behörden fehlen Mittel zur effektiven Begrenzung des Risikos für Wirtschaft und Gesellschaft und für Durchsetzung von Compliance
- Fehlendes Vertrauen in KI-Systeme
- Geringe Verfügbarkeit von Daten
- Fragmentierung des Binnenmarkts und eingeschränkte globale Wettbewerbsfähigkeit
- Beschränkte digitale Souveränität der EU

- Horizontaler Regulierungsansatz für Inverkehrbringen und Betrieb bestimmter KI-Systeme
- Produktsicherheit –NLF Mindestanforderungen, Marktüberwachung, Konformitätsbewertung

*Proposal for a regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), COM(2021) 206 final*

April 2021:  
EK  
Vorschlag

Juni 2023:  
Start Trilog

Annahme: ~  
Ende 2023

Anwendbar:  
~ 2026

# INTERNATIONALER KONTEXT

UN

- UNESCO Recommendation on the Ethics of AI (2021)

Council of Europe

- Draft Framework Convention on AI, Human Rights, Democracy and the Rule of Law

OECD

- Recommendation on AI (2022)

African Union

- AU-AI Continental Strategy

USA

- NIST Risk Management Framework, Blueprint for an AI Bill of Rights

China

- Regulation of Generative AI

**Ein schöner Tag beginnt mit einem guten Kaffee!**

**jura**  
Kaffeevollautomat  
ENA 8 Touch Full  
Metropolitan Black

- 1,1 Liter Wassertank
- 125 Gramm Bohnenbehälter
- 12 Kaffeespezialitäten
- Puls-Extraktionsprozess (P.E.P.®) optimiert die Extraktionszeit
- Touchscreen-Farbdisplay
- Auch in weiteren Farbausführungen erhältlich

Bestell-Nr.: 346 728

**899.-**  
Abhol-Barpreis

**Künstliche Intelligenz:**  
die am häufigsten bezogenen Produkte ordnen sich autom. auf den Plätzen 1 - 4 an.

Cappuccino, Latte Macchiato, Cortado etc. auf Knopfdruck

Gerät ohne Deko

**Sonderposten begrenzte Stückzahl**  
Abgabe nur in haushaltsüblichen Mengen

GENIUS X

DIE REVOLUTIONÄRE  
GENIUS X MIT  
KÜNSTLICHER  
INTELLIGENZ

- Art 3 Z 1 AIA: KI-System ist
  - ein **maschinengestütztes** System,
  - das für einen in unterschiedlichem Grade **autonomen Betrieb** ausgelegt ist,
  - das nach seiner Betriebsaufnahme **anpassungsfähig** sein kann und
  - das aus den erhaltenen Eingaben für **explizite oder implizite Ziele**
  - ableitet,
  - wie **Ausgaben** wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen hervorgebracht werden,
  - die physische oder virtuelle Umgebungen **beeinflussen können**.

**Ein schöner Tag beginnt mit einem guten Kaffee!**

**jura**  
Kaffeevollautomat  
ENA 8 Touch Full  
Metropolitan Black

- 1,1 Liter Wassertank
- 125 Gramm Bohnenbehälter
- 12 Kaffeespezialitäten
- Puls-Extraktionsprozess (P.E.P.®) optimiert die Extraktionszeit
- Touchscreen-Farbdisplay
- Auch in weiteren Farbausführungen erhältlich

Bestell-Nr.: 346 728

**899.-**  
Abhol-Barpreis

**Künstliche Intelligenz:**  
die am häufigsten bezogenen Produkte ordnen sich autom. auf den Plätzen 1 - 4 an.

Cappuccino, Latte Macchiato, Cortado etc. auf Knopfdruck

Gerät ohne Deko

**Sonderposten begrenzte Stückzahl**  
Abgabe nur in haushaltsüblichen Mengen

GENIUS X

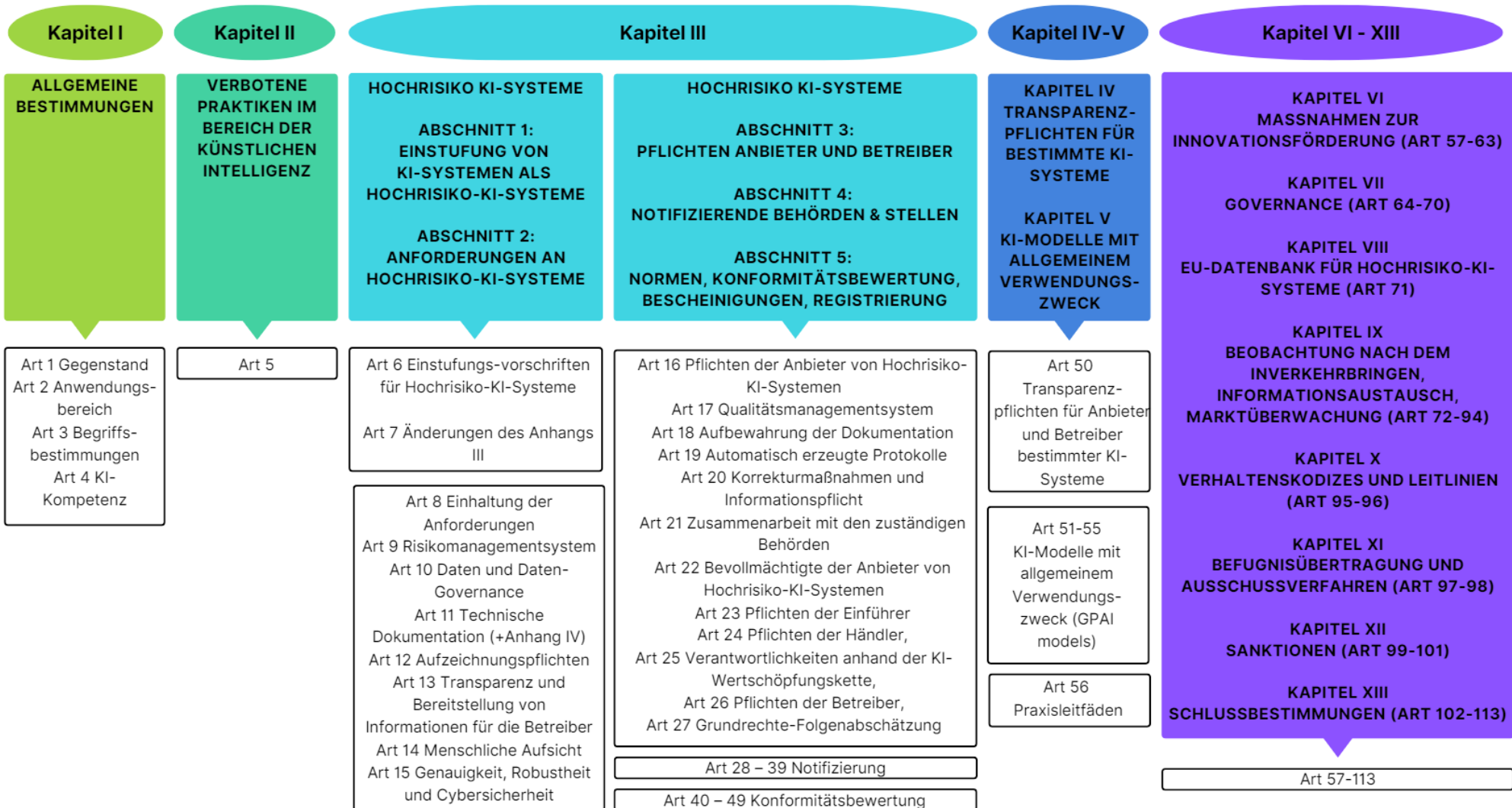
DIE REVOLUTIONÄRE  
GENIUS X MIT  
KÜNSTLICHER  
INTELLIGENZ

## • Details in ErwGr 12

- „sollte der Begriff auf den wesentlichen Merkmalen der KI beruhen, die ihn von **einfacheren herkömmlichen Softwaresystemen und Programmierungsansätzen abgrenzen**“
- „sollte sich **nicht** auf Systeme beziehen, die auf **ausschließlich von natürlichen Personen definierten Regeln** für das automatische Ausführen von Operationen beruhen.“
- „Zu den Techniken, die [...] das Ableiten beim Aufbau eines KI-Systems ermöglichen, gehören Konzepte für **maschinelles Lernen**, wobei aus Daten gelernt wird, wie bestimmte Ziele erreicht werden können, sowie **logik- und wissensgestützte Konzepte**, wobei aus kodierten Informationen oder symbolischen Darstellungen der zu lösenden Aufgabe abgeleitet wird.“

- AI Act ist im August 2024 in Kraft getreten
- Die Vorschriften der KI-Verordnung sind überwiegend nach 2 Jahren nach Inkrafttreten anwendbar
- Anwendbar nach 6 Monaten nach Inkrafttreten
  - allgemeine Vorschriften in Kapitel I
  - Verbot bestimmter KI-Systeme in Kapitel II der KI-Verordnung.
- Regelungen zur Klassifizierung von Hoch-Risiko-Systemen (Kapitel III) und die korrespondierenden Pflichten treten nach drei Jahren in Kraft

# KI Verordnung



# AI-ACT ZIELE (ART 1)

- harmonisierte Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen der künstlichen Intelligenz (im Folgenden „KI-Systeme“) in der Union;
- Verbote bestimmter Praktiken im Bereich der künstlichen Intelligenz;
- besondere Anforderungen an Hochrisiko-KI-Systeme und Verpflichtungen für Betreiber solcher Systeme;
- harmonisierte Transparenzvorschriften für KI-Systeme, die mit natürlichen Personen interagieren sollen, für KI-Systeme zur Emotionserkennung und zur biometrischen Kategorisierung sowie für KI-Systeme, die zum Erzeugen oder Manipulieren von Bild-, Ton- oder Videoinhalten verwendet werden;
- Vorschriften für die Marktbeobachtung und Marktüberwachung
- Vorschriften zur Förderung von Innovation (insb. SME und Start-ups, inkl Regulatory Sandboxes)

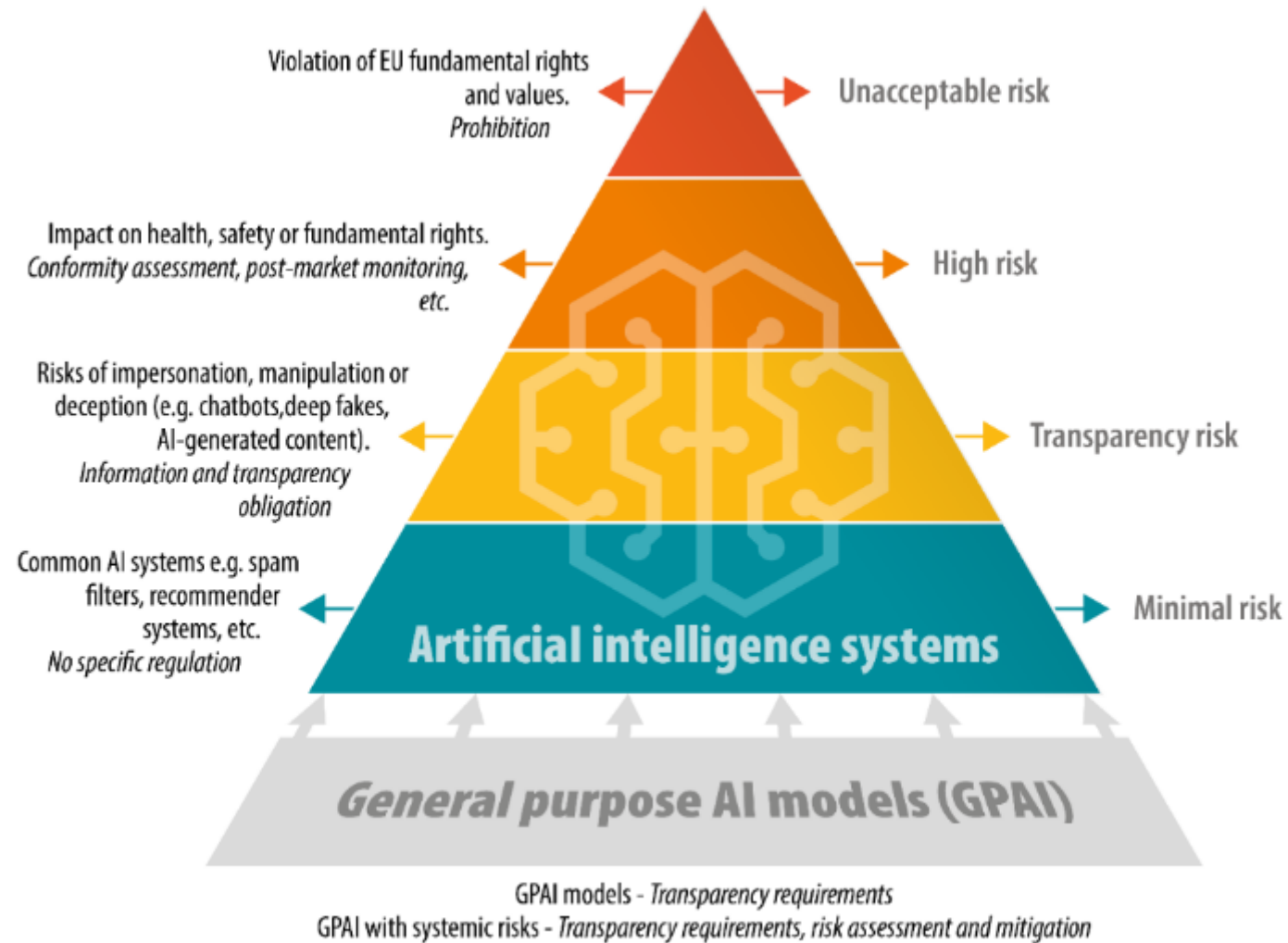
# ANWENDUNGSBEREICH

- **Anbieter**, die KI-Systeme/GPAI-Modelle in der Union **in Verkehr bringen oder in Betrieb nehmen**, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind;
- **Betreiber (professionelle Nutzer)** von KI-Systemen, die sich in der Union niedergelassen haben;
- Anbieter und Betreiber von KI-Systemen, die in einem Drittland niedergelassen oder ansässig sind, wenn das vom System hervorgebrachte **Ergebnis in der Union verwendet** wird

- Anwendungsbereiche **außerhalb des EU-Rechts**, insb die Kompetenzen des MS in Bezug auf nationale Sicherheit
  - Militär, Verteidigung, nationale Sicherheit
- **Behörden in Drittländern und internationale Organisationen** (soweit diese KI-Systeme im Rahmen internationaler Übereinkünfte im Bereich der Strafverfolgung und justiziellen Zusammenarbeit verwenden)
- KI-Systeme und Modelle, die ausschließlich für die wissenschaftliche **Forschung und Entwicklung** entwickelt und in Betrieb genommen werden

- **Forschung, Testen und Entwicklung** vor dem in Verkehr bringen oder in Betrieb nehmen
- Ausschließlich **private, nicht professionelle Nutzung** durch natürliche Personen als Betreiber
- KI-Systeme, die unter **Open Source Lizenzen** zur Verfügung gestellt werden
  - Ausnahmen für Hochrisiko-KI-Systeme, verbotene Praktiken, KI-Systeme nach Art 52 ff (ua GPAI)
- Partielle Ausnahme: Systeme nach **Anhang II Abschnitt B**
  - Bspw Flugzeug-, Automobilsektor

# RISIKO-BASIERTER ANSATZ



Data source: [European Commission](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1117).

# VERBOTENE SYSTEME

- KI-Systeme, die **Techniken der unterschwelligen Beeinflussung** außerhalb des Bewusstseins einer Person oder **bewusst manipulative oder täuschende Techniken** mit dem Ziel/Wirkung einsetzen, die Fähigkeit einer Person/Gruppe zur informierten Entscheidungsfindung zu beeinflussen, in einer Weise, die (signifikanten) Schaden verursacht
  - Wirtschaftliche/materielle Beeinträchtigungen nicht erfasst (zB Beeinflussung durch personalisierte Werbung)
- KI-Systeme, die eine **Schwäche oder Schutzbedürftigkeit** bestimmter Personen/Personengruppen **ausnützen** (zB Alter, Beeinträchtigung, soziale/wirtschaftliche Situation) mit dem Ziel/Wirkung das Verhalten zu beeinflussen, sodass (signifikanter) Schaden entsteht

# VERBOTENE SYSTEME

- **Biometrische Klassifizierungssysteme**, die natürliche Personen anhand aus ihren biometrischen Daten kategorisieren, um sensible Daten (zB Rasse) abzuleiten
- **Social Scoring**, das eine Schlechterstellung oder Benachteiligung verursacht
- Verwendung **biometrischer Echtzeit-Fernidentifizierungssysteme** in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken
- Systeme, die das Risiko einer **Straftat** anhand von Profiling vorhersagen/bewerten
- KI-Systeme, um Datenbanken für **Gesichtserkennung** durch unterschiedsloses „scraping“ zu erweitern/generieren
- **Emotionserkennung** am Arbeitsplatz/im Bildungsbereich

# HOCHRISIKO-KI-SYSTEME (ART 6)

- (1) KI-System ist eine Sicherheitskomponente eines Produkts oder ist selbst ein solches Produkt (gem. Harmonisierungsrechtsvorschriften in **Anhang II, wie bspw Maschinen, Spielzeug oder Medizinprodukte**) + Konformitätsbewertungsverfahren unter Einbindung **Dritter**
- (2) in **Anhang III** genannte „Stand-Alone“ KI-Systeme

# HOCHRISIKO-KI-SYSTEME (ART 6)

○ in **Anhang III** genannte KI-Systeme

1. Biometrie
2. kritische Infrastruktur
3. Allgemeine und berufliche Bildung
4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit
5. Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen
6. Strafverfolgung
7. Migration, Asyl und Grenzkontrolle
8. Rechtspflege und demokratische Prozesse

# HOCHRISIKO-KI-SYSTEME (ART 6)

## ○ Biometrie

- biometrische Fernidentifizierungssysteme
- biometrische Kategorisierung nach sensiblen oder geschützten Attributen oder Merkmalen auf der Grundlage von Rückschlüssen auf diese Attribute oder Merkmale
- Emotionserkennungssysteme

# HOCHRISIKO-KI-SYSTEME (ART 6)

## ○ Kritische Infrastruktur

- KI-Systeme als Sicherheitsbauteile im Rahmen der Verwaltung und des Betriebes kritischer Infrastruktur
  - kritische digitale Infrastruktur, Straßenverkehr, Wasser-, Gas- Wärme- oder Stromversorgung

# HOCHRISIKO-KI-SYSTEME (ART 6)

## ○ Allgemeine und berufliche Bildung

- Feststellung des Zugangs oder der Zulassung oder zur Zuweisung von Personen zu Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung
- Bewertung von Lernergebnissen
- Bewertung des angemessenen Bildungsniveaus, das eine Person im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung erhalten wird oder zu denen sie Zugang erhalten wird
- Überwachung und Erkennung von verbotenen Verhalten von Schülern bei Prüfungen im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung

# HOCHRISIKO-KI-SYSTEME (ART 6)

## ○ Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit

- Einstellung oder Auswahl natürlicher Personen (bspw gezielte Schaltung von Stellenanzeigen, Sichtung und Filterung von Bewerbungen, Bewertung von Bewerbern)
- Entscheidungen, die die Bedingungen von Arbeitsverhältnissen, Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen beeinflussen
- Zuweisung von Aufgaben aufgrund des individuellen Verhaltens oder persönlicher Merkmale oder Eigenschaften
- Beobachtung und Bewertung der Leistung und des Verhaltens von Personen in Beschäftigungsverhältnissen

# HOCHRISIKO-KI-SYSTEME (ART 6)

## ○ Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen

- Beurteilung von Behörden oder im Namen von Behörden, ob natürliche Personen Anspruch auf grundlegende öffentliche Unterstützungsleistungen und –dienste haben und ob solche Leistungen und Dienste zu gewähren, einzuschränken, zu widerrufen oder zurückzufordern sind
- Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen
- Risikobewertung und Preisbildung im Fall von Lebens- und Krankenversicherungen
- Bewertung und Klassifizierung von Notrufen
- Entsendung oder Priorisierung des Einsatzes von Not- und Rettungsdiensten
- Systeme für die Triage von Patienten bei der Notfallversorgung

# HOCHRISIKO-KI-SYSTEME (ART 6)

- **Strafverfolgung** (Nutzung durch Strafverfolgungsbehörden oder in deren Namen, Organen, Einrichtungen, sonstigen Stellen der EU)
  - Bewertung des Risikos einer natürlichen Person, zum Opfer von Straftaten zu werden
  - Lügendetektoren oder ähnliche Instrumente
  - Bewertung der Verlässlichkeit von Beweismitteln im Zuge der Ermittlung oder Verfolgung von Straftaten
  - Bewertung des Risikos, dass eine natürliche Person eine Straftat begeht oder erneut begeht, nicht nur auf der Grundlage der Erstellung von Profilen natürlicher Personen oder zur Bewertung persönlicher Merkmale und Eigenschaften oder vergangenen kriminellen Verhaltens von natürlichen Personen oder Gruppen
  - Erstellung von Profilen natürlicher Personen im Zuge der Aufdeckung, Ermittlung oder Verfolgung von Straftaten

# HOCHRISIKO-KI-SYSTEME (ART 6)

- **Migration, Asyl und Grenzkontrolle** (Nutzung durch Behörden oder in deren Namen, Organen, Einrichtungen, sonstigen Stellen der EU)
  - Lügendetektoren oder ähnliche Instrumente
  - Bewertung eines Risikos (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
  - Unterstützung 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
  - Systeme zum Zweck der Aufdeckung, Anerkennung oder Identifizierung natürlicher Personen

# HOCHRISIKO-KI-SYSTEME (ART 6)

## ○ Rechtspflege und demokratische Prozesse

- Unterstützung einer Justizbehörde bei der Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften und bei der Anwendung des Rechts auf konkrete Sachverhalte
  - erfasst auch alternative Streitbeilegung
- KI-Systeme, die verwendet werden sollen, um das Ergebnis einer Wahl oder eines Referendums oder das Wahlverhalten natürlicher Personen bei der Ausübung ihres Wahlrechts bei einer Wahl oder einem Referendum zu beeinflussen

# HOCHRISIKO-KI-SYSTEME - AUSNAHMEN

- Art 6 Abs 3 AIA (iVm ErwGr 53):
  - “ein KI-System [gilt] nicht als hochriskant, wenn es **kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte** natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst.“
- **Kriterien:**
  - KI-System ist dazu bestimmt, eine **eng gefasste Verfahrensaufgabe** durchzuführen
    - zB Datentransformation, Kategorisierung von Dokumenten, Erkennung von Duplikaten
  - KI-System, ist dazu bestimmt, **das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit zu verbessern**
    - zB Verbesserung der Sprache eines existierenden Dokuments, bspw professioneller oder wissenschaftlicher Stil

# HOCHRISIKO-KI-SYSTEME - AUSNAHMEN

## ○ Kriterien:

- KI-System ist dazu bestimmt, **Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen**, und ist nicht dazu gedacht, die zuvor abgeschlossene menschliche Bewertung, ohne eine angemessene menschliche Überprüfung zu ersetzen oder zu beeinflussen
  - zB Analyse eines menschlichen Benotungsmusters auf Abweichungen
- das KI-System ist dazu bestimmt, **eine vorbereitende Aufgabe für eine Bewertung durchzuführen**, die für die Zwecke der in Anhang III aufgeführten Anwendungsfälle relevant ist
  - zB intelligente Lösungen für die Bearbeitung von Dossiers, wie Indexierung, Suche, Text- und Sprachverarbeitung oder Verknüpfung von Daten mit anderen Datenquellen, oder KI-Systeme für die Übersetzung von Erstdokumenten

# ANFORDERUNGEN AN HOCHRISIKOSYSTEME

Risikomanagementsystem

Datenmanagement und  
Daten-Governance  
(Qualitätskriterien für  
Trainings-, Validierungs-  
und Testdatensätze)

Technische Dokumentation  
und Nachvollziehbarkeit

Aufzeichnungspflichten,  
Protokolle

Transparenz und  
Bereitstellung von  
Informationen für die  
Nutzer

Wirksame menschliche  
Aufsicht (Mensch-  
Maschine-Schnittstelle)

Genauigkeit, Robustheit  
und Cybersicherheit

Folgenabschätzung

# ANBIETERPFLICHTEN BEIM EINSATZ VON HOCHRISIKO-KI U.A.

Zu den Pflichten zählt die Sicherstellung der Anforderungen an Hochrisiko-KI-Systeme :

- Risikomanagementsystem
- Daten und Daten-Governance
- Technische Dokumentation
- Aufzeichnung von Ereignissen – „Protokollierung“
- Transparenz und Bereitstellung von Information für nachgelagerte Akteure
- Menschliche Aufsicht
- Genauigkeit, Robustheit und Cybersicherheit

# ANBIETERPFLICHTEN BEIM EINSATZ VON HOCHRISIKO-KI U.A.

## Weitere/sonstige Pflichten

- Qualitätsmanagement
- Kennzeichnung
- Aufbewahrung von bestimmten Unterlagen und Protokollereignissen
- Registrierung des KI-Systems
- Zusammenarbeit mit den zuständigen Behörden
- Konformitätsbewertung, -erklärung, -kennzeichnung
- Meldepflicht gegenüber zuständigen Behörden bei schwerwiegenden Vorfällen
- Sicherstellung der Barrierefreiheitsanforderungen
- Sofern erforderlich, Benennung eines Bevollmächtigten
- Sofern erforderlich, Korrekturmaßnahmen

# BETREIBERPFLICHTEN VON HOCHRISIKO-KI U.A.

- Einsatz von angemessenen technischen und organisatorischen Maßnahmen (TOMs) um sicherzustellen, dass das KI-System gemäß der Gebrauchsanweisung genutzt wird;
- Sicherstellung von menschlicher Aufsicht durch kompetente, geschulte natürliche Personen, welche die erforderliche Unterstützung erhalten und über die gebotene Autorität verfügen;
- Sicherstellung, dass Eingabedaten in Bezug auf die Zweckbestimmung „relevant und ausreichend repräsentativ“ sind;
- fortlaufende Überwachung nach Maßgabe der Gebrauchsanweisung und Sicherstellung der Außerbetriebnahme bei begründeter Annahme, dass die Anwendung zu einem unverhältnismäßigen Risiko für Gesundheit, Sicherheit oder Grundrechte führt;

# BETREIBERPFLICHTEN VON HOCHRISIKO-KI U.A.

- Meldepflichten bei Außerbetriebnahme oder schwerwiegenden Vorfällen;
- Dokumentationspflichten, insbesondere Speicherung von automatisch erzeugten Protokollen für mindestens sechs Monate, um das ordnungsgemäße Funktionieren des Systems nachweisen zu können oder Ex-Post-Kontrollen nachträglich zu ermöglichen;
- Vorabinformation von Arbeitnehmern und Arbeitnehmervertretern, wenn diese am Arbeitsplatz von einem Hochrisiko-KI-System betroffen sind;
- besondere Informationspflichten, wenn Hochrisiko-KI-Systeme Entscheidungen über natürliche Personen treffen oder bei diesen Entscheidungen unterstützen, dazu zählt auch das neue Recht des Betroffenen auf Erklärung einer Einzelfallentscheidung (Art. 86 KI-Verordnung)
- Tlw Durchführung von Fundamental Rights Impact Assessment
- Ggf Durchführung von DSFA

# TRANSPARENZPFLICHTEN FÜR BESTIMMTE KI-SYSTEME (ART 50)

- **Anbieter:** Information über KI-Systeme, die (direkt) **mit natürlichen Personen interagieren** (bspw Chatbots)
- **Anbieter:** Maschinenlesbares „**Wasserzeichen**“ (künstlich erzeugt/manipuliert) für den Output generativer Systeme (synthetische Audio-, Bild oder Textinhalte)
- **Betreiber:** Information über **Emotionserkennungssysteme/Systeme zur biometrischen Kategorisierung**
- **Betreiber:** Information über **Deepfakes** (künstlich erzeugte/manipulierte Bild-, ton- oder Videoinhalte)
- **Betreiber:** Information über **künstlich generierte/manipulierte Texte**, die veröffentlicht werden, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren

# DARSTELLUNG ANBIETERPFLICHTEN

## AI Act: Verpflichtungen von Anbietern

Der Umfang der Verpflichtungen nimmt entsprechend der Risikoklassifizierung des KI-Systems/KI-Modells ab

|                                                          | Hochrisiko<br>KI-System | GPAI-Modell<br>system. Risiko | GPAI-Modell      | KI-System<br>begrenzt. Risiko | KI-System<br>minimal. Risiko |
|----------------------------------------------------------|-------------------------|-------------------------------|------------------|-------------------------------|------------------------------|
| KI-Kompetenz                                             | Art. 4                  | Art. 4                        | Art. 4           | Art. 4                        | Art. 4                       |
| Transparenz gegenüber nachgelagerten Akteuren            | Art. 13                 | Art. 55 (1)                   | Art. 53 (1) b    | Art. 50 (1), (2)              |                              |
| Anforderungen an Daten                                   | Art. 10                 | Art. 55 (1)                   | Art. 53 (1) c, d |                               |                              |
| Technische Dokumentation                                 | Art. 11                 | Art. 55 (1)                   | Art. 53 (1) a    |                               |                              |
| Zusammenarbeit mit Behörden                              | Art. 21                 | Art. 55 (1)                   | Art. 53 (3)      |                               |                              |
| Bennenung Bevollmächtigter (sofern Drittstaat)           | Art. 22                 | Art. 55 (1)                   | Art. 54          |                               |                              |
| Risikomanagement                                         | Art. 9                  | Art. 55 (1) a, b              |                  |                               |                              |
| Genauigkeit, Robustheit und Cybersicherheit              | Art. 15                 | Art. 55 (1) d                 |                  |                               |                              |
| Registrierungs- bzw. Mitteilungspflichten                | Art. 49                 | Art. 52 (1)                   |                  |                               |                              |
| Meldepflichten gegenüber Behörden                        | Art. 73                 | Art. 55 (1) c                 |                  |                               |                              |
| Aufzeichnung von Ereignissen                             | Art. 12                 |                               |                  |                               |                              |
| Implementierung menschlicher Überwachungstools           | Art. 14                 |                               |                  |                               |                              |
| Kennzeichnungspflichten                                  | Art. 16 b               |                               |                  |                               |                              |
| Sicherstellung der Barrierefreiheitsanforderungen        | Art. 16 l               |                               |                  |                               |                              |
| Qualitätsmanagement                                      | Art. 17                 |                               |                  |                               |                              |
| Aufbewahrungspflichten                                   | Art. 18, 19             |                               |                  |                               |                              |
| Korrekturmaßnahmen                                       | Art. 20                 |                               |                  |                               |                              |
| Konformitäts-Bewertungsverf., -Erklärung, -Kennzeichnung | Art. 43, 47, 48         |                               |                  |                               |                              |

# DARSTELLUNG BETREIBERPFLICHTEN

## AI Act: Verpflichtungen von Betreibern

Der Umfang der Verpflichtungen nimmt entsprechend der Risikoklassifizierung des KI-Systems ab

|                                                                                                                                                  | Hochrisiko KI-System  | KI-System begrenzt. Risiko | KI-System minimal. Risiko |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|----------------------------|---------------------------|
| KI-Kompetenz                                                                                                                                     | Art. 4                | Art. 4                     | Art. 4                    |
| Transparenz gegenüber nachgelagerten Akteuren                                                                                                    | Art. 26 (11)          | Art. 50 (3), (4)           |                           |
| Verwendung des KI-Systems laut Betriebsanleitung                                                                                                 | Art. 26 (1), (3), (4) |                            |                           |
| Menschliche Aufsicht                                                                                                                             | Art. 26 (2)           |                            |                           |
| Überwachung des KI-Systems                                                                                                                       | Art. 26 (5)           |                            |                           |
| Meldung von schwerwiegenden Vorfällen                                                                                                            | Art. 26 (5), 73       |                            |                           |
| Aufbewahrung von erzeugten Protokollen                                                                                                           | Art. 26 (6)           |                            |                           |
| Sofern relevant, Datenschutz-Folgenabschätzung                                                                                                   | Art. 26 (9)           |                            |                           |
| Zusammenarbeit mit zuständigen nationalen Behörden                                                                                               | Art. 26 (12)          |                            |                           |
| Recht auf Erläuterung der Entscheidungsfindung im Einzelfall                                                                                     | Art. 86 (1)           |                            |                           |
| Informationspflichten gegenüber der Arbeitnehmer:innen-Vertretung<br><i>sofern Arbeitgeber:in Hochrisiko-KI-Systeme am Arbeitsplatz einsetzt</i> | Art. 26 (7)           |                            |                           |
| Registrierungspflicht<br><i>sofern EU-Organe, EU-Einrichtungen und sonstige EU-Stellen</i>                                                       | Art. 26 (8), 49       |                            |                           |
| Genehmigungspflicht einer Justiz- oder Verwaltungsbehörde<br><i>sofern Einsatz zur nachträglichen biometrischen Fernidentifizierung</i>          | Art. 26 (10)          |                            |                           |
| Erstellung einer Grundrechte-Folgenabschätzung<br><i>sofern u. a. öffentl. oder private Einrichtungen öffentliche Dienste erbringen</i>          | Art. 27               |                            |                           |

# PFLICHT ZUR UMSETZUNG VON KI-KOMPETENZ (UNABHÄNGIG VON RISIKOKLASSE)

- Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen,
- Dabei sind
  - ihre technischen Kenntnisse,
  - ihre Erfahrung,
  - ihre Ausbildung und Schulung und der Kontext,
  - in dem die KI-Systeme eingesetzt werden sollen,
  - sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen.
- Ziel: im Hinblick auf KI-Systeme sollen informierte Entscheidungen getroffen und ein Bewusstsein für die Potenziale und Risiken von KI geschaffen werden

# GENERAL PURPOSE AI (GPAI)

- KI-Systeme mit allgemeinem Verwendungszweck (GPAI) & Basismodelle
  - KI mit allgemeinem Verwendungszweck
  - Anders als auf bestimmten Zweck ausgerichtete KI-Modelle
  - Es gelten andere Risikokategorien als für „herkömmliche“ KI-Modelle, die nach ihren spezifischen Anwendungsfällen/Verwendungszweck
  - Einstufung basiert nicht auf der Anwendung, sondern auf der Funktion des zugrunde liegenden Basismodells.
- **Pflichten für Anbieter von GPAI-Modellen:**
  - Technische Dokumentation
  - Information und Dokumentation für Betreiber, die das Modell in ein KI-System integrieren wollen (zB Fähigkeiten, Limitationen)
  - Policy zur Wahrung von Urheberrecht
  - Veröffentlichung einer Zusammenfassung des Inhalts der Trainingsdaten
- Partielle Ausnahme für Modelle, die unter einer **open-Source-Lizenz** veröffentlicht werden
- **Weitere Pflichten für Anbieter von GPAI-Modellen mit systemischem Risiko (besonders leistungsstarke GPAI-Modelle)**

- **Beschwerderecht** bei Marktaufsichtsbehörde (Art 85)
  - Behauptung der Verletzung von Bestimmungen des AIA
  - Berücksichtigung bei Marktüberwachungstätigkeiten
  - kein Rechtsmittel gegen diese Entscheidung
  
- **Recht auf Erklärung** der der Entscheidungsfindung (Art 86)
  - beschränkt auf stand alone KI-Systeme
  - Entscheidungen mit rechtlicher Auswirkung/erhebliche Beeinträchtigung in ähnlicher Art (vgl Art 22 DSGVO)
  - klare und aussagekräftige Erläuterung der
    - Rolle des KI-Systems im Entscheidungsprozess
    - Wichtigste Elemente (zuvor Hauptparameter) der Entscheidung
  - subsidiär zu anderen Rechten (bspw DSGVO)

# AI-ACT DURCHSETZUNG

- Ex ante: Konformitätsprüfung und Registrierung bei Hochrisikosystemen
- Ex post: Nationale Behörden (Marktüberwachungsbehörden)
- Verwaltungsstrafen:
  - bis zu €35 Mio oder 7% des jährl. weltweiten Umsatzes (**Verletzung verbotener Praktiken**)
  - **ansonsten** €15 Mio oder 3% des jährl. weltweiten Umsatzes (bzw. bei **Verstoß gegen Transparenzpflichten**)
  - **GPAI-Modelle**: bis zu €15 Mio oder 3% des jährl. weltweiten Umsatzes (Kompetenz der Kommission)

- Übergangsfristen zur Anpassung an die neuen Vorgaben:
  - 6 Monate für verbotene KI-Systeme
  - 12 Monate für General Purpose AI Modelle
  - 24 Monate nach Inkrafttreten des AI Act (sohin der 2.8.2026) gelten grundsätzlich alle Verpflichtungen (Anforderungen an Hochrisiko-KI-Systeme gemäß Anhang III (nicht hingegen Anhang I), KI-Systeme mit geringem und minimalem Risiko
  - 36 Monate für Hoch-Risiko-KI-Systeme in bereits regulierten Bereichen nach Annex II des AI Acts
- Verbotene KI-Systeme müssen innerhalb von 6 Monaten, vom europäischen Markt genommen werde



- Nur wenige KI-Systeme sind verboten
- Nur manche KI-Systeme werden als Hochrisiko-System eingestuft (betrifft zB Emotionserkennung)
- Pflichten aus dem AI Act für Betreiber nicht hochriskanter Systeme halten sich in Grenzen
- Es bestehen nach dem AI Act für Betreiber ansonsten vorwiegend bestimmte Transparenzpflichten
- Sicherstellung der „KI-Kompetenz“ aber auch auf Betreiberebene relevant
- Für Anwender die GPAI-Systeme verwenden, bestehen keine zusätzlichen Anforderungen
  - Erste Tools zur Selbsteinschätzung in Entwicklung, zB <https://artificialintelligenceact.eu/de/bewertung/eu-ai-act-compliance-checker/>
  - Achtung Tools tlw fehlerhaft
  - Es bestehen (bereits jetzt) auf anderen Ebenen rechtliche Anforderungen...

# HINWEIS: KI-HAFTUNG SOLL EIGENS GEREGLT WERDEN

- AI-Act regelt nicht zivilrechtliche Haftung
- Paket aus Regelungen zu verschuldensabhängiger und Produkthaftung
  - eigene Richtlinie über KI-Haftung
  - Einbeziehung von Software in neue Produkthaftungs-Richtlinie
- derzeit jeweils ordentliches Gesetzgebungsverfahren
- AI Liability Directive (AILD)
  - Abwägung verschiedener Optionen und Evaluierung später
  - verschuldensabhängige, außervertragliche, zivilrechtliche Schadenersatzansprüche
  - Im Kern: Offenlegungspflicht und Kausalitätsvermutung

## Datenschutz/DSGVO

***AI-Act: ...die DSGVO bleibt unberührt...***

# DATENSCHUTZRECHT UND KI

- Datenschutzrechtliche Erfordernisse spielen eine entscheidende Rolle bei der Umsetzung von KI-Projekten wenn pb Daten verarbeitet werden
- Klärung der datenschutzrechtlichen Rollen (wer ist verantwortlich, besteht eine gemeinsame Verantwortlichkeit, gibt es ein AV-Verhältnis?)
- Herausforderung der Einhaltung der datenschutzrechtlichen Grundsätze (insb Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenrichtigkeit..)
- Informierte Einwilligung möglich? Berechtigte Interessen?
- Sicherstellung der Betroffenenrechte?
- Im Idealfall soweit möglich Anonymisierung der Trainingsdaten bereits während der Aufbereitung
- Prüfung ob automatisierte Entscheidung im Einzelfall vorliegt
- Prüfung ob Datenschutz-Folgenabschätzung erforderlich ist

# RISIKEN BEI EINBINDUNG VON CHATGPT IN PRODUKTE UND SERVICES

- Datenschutz u.a.:
  - Auftragsverarbeitervertrag?
  - Rechtmäßigkeit der Datenverarbeitung?
  - Haftung?
  - Privacy by Design, DSFA und TIA?
  - Transparenz? (Fehlende) Datenschutzinformation?
  - Datenquelle (Ausgewogenheit, Richtigkeit)?
  - Betroffenenrechte?
- Sonstige Bedenken:
  - Korrektheit und Genauigkeit – Faktencheck
  - Sensible oder proprietäre Unternehmensdaten
  - Copyright und IPR Probleme
  - Ethische Aspekte (insb. im akademischen/Forschungsbereich)

Vorsicht bei Eingabe

- personenbezogener Daten
- sonstige heikle Daten (zB Geschäftsgeheimnis, Code, IPR)
- finanzielle Information, Informationssicherheits-relevanter Input

Prüfung von

- Terms of Use, Datenschutzinformation, rechtl. Rahmen
- faktische Richtigkeit und Genauigkeit
- Haftungsaspekte
- Output auf IPR und Copyright, pb Informationen

*OpenAI Business Terms govern use of our APIs, ChatGPT Enterprise, ChatGPT Team, and other services for businesses and developers.*

## 6. Privacy

*6.1 Personal Data. If you use the Services to process personal data, you must*

- (a) provide legally adequate privacy notices and obtain necessary consents for the processing of personal data by the Services,*
- (b) process personal data in accordance with applicable law, and*
- (c) if processing “personal data” or “Personal Information” as defined under applicable data protection laws, execute our **Data Processing Addendum** by filling out this form.*

<https://openai.com/policies/business-terms>



## Data Processing Addendum

Please complete this form to execute OpenAI's Data Processing Agreement.

Note that this agreement is only applicable to our business service offerings (ChatGPT Enterprise, ChatGPT Team, APIs, or any OpenAI Services for businesses or developers) and **NOT** our consumer services (ChatGPT, DALL-E Labs).

Unfortunately, we are unable to review or sign DPAs provided by our customers or customize our DPA on a case by case basis.

Once you submit this form, you will have the opportunity to review the agreement before accepting or rejecting the terms. A request to review the agreement will also be sent to the signer email address you provided.

The agreement will only be considered legally binding after you accepted the terms.

Abrufbar unter <https://ironcladapp.com/public-launch/63ffefa2bed6885f4536d0fe>

# DATENSCHUTZRECHT UND KI - FAZIT

- Klärung der datenschutzrechtlichen Rollen (wer ist verantwortlich, besteht eine gemeinsame Verantwortlichkeit, gibt es ein AV-Verhältnis?)
- Herausforderung der Einhaltung der datenschutzrechtlichen Grundsätze (insb Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenrichtigkeit..)
- Informierte Einwilligung möglich? Berechtigte Interessen?
- Sicherstellung der Betroffenenrechte?
- Im Idealfall soweit möglich Anonymisierung der Trainingsdaten bereits während der Aufbereitung
- Prüfung ob automatisierte Entscheidung im Einzelfall vorliegt
- Prüfung ob Datenschutz-Folgenabschätzung erforderlich ist
- Bei Nutzung von LLMs wie ChatGPT jedenfalls kostenpflichtige Varianten verwenden und Data Processing Addendum abschließen
- Betroffenen Datenschutzinformationen erteilen

# Urheberrecht

- Anbieter trainieren oftmals Training mit Daten die selbst urheberrechtlich geschützt sind (ohne entsprechende Lizenzen zu haben)
  - Zahlreiche Prozesse sind im Gange
- Was gilt für von Nutzern selbst hochgeladene Daten?
  - Nutzer ist für die (hochgeladenen) Inhalte verantwortlich
    - Liegt ein urheberrechtlich geschütztes Werk vor?
    - Wenn ja, hat man grundsätzlich ausreichende Rechte
  - Analyse der Nutzungsbedingungen; idR Rechtevorbelt für KI-Training
  - ChatGPT/Open-AI räumt nicht exklusive Nutzerlizenz an den Ergebnissen ein
  - Häufig Rechtevorbelt für KI-Training

## KI-Guidelines

- Typischer Use-Case:
  - Mitarbeiter geben in ChatGPT geheime Unternehmensdaten ein, um Arbeitsaufgaben effizienter lösen zu können
- ChatGPT nutzt unter gewissen Umständen alle Inputdaten für KI-Training
- Interne Guidelines sind notwendig für den Schutz von Geschäftsgeheimnissen und aus datenschutzrechtlichen Gründen

## ○ Was sollte geregelt werden?

- Umgang mit Daten und Datenschutz
- Schutz von Betriebs- und Geschäftsgeheimnissen
- Sicherstellung von guter Qualität
- Vermeidung von Biases/Verzerrungen
- Interne Verantwortlichkeiten
- Mitarbeiterschulungen zum Umgang mit KI (AI-Literacy)
- Gutes Beispiel für Guidelines:

[https://www.austriatourism.com/fileadmin/user\\_upload/Media\\_Library/Test/Schulung/OEW Interne Leitlinien zur Nutzung von KI.pdf](https://www.austriatourism.com/fileadmin/user_upload/Media_Library/Test/Schulung/OEW_Interne_Leitlinien_zur_Nutzung_von_KI.pdf)

- Wenige Systeme verboten
- Großteil der Regelungen gelten für Hochrisiko-KI-Systeme
- Hochrisiko-Systeme eher die Ausnahme
- Transparenzpflichten im Bereich Emotionserkennung und künstlich generierter Texte/Bilder
- Systeme für Churn-Prediction/Prävention primär ein DSGVO-Thema
- Insgesamt DSGVO und Urheberrecht beachten!
- KI-Kompetenz sicherstellen
- Organisationsinterne Guidelines schaffen!

- Schwartmann/Keber/Zenner, KI-VO Leitfaden für die Praxis
- Ulbricht, Brajovic, Duhme, Hawighorst, Huber, Iber, Nemec Praxishandbuch KI und Recht: Rechtliche Aspekte beim Einsatz von Künstlicher Intelligenz – inkl. der neuen KI-Verordnung der EU
- Windholz, Praxishandbuch KI-VO: Künstliche Intelligenz rechtskonform im privaten und öffentlichen Bereich einsetzen

# Vielen Dank!



Abonnieren Sie unseren Newsletter und  
besuchen Sie uns unter: [www.researchinstitute.at](http://www.researchinstitute.at)

# RECHTLICHE HINWEISE

**Zweck:** Dieses Dokument dient als Trainingsunterlage.

Erstellt von: Dr. Heidi Scheichenbauer

**Copyright:**

Die vorliegenden elektronischen Unterlagen und Dateien wurden von den genannten Erstellern entwickelt und sind frei von Urheberrechten Dritter. Wir dürfen Sie daher bitten, das geistige Eigentum im Sinne des Urheberrechts zu respektieren. Als Seminarteilnehmer/in erwerben Sie selbstverständlich das Recht, alle vermittelten Methoden und Konzepte selbst anzuwenden (Nutzungsbewilligung), nicht aber das Recht, diese in organisierter Form weiterzuvermitteln. Auch die Vervielfältigung der Unterlagen und Dateien, die kein veröffentlichtes Werk darstellt, ist nicht gestattet. Ohne schriftliche Genehmigung von Christof Tschohl dürfen weder die Unterlagen selbst noch einzelne Informationen daraus reproduziert oder an Dritte weitergegeben werden.

**Disclaimer:**

Dieses Dokument wurde auf Basis jener Informationen erstellt, die dem Autor als für den Zweck des Dokuments relevant erschienen. Der Autor übernimmt jedoch keine Haftung/Gewähr für Vollständigkeit und Richtigkeit der in diesem Dokument zur Verfügung gestellten Informationen. Die Angaben in diesem Dokument können von dem Empfänger nicht als Zusicherung oder Garantie verstanden werden. Die in diesem Dokument enthaltenen Informationen können sich im Laufe der Zeit verändern oder zum Übergabezeitpunkt bereits verändert haben. Technische Änderungen vorbehalten.

Kontakt Daten: [heidi.scheichenbauer@researchinstitute.at](mailto:heidi.scheichenbauer@researchinstitute.at)