

# Der neue EU AI Act und mögliche Folgen für das geistigen Eigentum

Prof. Dr. Christian Heinze, LL.M. (Cambridge)

Institut für deutsches und europäisches Gesellschafts- und Wirtschaftsrecht

Ruprecht-Karls-Universität Heidelberg

# Nowy AI Act i możliwe konsekwencje dla własności intelektualnej

Prof. Dr. Christian Heinze, LL.M. (Cambridge)

Instytut Niemieckiego i Europejskiego Prawa Spółek i Prawa Gospodarczego

Uniwersytet Ruprechta i Karola w Heidelbergu



# KI-Regulierung – status quo

- Status quo
  - Patentrecht
    - Patentierbarkeit (EPA RL G II 3.3.1; EPA T 0702/20, GRUR-RS 2022, 40533)
    - KI als Erfinder (BPatG GRUR 2022, 1213 – Food Container; EPA J 0009/20, GRUR-RS 2021, 55794); KI und Durchschnittsfachmann
    - Patentverletzung durch Entwicklung, Anwendung und Verbreitung von KI (Heinze FS Taeger (2020) 663)
    - Praktische Folgen durch Einsatz von KI für die Abfassung von Patenten und die Suche nach Patentverletzungen
  - Urheberrecht:
    - § 44a UrhG, Rechtsverletzung durch Ausgaben generativer KI, Schutz von KI-Erzeugnissen, Zurechnungsfragen
  - DSGVO:
    - Trainingsdaten, Nutzereingaben, Richtigkeit der Ausgaben, Informationspflichten
  - Allgemeines Persönlichkeitsrecht
  - Sektoriell Produkt sicherheitsrecht
  - Sonstiges
    - BVerfG 1 BvR 1547/19 und 1 BvR 2634/20: predictive policing

# Regulacje dotyczące AI – status quo

- Status quo
  - Prawo patentowe
    - Zdolność patentowa (EPA RL G II 3.3.1; EPA T 0702/20, GRUR-RS 2022, 40533)
    - AI jako wynalazca (BPatG GRUR 2022, 1213 – Food Container; EPA J 0009/20, GRUR-RS 2021, 55794); AI i przeciętny fachowiec
    - Naruszenie patentu poprzez rozwijanie, stosowanie i rozpowszechnianie AI (Heinze FS Taeger (2020) 663)
    - Praktyczne konsekwencje wykorzystania AI do opracowywania patentów i wyszukiwania naruszeń patentów
  - Prawo autorskie:
    - § 44a UrhG, naruszenie prawa przez wyniki generatywnej sztucznej inteligencji, ochrona produktów AI, kwestie przypisania
  - RODO:
    - Dane treningowe, dane wprowadzane przez użytkowników, prawidłowość wyników, obowiązki informacyjne
  - Ogólne dobra osobiste
  - Sektorowe prawo bezpieczeństwa produktów
  - Pozostałe
    - BVerfG 1 BvR 1547/19 i 1 BvR 2634/20: predictive policing

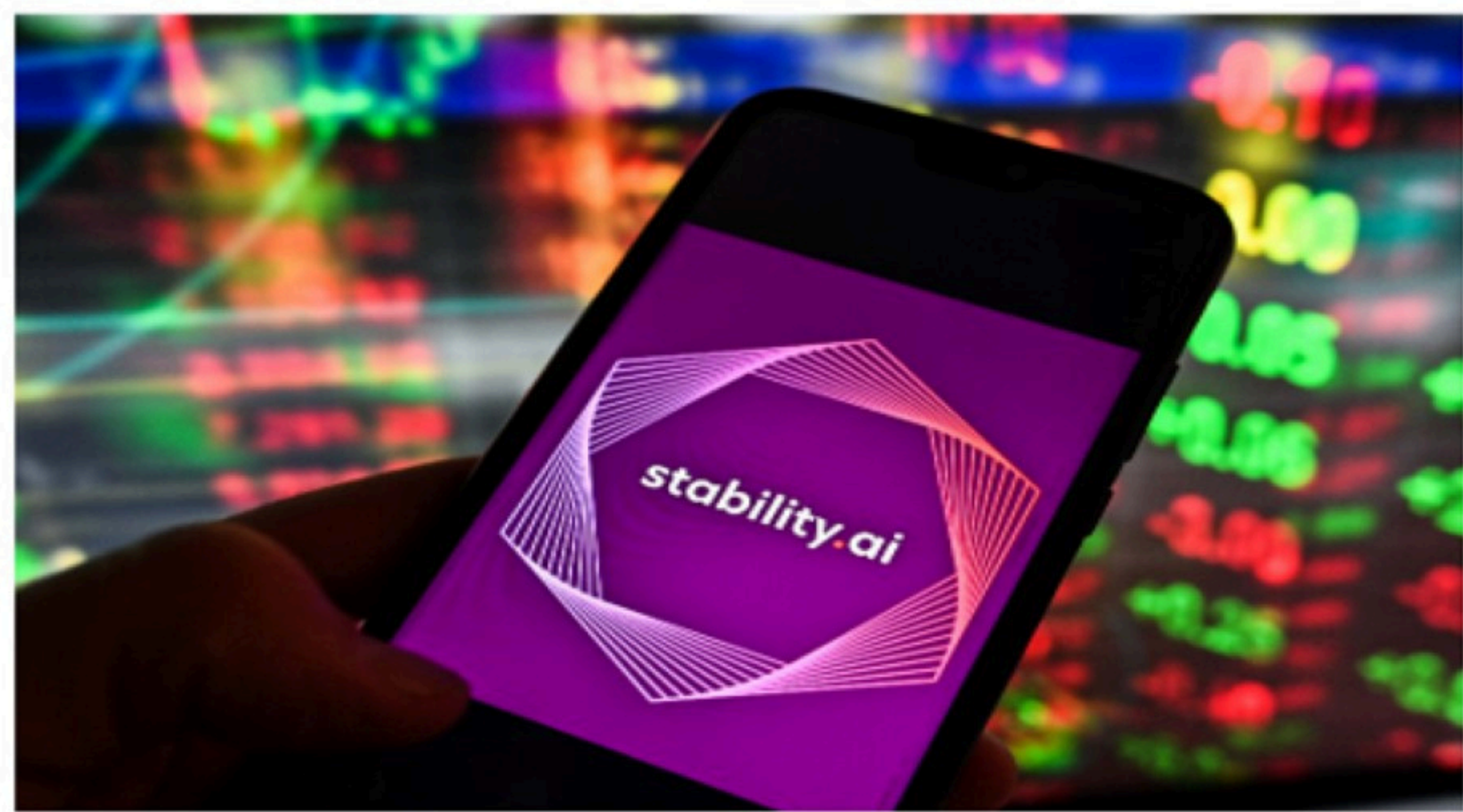


[home](#) • [artnews](#) • [news](#)

# Getty Images Sues Stability AI Over Photos Used to Train Stable Diffusion Image Generator

BY [KAREN K. HO](#)  February 7, 2023 2:17pm

[f](#) [t](#) [i](#) [p](#) [+](#)



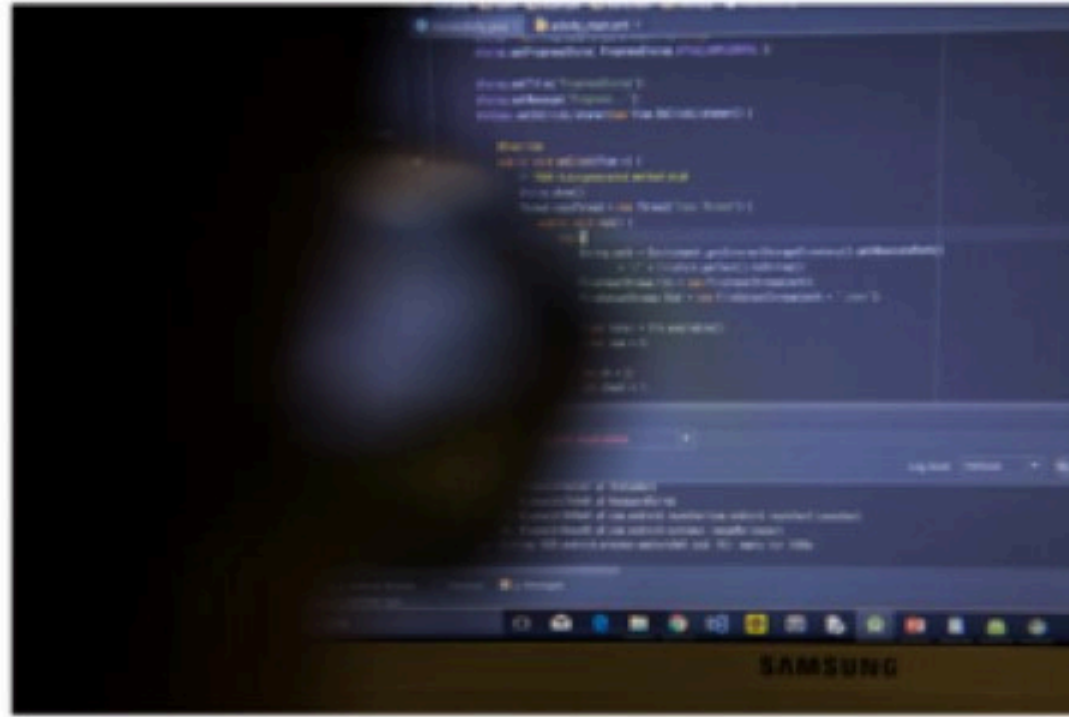
ADVERTISEMENT

Getty Images is suing Stability AI Inc., accusing it of copying more than 12 million photographs from its collection. PHOTO ILLUSTRATION BY OMAR MARQUES/SOPA IMAGES/LIGHTROCKET VIA GETTY IMAGES





# The lawsuit that could rewrite the rules of AI copyright



The key question in the lawsuit is whether open-source code can be reproduced by AI without attached licenses. Credit: Getty Images

/ Microsoft, GitHub, and OpenAI are being sued for allegedly violating copyright law by reproducing open-source code using AI. But the suit could have a huge impact on the wider world of artificial intelligence.

By JAMES VINCENT

Nov 8, 2022, 5:09 PM GMT+1 | 9 Comments / 9 New



Microsoft, its subsidiary GitHub, and its business partner OpenAI have been targeted in a proposed class action lawsuit alleging that the companies' creation of AI-powered coding assistant GitHub Copilot relies on "software piracy on an unprecedented scale." The case is only in its earliest stages but could have a huge effect on the broader world of AI, where companies are making fortunes training software on copyright-protected data.

Copilot, which was unveiled by Microsoft-owned GitHub in June 2021, is trained on public repositories of code scraped from the web, many of which are published with licenses that require anyone reusing the code to credit its creators. Copilot has been found to regurgitate long sections of licensed code without providing credit — prompting this





Caption	Brief Description	Algorithm	Jurisdiction	Application Areas	Cause of Action	Issues	Date Action Filed
<a href="#">Raw Story Media, Inc. v. OpenAI Inc.</a>	Raw Story, America's largest independent progressive news site, filed suit against OpenAI for using thousands of Raw Story's news articles to train ChatGPT in violation of the Digital Millennium Copyright Act.	ChatGPT	District Court, S.D. New York	Copyright, Generative AI, Natural Language Processing	Copyright Infringement, 17 U.S.C. 1202 Removal of Copyright Management Information, Digital Millennium Copyright Act	Infringement, Copyright Infringement	2/28/24 <a href="#">Data Table</a>
<a href="#">The Intercept Media, Inc. v. OpenAI, Inc.</a>	Several prominent news organizations, including The Intercept, have filed lawsuits against OpenAI in a New York federal court. The suits allege that OpenAI, backed by Microsoft, has unlawfully utilized its articles to train its popular AI chatbot, ChatGPT.	ChatGPT	District Court, S.D. New York	Copyright, Generative AI, Intellectual Property, Natural Language Processing	Copyright Infringement, 17 U.S.C. 1202 Removal of Copyright Management Information, Digital Millennium Copyright Act	Infringement, Copyright Infringement	2/28/24
<a href="#">Main Sequence, Ltd. v. Dudesy, LLC</a>	The estate of George Carlin sued a pair of podcasters for using artificial intelligence to create a script and voice imitating the late comedian for a new comedy routine, citing the right of publicity and copyright infringement.		US District Court for the Central District of California	Copyright, Generative AI, Infringement, Intellectual Property	Copyright Infringement, Permanent Injunction, Preliminary Injunction, Right to Publicity, Right of Publicity	Infringement, Copyright Infringement	
<a href="#">Basbanes v. Microsoft Corporation</a>	OpenAI and its financial backer Microsoft (MSFT.O), were sued on Jan 5, 2024, in Manhattan federal court by a pair of nonfiction authors who say the companies misused their work to train the artificial-intelligence models behind the popular chatbot ChatGPT and other AI-based services.  Writers Nicholas Basbanes and Nicholas Gage told the court in a proposed class action, that the companies infringed their copyrights by including several of their books as part of the data used to train OpenAI's GPT large language model.		US District Court for the Southern District of New York	Copyright, Generative AI, Infringement, Intellectual Property	Copyright Infringement	Copyright Infringement	
<a href="#">Andersen v. Stability AI Ltd.</a>	Three artists file class action lawsuit alleging copyright infringement, violation of rights of publicity, and other causes of action based on use of their visual art as training data for an artificial intelligence image	Stable Diffusion	Federal: US Dist. Ct. N.D. Ca.	Copyright, Generative AI, Intellectual Property	Copyright Infringement, Unfair Competition, Right of Publicity, 17 U.S.C. 1202 Removal of Copyright Management	Misuse of AI	3/13/24

<https://blogs.gwu.edu/law-eti/ai-litigation-database/>



ChatGPT Has a Big Privacy Problem

https://www.wired.co.uk/article/italy-ban-chatgpt-privacy-gdpr

http--www.ebay-kl...GMX Suche - die S...Vorgeschlagene SitesBookmarkletDBIS: Alphabetisch...s&p 500 - Google S...EZ9 Zeitschriftensuche |...Weitere Favoriten

WIRED


LONG READSBUSINESSCULTUREGEARSCIENCESECURITYVIDEO

SUBSCRIBE

MATT BURGESSSECURITY04.04.2023 05:00 PM

# ChatGPT Has a Big Privacy Problem


Italy's recent ban of Open AI's generative text tool may just be the beginning of ChatGPT's regulatory woes.



PHOTOGRAPH: BADAHD/GETTY IMAGES

18°C  
Stark bewölkt

Suche



DEU

17:08  
27/04/2023







# Der Kommissionsvorschlag für den AI Act



- **April 2021:** Vorschlag der EU Kommission für einen **Artificial Intelligence Act** – **AI Act COM(2021) 206**
- Ziel: **safe and trustworthy use of data and AI** (*“ecosystem of trust”*) und gleichzeitig Förderung von Innovation in der EU
- Schaffung einheitlicher Regeln im Binnenmarkt für Angebot und Nutzung von KI-Systemen
- **Horizontaler Ansatz** = nicht sektorbezogen
- Teil einer umfassenderen Strategie der EU zur Digitalregulierung

## Wniosek Komisji dotyczący AI Act




- **Kwiecień 2021:** Wniosek Komisji Europejskiej dotyczący **Ustawy o sztucznej inteligencji – Artificial Intelligence Act, AI Act COM(2021) 206**
- Cel: **bezpieczne i godne zaufania wykorzystanie danych oraz AI** (*„ekosystem zaufania”*) przy jednoczesnym wspieraniu innowacji w UE
- Stworzenie znormalizowanych zasad na rynku wewnętrznym w zakresie dostarczania i użytkowania systemów AI
- **Podejście horyzontalne** = niezwiązane z sektorami
- Część szerszej strategii UE w zakresie regulacji cyfrowych



# EU AI Act: Gesetzgebungsverfahren

Europäisches Parlament  
2019-2024



ANGENOMMENE TEXTE

P9\_TA(2024)0138

**Gesetz über künstliche Intelligenz**

Legislative Entschließung des Europäischen Parlaments vom 13. März 2024 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

Das Europäische Parlament,

- unter Hinweis auf den Vorschlag der Kommission an das Europäische Parlament und den Rat (COM(2021)0206),
- gestützt auf Artikel 294 Absatz 2 sowie Artikel 16 und Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, auf deren Grundlage ihm der Vorschlag der Kommission unterbreitet wurde (C9-0146/2021),
- gestützt auf Artikel 294 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union,
- unter Hinweis auf die Stellungnahme der Europäischen Zentralbank vom 29. Dezember 2021<sup>1</sup>,
- nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 22. September 2021<sup>2</sup>,
- unter Hinweis auf die vorläufige Einigung, die gemäß Artikel 74 Absatz 4 seiner Geschäftsordnung von den zuständigen Ausschüssen angenommen wurde und auf die

22.9., 2.12. and 29.12.2022: Stellungnahmen des Wirtschafts- und Sozialausschusses, des Ausschusses der Regionen und der EZB

Seit April 2022: Beratungen im Rat der European Union


- Erhebliche Änderungen des Kommissionsvorschlags.
- General approach des Rats vereinbart am 6.12.2022, Council document 15698/22.

22.5./14.6.2023: Report A9-0188/2023 im EU-Parlament.

13.4.2024: Abschluss des Trilogs mit legislativer Entschließung des EP

# Unijny AI Act: Procedura ustawodawcza

Europäisches Parlament  
2019-2024



ANGENOMMENE TEXTE

P9\_TA(2024)0138

**Gesetz über künstliche Intelligenz**

Legislative Entschließung des Europäischen Parlaments vom 13. März 2024 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

Das Europäische Parlament,

- unter Hinweis auf den Vorschlag der Kommission an das Europäische Parlament und den Rat (COM(2021)0206),
- gestützt auf Artikel 294 Absatz 2 sowie Artikel 16 und Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, auf deren Grundlage ihm der Vorschlag der Kommission unterbreitet wurde (C9-0146/2021),
- gestützt auf Artikel 294 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union,
- unter Hinweis auf die Stellungnahme der Europäischen Zentralbank vom 29. Dezember 2021<sup>1</sup>,
- nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 22. September 2021<sup>2</sup>,
- unter Hinweis auf die vorläufige Einigung, die gemäß Artikel 74 Absatz 4 seiner Geschäftsordnung von den zuständigen Ausschüssen angenommen wurde und auf die

22.9., 2.12. i 29.12.2022: Stanowiska Komitetu Ekonomiczno-Społecznego, Komitetu Regionów i EBC

Od kwietnia 2022 r.: Dyskusje w Radzie Unii Europejskiej

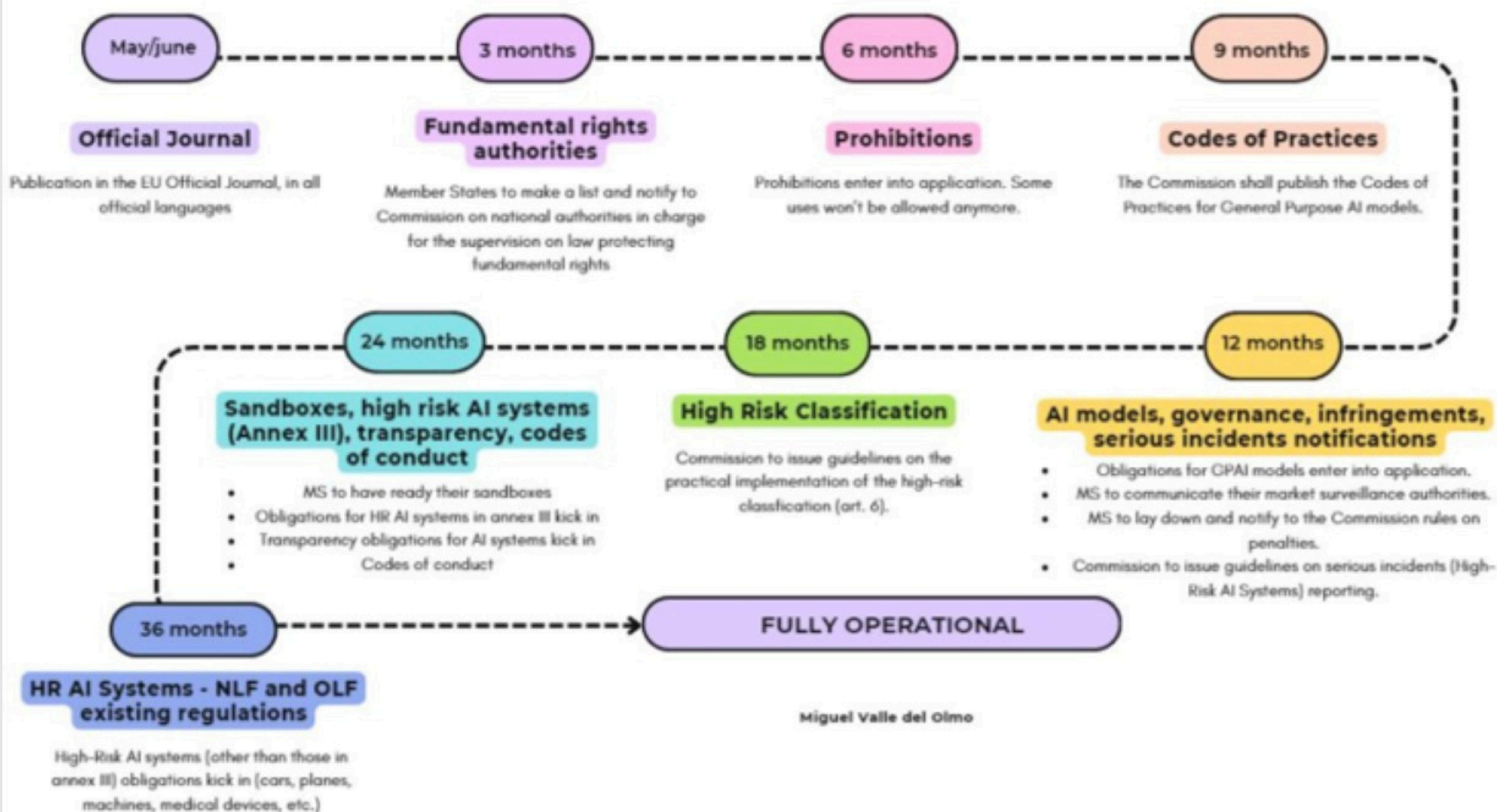
- Istotne zmiany w stosunku do wniosku Komisji.
- Podejście ogólne Rady uzgodnione dnia 06.12.2022 r., dokument Rady 15698/22.

22.5./14.6.2023: Sprawozdanie A9-0188/2023 w Parlamencie Europejskim.

13.4.2024: Zakończenie rozmów trójstronnych rezolucją legislacyjną PE



# AIA Timeline - some important tasks





# Überblick über den AI Act

- **Struktur:**
  - **Kapitel I: Allgemeine Bestimmungen (Art. 1-4), v.a. Anwendungsbereich und Definitionen**
  - **Kapitel II: Verbotene Praktiken (Art. 5)**
  - **Kapitel III: Hochrisiko-KI-Systeme**
    - Einstufung als Hochrisiko-System (Art 6-7)
    - Anforderungen an Hochrisiko-KI-Systeme (Art 8-15)
    - Pflichten der Anbieter, Betreiber, Importeure und Händler von Hochrisiko-KI-Systemen (Art 16-27)
    - Notifizierende Behörden (Konformitätsbewertungsstellen) und notifizierte Stellen (Art 28-39)
    - Normen, Konformitätsbewertung, Bescheinigungen, Registrierung (Art. 40-49)
  - **Kapitel IV: Transparenzpflichten für Anbieter und Nutzer bestimmter KI-Systeme (Art. 50)**
  - **Kapitel V: KI-Modelle mit allgemeinem Verwendungszweck (Art. 51-56)**
  - **Kapitel VI: Maßnahmen zur Innovationsförderung (Art 57-63)**
  - **Title VII-IX: Governance, EU-Datenbank for Hochrisiko-KI-Systeme, Beobachtung nach dem Inverkehrbringen, Informationsaustausch, Marktüberwachung (Art. 64-94)**
  - **Title X: Verhaltenskodizes und Leitlinien (Art. 95-96)**
  - **Title XI-XII: Befugnisübertragung und Ausschussverfahren (Art. 97-98), Sanktionen (Art. 99-101), Schlussbestimmungen (Art. 102-113)**

## Ustawa o sztucznej inteligencji w skrócie

- **Struktura:**
  - **Rozdział I: Postanowienia ogólne (art. 1-4), w szczególności zakres stosowania i definicje**
  - **Rozdział II: Zakazane praktyki (art. 5)**
  - **Rozdział III: Systemy AI wysokiego ryzyka**
    - Klasyfikacja jako system wysokiego ryzyka (art. 6-7)
    - Wymogi dotyczące systemów AI wysokiego ryzyka (art. 8-15)
    - Obowiązki dostawców, podmiotów stosujących, importerów i dystrybutorów systemów AI wysokiego ryzyka (art. 16-27)
    - Organy notyfikujące (jednostki oceniające zgodność) i jednostki notyfikowane (art. 28-39)
    - Normy, ocena zgodności, certyfikaty, rejestracja (art. 40-49)
  - **Rozdział IV: Obowiązki w zakresie przejrzystości dla dostawców i użytkowników niektórych systemów AI (art. 50)**
  - **Rozdział V: Modele AI ogólnego przeznaczenia (art. 51-56)**
  - **Rozdział VI: Środki wspierające innowacje (art. 57-63)**
  - **Tytuł VII-IX: Zarządzanie, unijna baza danych systemów AI wysokiego ryzyka, monitorowanie po wprowadzeniu do obrotu, wymiana informacji, nadzór rynku (art. 64-94)**
  - **Tytuł X: Kodeksy postępowania i wytyczne (art. 95-96)**
  - **Tytuł XI-XII: Przekazanie uprawnień i procedura komitetowa (art. 97-98), sankcje (art. 99-101), przepisy końcowe (art. 102-113)**



# AI Act als Teil der EU-Digitalregulierung (Ausschnitt)

Geistiges Eigentum	Sicherheit	Datenschutz und Datenwirtschaft	E-Commerce & Verbraucherschutz	Plattformen
Standardessentielle Patente, 2023/0133 (COD) Zwangslizenzen, 2023/0129 (COD)	Produkthaftung RL 85/374 (Reform: 2022/0302 COD)	DSGVO 2016/679; E-Privacy-RL 2002/58 (2017/0003 (COD)); Health Data Space (2022/0140)	UGP-RL 2005/29 mit Reform	P2B-VO 2019/1150
Urheberrecht, zB RL 96/9; RL 2009/24; RL 2019/790	Produktsicherheit VO 2023/988	Freizügigkeit von Daten: VO 2018/1807	Verbraucherrechte RL 2011/83	Digital Market Act VO 2022/1925
Rechtsdurchsetzung: RL 2004/48	MaschinenVO 2023/1230	Open-Data-RL 2019/1024	DigitalgüterRL+ Warenkauf 2019/770 + 2019/771	Digital Services Act VO 2022/2065
Geschäftsgeheimnisse RL 2016/679	AI Act 2021/0106 COD + AI Liability 2022/0303 COD	Data Governance Act, VO 2022/868	Politische Werbung 2021/0381 COD	Crypto-Assets VO 2023/1114 (MiCar)
EU Design VO 6/2002 + RL 98/71 (Reform)	Öko-Design VO 2022/0095 COD	Data Act, 2022/0140 (COD)	Recht auf Reparatur RL 2023/0083 COD	Media Freedom Act 2022/0277 COD

## Ustawa o sztucznej inteligencji jako część regulacji cyfrowych UE (fragment)

Prawa własności intelektualnej	Bezpieczeństwo	Ochrona danych i gospodarowanie danymi	E-Commerce i ochrona konsumentów	Platformy
Standardowe niezbędne patenty, 2023/0133 (COD) Licencje przymusowe, 2023/0129 (COD)	Dyrektywa w sprawie odpowiedzialności za produkt 85/374 (Reforma: 2022/0302 COD)	RODO 2016/679; Dyrektywa o prywatności i łączności elektronicznej 2002/58 (2017/0003 (COD)); Health Data Space (2022/0140)	Dyrektywa dotycząca nieuczciwych praktyk handlowych 2005/29 z reformą	Rozporządzenie P2B 2019/1150
Prawo autorskie, np. dyrektywa 96/9; dyrektywa 2009/24; dyrektywa 2019/790	Rozporządzenie w sprawie bezpieczeństwa produktów 2023/988	Swobodny przepływ danych: rozporządzenie 2018/1807	Prawa konsumentów dyrektywa 2011/83	Digital Market Act rozporządzenie 2022/1925
Egzekwowanie prawa: dyrektywa 2004/48	Rozporządzenie w sprawie maszyn 2023/1230	Dyrektywa w sprawie otwartych danych 2019/1024	Dyrektywa w sprawie treści i usług cyfrowych + Zakup towarów 2019/770 + 2019/771	Digital Services Act rozporządzenie 2022/2065
Tajemnice przedsiębiorstwa dyrektywa 2016/679	AI Act 2021/0106 COD + AI Liability 2022/0303 COD	Data Governance Act, rozporządzenie 2022/868	Reklama polityczna 2021/0381 COD	Rozporządzenie w sprawie rynków kryptoaktywów 2023/1114 (MiCar)
Wzory wspólnotowe rozporządzenie 6/2002 +	Ekoprojekt rozporządzenie	Data Act, 2022/0140 (COD)	Prawo do naprawy dyrektywa 2023/0083	Media Freedom Act 2022/0277 COD



# Ziel der KI-VO

- **Art. 1 Gegenstand**

- (1) Zweck dieser Verordnung ist es, das
- Funktionieren des Binnenmarkts zu verbessern und die
- Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen künstlichen Intelligenz (KI) zu fördern und
- gleichzeitig ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in der Charta der Grundrechte verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, vor schädlichen Auswirkungen von Systemen der künstlichen Intelligenz (KI-Systeme) in der Union zu gewährleisten und die
- Innovation zu unterstützen.

# Cel rozporządzenia AI

- **Art. 1 Przedmiot**

- (1) Celem niniejszego rozporządzenia jest
- poprawa funkcjonowania rynku wewnętrznego i
- promowanie upowszechniania zorientowanej na człowieka i godnej zaufania sztucznej inteligencji (AI),
- przy jednoczesnym zapewnieniu wysokiego poziomu ochrony zdrowia, bezpieczeństwa, praw podstawowych zapisanych w Karcie, w tym demokracji, praworządności i ochrony środowiska, przed szkodliwymi skutkami systemów AI w Unii oraz
- wspieraniu innowacji.



# Gegenstand der KI-VO

## • **Art. 1 Gegenstand**

- (2) In dieser Verordnung wird Folgendes festgelegt:
- a) harmonisierte Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen in der Union;
- b) Verbote bestimmter Praktiken im KI-Bereich;
- c) besondere Anforderungen an Hochrisiko-KI-Systeme und Pflichten für Akteure in Bezug auf solche Systeme;
- d) harmonisierte Transparenzvorschriften für bestimmte KI-Systeme;
- e) harmonisierte Vorschriften für das Inverkehrbringen von KI-Modellen mit allgemeinem Verwendungszweck;
- f) Vorschriften für die Marktbeobachtung sowie die Governance und Durchsetzung der Marktüberwachung;
- g) Maßnahmen zur Innovationsförderung mit besonderem Augenmerk auf KMU, einschließlich Start-up-Unternehmen.

# Przedmiot rozporządzenia AI

## • **Art. 1 Przedmiot**

- (2) W niniejszym rozporządzeniu ustanawia się:
- a) zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania systemów AI w Unii;
- b) zakazy dotyczące niektórych praktyk w zakresie AI;
- c) szczególne wymogi dotyczące systemów AI wysokiego ryzyka oraz obowiązki spoczywające na operatorach takich systemów;
- d) zharmonizowane przepisy dotyczące przejrzystości w przypadku niektórych systemów AI;
- e) zharmonizowane przepisy dotyczące wprowadzania do obrotu modeli AI ogólnego przeznaczenia;
- f) przepisy dotyczące monitorowania wprowadzania do obrotu oraz zarządzania i egzekwowania nadzoru rynku;
- g) środki wspierające innowacje, ze szczególnym uwzględnieniem MŚP, w tym przedsiębiorstw typu start-up.



# Was wird geregelt? – Anwendungsbereich: Position von KOM und Rat

- **KI-Systeme (Art 3(1))**

- KOM Vorschlag hatte eine weite Definitionsliste mit unterschiedlichen Technologien: Machine Learning, logic- & knowledge-based approaches, statistical approaches such as Bayesian methods). Abgrenzung zu Software wurde als unklar kritisiert.
- Der Rat sprach sich für eine engere Definition aus:
- „‘artificial intelligence system’ (AI system) means a system that is [1] **designed to operate with elements of autonomy** and that, [2] **based on machine and/or human-provided data and inputs**, [3] **infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches**, and [4] **produces** system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, **influencing the environments** with which the AI system interacts”.
- Im Kern vier Kriterien: (1) elements of autonomy, (2) based on data and inputs, (3) infers how to achieve objectives using ML or logic-/knowledge based approaches, (4) produces system-generated outputs which influences environment.

# Co podlega regulacji – Zakres stosowania: Stanowisko Komisji i Rady

- **Systemy AI (Art. 3(1))**

- Wniosek Komisji posiadał szeroką listę definicji obejmujących różne technologie: uczenie maszynowe, podejścia oparte na logice i wiedzy, podejścia statystyczne, takie jak metody bayesowskie). Odgraniczenie od oprogramowania zostało skrytykowane jako niejasne.
- Rada opowiedziała się za węższą definicją:
- „‘system sztucznej inteligencji’ (system AI) oznacza system, który został [1] **zaprojektowany do działania z elementami autonomii** i który, [2] **w oparciu o dane i informacje wejściowe dostarczone przez maszynę i/albo człowieka**, [3] **wnioskuje, jak osiągnąć dany zestaw celów przy użyciu uczenia maszynowego i/albo podejść opartych na logice i wiedzy**, a także [4] **produkuje** generowane przez system dane wyjściowe, takie jak treść (generatywna AI), predykcje, zalecenia lub decyzje, **wpływając na środowisko**, z którym system AI wchodzi w interakcje”.
- Zasadniczo cztery kryteria: (1) elementy autonomii, (2) w oparciu o dane i informacje wejściowe, (3) wnioskuje, jak osiągnąć cele przy użyciu ML lub podejść opartych na logice/wiedzy, (4) produkuje generowane przez system dane wyjściowe, które wpływają na środowisko.



# Anwendungsbereich: Position des Parlaments

- **Was? AI systems (Art 3(1))**

- Parlament schlug eine kürzere Definition vor:
- 'artificial intelligence system' (AI system) means a machine-based system that is [1] designed to operate with varying levels of autonomy and that can, [2] for explicit or implicit objectives, [3] generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments.
- The notion of AI system in this Regulation [...] it should be based on key characteristics of artificial intelligence, such as its learning, reasoning or modelling capabilities, so as to distinguish it from simpler software systems or programming approaches.
- AI systems are designed to operate with varying levels of autonomy, meaning that they have at least some degree of independence of actions from human controls and of capabilities to operate without human intervention.

# Zakres stosowania: Stanowisko Parlamentu

- **Co? Systemy AI (art. 3(1))**

- Parlament zaproponował krótszą definicję:
- 'system sztucznej inteligencji' (system AI) oznacza system maszynowy, który został [1] zaprojektowany do działania z różnym poziomem autonomii i który może, [2] na potrzeby wyraźnych lub dorozumianych celów, [3] generować wyniki, takie jak predykcje, zalecenia lub decyzje, które wpływają na środowisko fizyczne lub wirtualne.
- Pojęcie systemu sztucznej inteligencji w niniejszym Rozporządzeniu [...] powinno opierać się na kluczowych cechach charakterystycznych sztucznej inteligencji, takich jak zdolność uczenia się, rozumowania lub modelowania, aby odróżnić ją od prostszych systemów oprogramowania lub założeń programistycznych.
- Systemy AI są zaprojektowane do działania na różnych poziomach autonomii, co oznacza, że wyróżnia je co najmniej  pewien stopień niezależności  działań od kontroli człowieka oraz możliwości działania bez jego interwencji.



# Anwendungsbereich: Finale Verordnung

- **Was ist ein KI-System?** (Art. 3 Nr. 1 und ErwG 12 AI Act)
  - (1) **maschinengestütztes** System,
  - (2) das für einen in wechselndem Maße **autonomen Betrieb** ausgelegt sind [sic],
    - System kann bis zu einem gewissen Grad unabhängig von menschlichem Zutun agieren und ist in der Lage, ohne menschliches Eingreifen zu arbeiten
  - (3) das nach seiner Einführung **anpassungsfähig** sein kann und das
    - System kann sich während seiner Verwendung verändern
  - (4) aus den erhaltenen **Eingaben** für explizite oder implizite Ziele **ableitet**, wie Ergebnisse wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen hervorgebracht werden, die physische oder virtuelle Umgebungen beeinflussen können.
    - Prozess des Erhalts von Ergebnissen, ... die physische und virtuelle Umgebungen beeinflussen können, sowie die Fähigkeit von KI-Systemen, Modelle oder Algorithmen aus Eingaben oder Daten abzuleiten.
- Vgl. EPA-Richtlinien G II 3.3.1 KI und maschinelles Lernen
  - „Künstliche Intelligenz und maschinelles Lernen basieren auf Rechenmodellen und Algorithmen zur Klassifizierung, Bündelung, Regression und Dimensionalitätsreduktion wie zum Beispiel neuronalen Netzen, genetischen Algorithmen, Support Vector Machines, k-Means, Kernel-Regression und Diskriminanzanalyse“.

## Zakres stosowania: Rozporządzenie finalne

- **Czym jest system AI?** (art. 3 nr 1 i motyw 12 AI Act)
  - (1) system **maszynowy**,
  - (2) który został zaprojektowany do działania z różnym poziomem **autonomii** [sic],
    - System jest w pewnym stopniu niezależny od zaangażowania ze strony człowieka i zdolny do działania bez interwencji człowieka
  - (3) który może wykazywać **zdolność adaptacji** po jego wdrożeniu, i który
    - System może ulec zmianie w czasie jego wykorzystywania
  - (4) na potrzeby wyraźnych lub dorozumianych celów **wnioskuje** na podstawie otrzymanych **informacji wejściowych**, jak generować wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne.”
    - Proces uzyskiwania wyników, ... które mogą wpływać na środowisko fizyczne i wirtualne, a także zdolność systemów AI do wnioskowania modeli lub algorytmów z informacji wejściowych lub danych.
- Por. Wytyczne EUP G II 3.3.1 AI i uczenie maszynowe
  - „Sztuczna inteligencja i uczenie maszynowe bazują na modelach obliczeniowych i algorytmach klasyfikacji, grupowania, regresji i redukcji wymiarowości, takich jak przykładowo sieci neuronowe, algorytmy genetyczne, maszyny wektorów nośnych (Support Vector Machines), k-średnie, regresja jądrowa i analiza dyskryminacyjna”.



# Anwendungsbereich: Finale Verordnung

- **Keine KI** sind (ErwG 12):
  - Herkömmliche Softwaresysteme und Programmierungsansätze,
  - Systeme, die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen
    - Klassische Wenn-Dann-Programmierung
  - Einfache Datenverarbeitung.

## Zakres stosowania: Rozporządzenie finalne

- **AI nie** stanowią (motyw 12):
  - Tradycyjne systemy oprogramowania i założenia programistyczne,
  - Systemy oparte na zasadach określonych wyłącznie przez osoby fizyczne w celu automatycznego wykonywania operacji
    - Klasyczne programowanie z zastosowaniem instrukcji warunkowej
  - Proste przetwarzanie danych.



# Anwendungsbereich: Finale Verordnung

- **KI ist (ErwG 12):**
  - Maschinelles Lernen, v.a. künstliche neuronale Netze: beaufsichtigtes, unbeaufsichtigtes und bestärkendes Lernen einschließlich des tiefen Lernens (Deep Learning)
    - „Datengetriebene KI“
  - Logik- und wissensgestützte Konzepte, bei denen aus kodierten Informationen oder symbolischen Darstellungen Schlüsse für die zu lösende Aufgabe abgeleitet werden:
    - Wissensbasierte Systeme/Expertensysteme/explicite Repräsentation von Wissen: „Wissensbasierte KI“
  - Nicht klar ist, ob auch Mustererkennung durch statistische Verfahren noch als KI anzusehen ist (im COM-Vorschlag noch als dritte Kategorie erwähnt)
    - Beispiel: Regressionsanalyse aus vorhandenen Datenpunkten, aus denen ein Modell (eine Regressionsgrade) abgeleitet wird, mit deren Hilfe auch die Eigenschaften bisher unbekannter Datenpunkte prognostiziert werden können.
    - Zwar ist dies eine Form der Modellierung.
    - Aber im Unterschied zum KOM-Vorschlag nicht mehr als Technik der KI erwähnt.

## Zakres stosowania: Rozporządzenie finalne

- **AI to (motyw 12):**
  - Uczenie maszynowe, przede wszystkim sztuczne sieci neuronowe: nadzorowane, nienadzorowane i wzmocnione uczenie, w tym uczenie głębokie (Deep Learning)
    - „AI oparta na danych”
  - Koncepcje oparte na logice i wiedzy, które polegają na wnioskowaniu na podstawie zakodowanej informacji lub symbolicznego przedstawienia zadania, które należy rozwiązać:
    - Systemy oparte na wiedzy/systemy eksperckie/wyraźna reprezentacja wiedzy: „AI oparta na wiedzy”
  - Nie jest jasne, czy rozpoznawanie wzorców przy użyciu metod statystycznych również powinno być traktowane jako AI (we wniosku Komisji wymieniane jeszcze jako trzecia kategoria)
    - Przykład: Analiza regresji na podstawie istniejących punktów danych, z których wyprowadzany jest model (linia regresji), za pomocą którego można przewidywać również właściwości nieznanymi dotychczas punktów danych.
    - Jest to w istocie forma modelowania.
    - Jednak w odróżnieniu od wniosku Komisji, nie jest już wymieniana jako technologia AI.



# Bewertung

- **Begriff des KI-Systems**

- Die Definition des Parlaments war weiter und ggf. technologieoffener. Andererseits war m.E. das einzige Abgrenzungskriterium zur „normalen“ Software die „autonomy“ („some degree of independence of actions from human control“).
- Die Bindung an Trainingsdaten und Inputs und die Begrenzung auf maschinelles Lernen und logik-/wissensbasierte Ansätze im Vorschlag des Rats war enger und präziser.
- Die finale Definition mit den Kern-Merkmalen „Autonomie“ und „Ableitung“ von Informationen/Modellen aus Daten sowie die beispielhafte Erwähnung zweier konkreter Verfahren (maschinelles Lernen und logik- bzw. wissensbasierte Konzepte) trifft den Kern der (aus Produktsicherheitsperspektive regelungsbedürftiger) KI-Verfahren, wobei die Abgrenzung von Expertensystemen und Datenbanken ggf. problematisch sein kann.

# Ocena

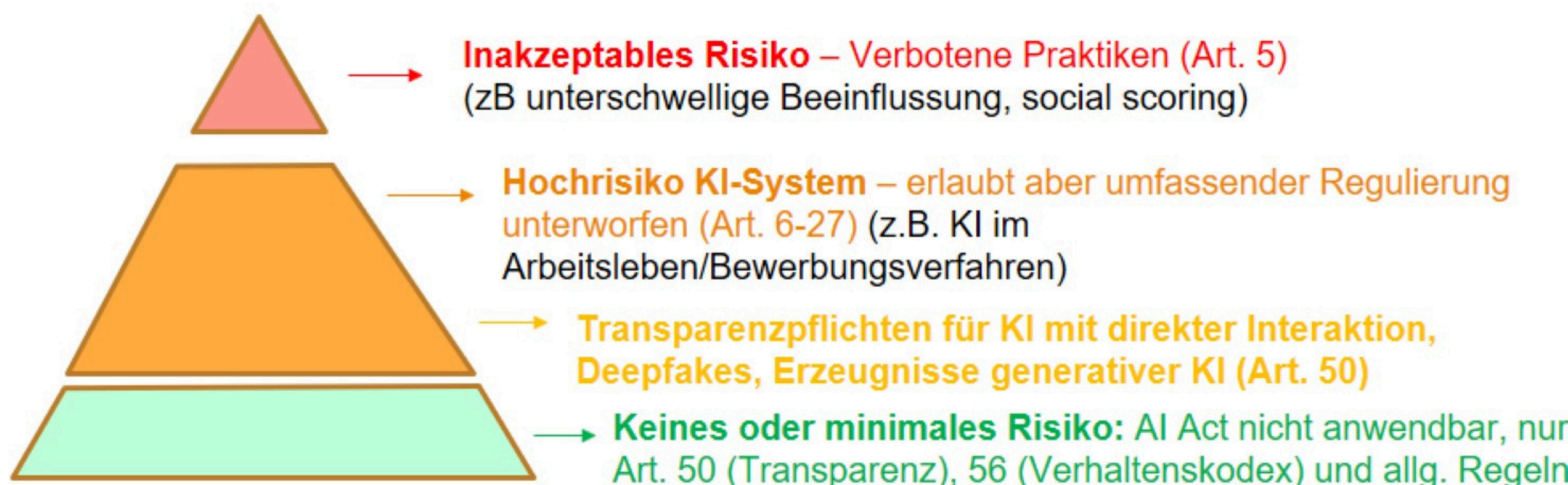
- **Pojęcie systemu AI**

- Definicja Parlamentu była szersza i być może bardziej otwarta na technologię. Z drugiej strony, moim zdaniem, jedynym kryterium odróżniającym ją od „normalnego” oprogramowania była „autonomia” („pewien stopień niezależności działań od ludzkiej kontroli”).
- Powiązanie z danymi treningowymi i informacjami wejściowymi oraz ograniczenie do uczenia maszynowego i podejść opartych na logice/wiedzy we wniosku Rady były węższe i bardziej precyzyjne.
- Ostateczna definicja z podstawowymi cechami „autonomii” i „wnioskowania” informacji/modeli z danych, a także przykładowa wzmianka o dwóch konkretnych procedurach (uczenie maszynowe i koncepcje oparte na logice lub wiedzy) trafia w samo sedno procedur AI (które z punktu widzenia bezpieczeństwa produktu wymagają uregulowania), przy czym rozróżnienie od systemów eksperckich i baz danych może okazać się problematyczne.



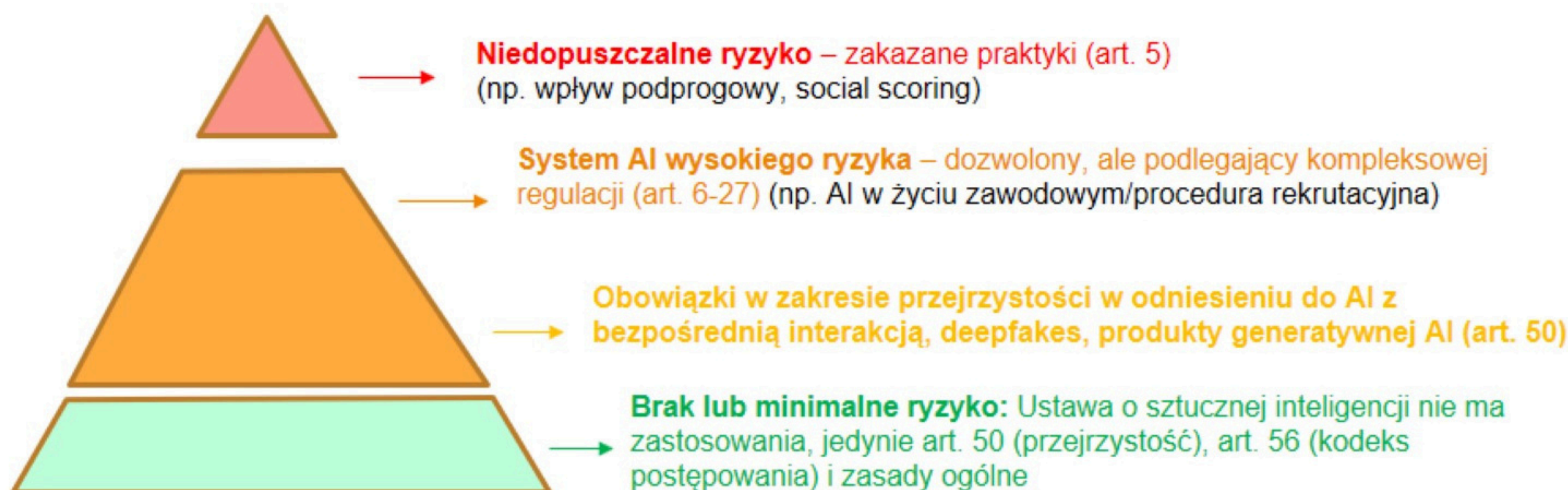
# Wie wird geregelt? – Ursprünglich: Risikobasierte Regulierung

- KOM-Vorschlag: Je höher das Risiko, desto strenger die Regeln.
- Keine Regulierung von KI als solcher, sondern nur konkreter Anwendungen.



## Sposób regulacji? – Początkowo: Regulacja w oparciu o ryzyko

- Wniosek Komisji: Im wyższe ryzyko, tym surowsze reguły.
- Brak regulacji dotyczących AI jako takiej, tylko regulacje dotyczące konkretnych zastosowań.





# KI-System mit allgemeinem Verwendungszweck (general purpose AI)

- Aufkommen von Large Language Models und anderen KI-Modellen mit allgemeinem Verwendungszweck wirft die Frage auf, wen die Pflichten aus der KI-VO treffen sollen:
  - Anbieter des allgemeinen KI-Modells oder
  - Betreiber, der das allgemeine KI-Modell für ein spezielles KI-System mit spezifischem (riskantem) Zweck nutzt?
- Ausgangspunkt (COM): Regulierung knüpft an Hochrisiko-Einsatz an.
- Erste Reform (Rat) (nach Aufkommen von ChatGPT 3.5): Regulierung von general purpose AI
- Zweiter Ansatz (Parlament): Regulierung von general purpose AI und foundation models

## System AI ogólnego przeznaczenia (general purpose AI)

- Pojawienie się dużych modeli językowych i innych modeli AI ogólnego przeznaczenia rodzi pytanie, kto powinien podlegać obowiązkom wynikającym z rozporządzenia AI:
  - Dostawca ogólnego modelu AI czy
  - Podmiot stosujący, wykorzystujący ogólny model AI dla konkretnego systemu AI w konkretnym (ryzykownym) celu?
- Stan wyjściowy (COM): Regulacja nawiązuje do wykorzystania obarczonego wysokim ryzykiem.
- Pierwsza reforma (Rada) (po pojawieniu się ChatGPT 3.5): Regulacja dotycząca sztucznej inteligencji ogólnego przeznaczenia
- Drugie podejście (Parlament): Regulacja dotycząca sztucznej inteligencji ogólnego przeznaczenia oraz modeli podstawowych (foundation models)



# KI-System mit allgemeinem Verwendungszweck (general purpose AI): Lösung des AI Act

- Art. 3 Nr. 66: „KI-System mit allgemeinem Verwendungszweck: KI-System, das auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen“
- Art. 3 Nr. 63: „KI-Modell mit allgemeinem Verwendungszweck“: KI-Modell (...), das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrer Markteinführung für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen verwendet werden;
  - EG 98: „Modelle mit mindestens einer Milliarde Parametern, die mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert werden, [gelten] als Modelle ..., die eine erhebliche allgemeine Verwendbarkeit aufweisen und ein breites Spektrum unterschiedlicher Aufgaben kompetent erfüllen“
  - Bsp: Große generative KI-Modelle (EG 99), da sie flexible Erzeugung von Inhalten ermöglichen
- EG 97: Unterschied KI-System und KI-Modell: KI-Modelle sind wesentliche Komponenten von KI-Systemen, aber keine KI-Systeme: „Damit KI-Modelle zu KI-Systemen werden, ist die Hinzufügung weiterer Komponenten, zum Beispiel einer Nutzerschnittstelle, erforderlich“.

## System AI ogólnego przeznaczenia (general purpose AI) Rozwiązanie ustawy o sztucznej inteligencji

- Art. 3 nr 66: „system AI ogólnego przeznaczenia” oznacza system AI oparty na modelu AI ogólnego przeznaczenia, który to system może służyć różnym celom, nadający się zarówno do bezpośredniego wykorzystania, jak i do integracji z innymi systemami AI;
- Art. 3 nr 63: „model AI ogólnego przeznaczenia”: model AI, (...), który wykazuje znaczną ogólność i jest w stanie kompetentnie wykonywać szeroki zakres różnych zadań, niezależnie od sposobu, w jaki model ten jest wprowadzany do obrotu, i który można zintegrować z różnymi systemami lub aplikacjami niższego szczebla – z wyłączeniem modeli AI, które są wykorzystywane na potrzeby działań w zakresie badań, rozwoju i tworzenia prototypów przed wprowadzeniem ich do obrotu;
  - Motyw 98: „(...) modele o co najmniej miliardzie parametrów i trenowane w oparciu o dużą ilość danych z wykorzystaniem nadzoru własnego na dużą skalę są bardzo ogólne i kompetentnie wykonują szeroki zakres różnych zadań.”
  - Np.: Duże generatywne modele AI (motyw 99), ponieważ umożliwiają elastyczne generowanie treści
- Motyw 97: Różnica między systemem AI a modelem AI: Modele AI są zasadniczymi komponentami systemów AI, ale nie są systemami AI: „Aby model AI mógł stać się systemem AI należy dodać do niego dodatkowe elementy, takie jak na przykład interfejs użytkownika.”



# KI-Modelle mit allgemeinem Verwendungszweck

- Finaler Text: Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck (Art. 53 Abs. 1 KI-VO):
  - a) erstellen und aktualisieren der Dokumentation des Modells,
  - b) Information und Dokumentation über Fähigkeiten des Systems für Anbieter, die das KI-System in ihre KI-Systeme integrieren
    - Muss Anbieter in die Lage versetzen, die Fähigkeiten und Grenzen des KI-Modells zu verstehen und ihren Pflichten nach der KI-VO nachzukommen, mindestens Ergebnis der Konformitätsbewertung
    - „unbeschadet“ des Schutzes geistigen Eigentums und von Geschäftsgeheimnissen
  - c) Strategie zur Einhaltung des Urheberrechts der Union, insbesondere zur Einhaltung des technischen Vorbehalts für Text und Data Mining
  - d) Zusammenfassung der Trainingsinhalte.
  - Abs. 2: Lit. a und b gelten nicht für Open Source Modelle, deren Parameter publik sind und keine systemischen Risiken begründen.
  - Abs. 4: Pflichten können bis zum Erlass einer harmonisierten Norm mit Verhaltenskodex Compliance nachweisen.
  - Abs. 7: Dokumentationen aufgrund von Art. 53 KI-VO unterliegen Vertraulichkeit.

## Modele AI ogólnego przeznaczenia

- Tekst finalny: Obowiązki dostawców modeli AI ogólnego przeznaczenia (art. 53 ust. 1 rozporządzenia AI):
  - a) sporządzanie i aktualizowanie dokumentacji modelu,
  - b) informowanie i dokumentowanie zdolności systemu dla dostawców, którzy zamierzają zintegrować system AI ze swoimi systemami AI
    - Musi umożliwiać dostawcom zrozumienie możliwości i ograniczeń modelu AI oraz wypełnianie ich obowiązków wynikających z rozporządzenia AI, co najmniej wynik oceny zgodności
    - „bez uszczerbku” dla ochrony praw własności intelektualnej i tajemnic przedsiębiorstwa
  - c) polityka służąca zapewnieniu zgodności z prawem autorskim UE, w szczególności zapewnieniu technicznego zastrzeżenia w odniesieniu do eksploracji tekstów i danych
  - d) sporządzanie streszczenia na temat treści wykorzystanych do trenowania.
  - Ust. 2: Lit. a) i b) nie stosuje się do modeli typu open source, których parametry są podawane do wiadomości publicznej, i które nie stanowią żadnego ryzyka systemowego.
  - Ust. 4: Do czasu opublikowania normy zharmonizowanej dostawcy mogą opierać się na kodeksach praktyk w celu wykazania zgodności.
  - Ust. 7: Dokumentacja oparta na art. 53 rozporządzenia AI podlega poufności.



# Bewertung: Regulierung von KI-Modellen mit allgemeinem Verwendungszweck

- Verzicht auf (ursprünglich vorgeschlagenes) Risikomanagementsystem sinnvoll, da Anbieter Einsatzumgebung nicht kennen wird (weitergehende Vorschläge von Rat und Parlament mit Recht nicht aufgegriffen)
- Richtig, den Einsatz von general purpose AI nur im konkreten Hochrisikokontext zu regulieren, also primär den die general purpose AI adaptierenden Anwender zu verpflichten („Aufrücken zum Hersteller“, vgl. Art. 25 KI-VO).
- Sinnvoll sind auch die Transparenz- und Informationspflichten des Anbieters von gpAI (ausgestaltet als zwingende Regeln) mit zugehöriger Dokumentation (Art. 25 KI-VO).
  - Das Ziel dieser Pflichten ist, dass Nutzer den Einsatz des KI-Systems in einer Hochrisiko-Umgebung nachvollziehen und gestalten können.
- Nicht ganz klar ist, wie die verbleibenden Pflichten des Erstanbieters zur Information und technischen Unterstützung (Art. 25 Abs. 2) und die schriftliche Vereinbarung zwischen Hochrisiko-KI-System-Betreiber und Komponentenanbieter (Art. 25 Abs. 4) ausgestaltet sein werden (strenger noch Art. 28a EP-Vorschlag: Klauselkontrolle). Mustervertragsbedingungen sind rein freiwillig.

## Ocena: Regulacje dotyczące modeli AI ogólnego przeznaczenia

- Rezygnacja z (pierwotnie proponowanego) systemu zarządzania ryzykiem jest słuszna, ponieważ dostawca nie będzie zaznajomiony ze środowiskiem zastosowania (dalej idące wnioski słusznie nie zostały podjęte przez Radę i Parlament)
- Słuszne jest uregulowanie wykorzystania AI ogólnego przeznaczenia tylko w określonych kontekstach wysokiego ryzyka, tj. w pierwszej kolejności nałożenie obowiązków na użytkownika dokonującego adaptacji AI ogólnego przeznaczenia („awans na producenta”, por. art. 25 rozporządzenia AI).
- Rozsądne są również obowiązki dostawcy gpAI w zakresie przejrzystości i informowania (przewidziane jako przepisy bezwzględnie obowiązujące) wraz z powiązaną dokumentacją (art. 25 rozporządzenia AI).
  - Celem tych obowiązków jest umożliwienie użytkownikom zrozumienia i zorganizowania korzystania z systemu AI w środowisku wysokiego ryzyka.
- Nie jest do końca jasne, w jaki sposób zostaną określone pozostałe obowiązki pierwotnego dostawcy w zakresie dostarczania informacji i wsparcia technicznego (art. 25 ust. 2) oraz pisemne porozumienie pomiędzy podmiotem stosującym system AI wysokiego ryzyka a dostawcą komponentu (art. 25 ust. 4) (bardziej rygorystyczny art. 28a wniosek PE): Kontrola klauzul). Warunki wzoru umowy są całkowicie dobrowolne.



# Was bedeutet Vertraulichkeit (Art. 78)?

- Richtet sich an Behörden und “alle anderen natürlichen oder juristischen Personen, die an der Anwendung dieser Verordnung beteiligt sind”.
- Vertraulichkeit der Informationen und Daten, in deren Besitz sie bei der Ausführung ihrer Aufgaben und Tätigkeiten gelangen, sodass insbesondere Folgendes geschützt ist:
  - Rechte des geistigen Eigentums sowie vertrauliche Geschäftsinformationen (Ausn.: Art. 5 RL 2016/953) oder
  - Durchführung der Verordnung, zB Inspektionen
  - Öffentliche und private Sicherheitsinteressen,
  - Durchführung von Straf- oder Verwaltungsverfahren,
  - Als Verschlusssache eingestufte Informationen.
- Nur Abfrage von Daten durch Behörden, die für die Risikobewertung “unbedingt erforderlich” sind.
- Wird Akteneinsicht zur Durchsetzung zivilrechtlicher Ansprüche möglich sein (vgl. Diskussion im Kartellrecht: Donau-Chemie et al)?

# Co oznacza poufność (art. 78)?

- Skierowana do organów i „wszelkich innych osób fizycznych lub prawnych zaangażowanych w stosowanie niniejszego rozporządzenia”.
- Poufność informacji i danych uzyskanych podczas wykonywania swoich zadań i swojej działalności, aby w szczególności chronić:
  - prawa własności intelektualnej oraz poufne informacje handlowe (wyjątek: art. 5 dyrektywy 2016/953) lub
  - wdrożenie rozporządzenia, np. kontrole
  - interesy bezpieczeństwa publicznego i narodowego;
  - przebieg postępowań karnych i administracyjnych;
  - informacje niejawne.
- Wyszukiwanie przez organy wyłącznie danych „absolutnie niezbędnych” do oceny ryzyka.
- Czy możliwe będzie uzyskanie wglądu do akt w celu dochodzenia roszczeń cywilnoprawnych (por. dyskusja na gruncie prawa antymonopolowego: Donau-Chemie et al)?



# KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko

- Systemrisiko (Art. 3 Nr. 65): Risiko, das für die Fähigkeiten mit hohem Wirkungsgrad [Art. 3 Nr. 64] von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können.
- Zusätzlich zu Art. 53 (Art. 55 Abs. 1 KI-VO):
  - a) Modellbewertung mit standardisierten Protokollen einschließlich "Angriffstests"
  - b) Bewertung und Minderung der möglichen systemischen Risiken auf Unionsebene
  - c) Erfassen und Dokumentieren von "schwerwiegenden Vorfällen"
  - d) Angemessenes Maß an Cybersicherheit für KI-Modell und seine physische Infrastruktur gewährleisten
  - Abs. 2: Bis zur Normung genügen Verhaltenskodizes (widerlegbar?)
  - Abs. 3: Dokumentation ist vertraulich nach Art. 78
  - Keine Ausnahmen für Open-Source-Modelle, nur wenn Modell "ausschließlich für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen verwendet" wird
- Strengere Regeln für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko (Art. 55, 56 KI-VO)

## Modele AI ogólnego przeznaczenia z ryzykiem systemowym

- Ryzyko systemowe (art. 3 nr 65): Ryzyko, które jest charakterystyczne dla modeli AI ogólnego przeznaczenia posiadających zdolności dużego oddziaływania [art. 3 nr 64] i ma znaczący wpływ na rynek Unii ze względu na zasięg tych modeli lub rzeczywiste lub dające się racjonalnie przewidzieć negatywne skutki dla zdrowia publicznego, porządku publicznego, bezpieczeństwa publicznego, praw podstawowych lub całego społeczeństwa, mogące rozprzestrzenić się na dużą skalę w całym łańcuchu wartości.
- W uzupełnieniu do art. 53 (art. 55 ust. 1 rozporządzenia AI):
  - a) ocena modelu zgodnie ze znormalizowanymi protokołami, w tym „testy ataku”
  - b) ocena i ograniczanie ewentualnego ryzyka systemowego na poziomie Unii
  - c) rejestrowanie i dokumentowanie „poważnych incydentów”
  - d) zapewnianie odpowiedniego poziomu cyberochrony modelu AI oraz infrastruktury fizycznej tego modelu
  - Ust. 2: Do momentu unormowania wystarczające są kodeksy postępowania (możliwość podważenia?)
  - Ust. 3: Dokumentacja jest poufna zgodnie z art. 78
  - Brak wyjątków dla modeli open source, tylko jeśli model „jest wykorzystywany wyłącznie do celów działalności badawczo-rozwojowej i tworzenia prototypów”
- Bardziej rygorystyczne reguły dla dostawców modeli AI ogólnego przeznaczenia obciążonych ryzykiem systemowym (art. 55, 56 rozporządzenia AI)



# Verantwortlichkeit entlang der KI-Wertschöpfungskette (Art. 25)

- Abs. 1: Aufrücken zum Hersteller bei Veränderung oder Einsatz im Hochrisiko-Kontext.
  - Erstanbieter ist nicht mehr verantwortlich (Abs. 2). Nur noch Zusammenarbeitspflicht, sofern nicht Einsatz im Hochrisiko-Kontext nicht eindeutig verboten wurde.
- Abs. 3: Bei Einbettung in besonders regulierte Produkte gilt Produkthersteller als Anbieter des KI-Systems.
- Abs. 4: Anbieter eines Hochrisiko-KI-Systems und Dritter, der ein KI-System bereitstellt, das innerhalb eines Hochrisiko-KI-Systems verwendet wird, legen in schriftlicher Vereinbarung Informationen, Fähigkeiten, technischen Zugang und sonstige Unterstützung nach dem allgemein anerkannten Stand der Technik fest, die erforderlich sind, damit der Anbieter des Hochrisiko-KI-Systems die in der KI-VO festgelegten Pflichten vollständig erfüllen kann
- Gilt nicht bei Open-Source-KI-Modellen.
- Abs. 5 Geistiges Eigentum und Geschäftsgeheimnisschutz bleiben unberührt.

## Odpowiedzialność w całym łańcuchu wartości AI (art. 25)

- Ust. 1: Awans na producenta w przypadku zmiany lub wykorzystania w kontekście wysokiego ryzyka.
  - Pierwotny dostawca nie jest już odpowiedzialny (ust. 2). Istnieje już tylko obowiązek współpracy, chyba że użycie w kontekście wysokiego ryzyka nie zostało wyraźnie zabronione.
- Ust. 3: W przypadku wbudowania w produkty podlegające specjalnym regulacjom, producent produktu jest uważany za dostawcę systemu AI.
- Ust. 4: Dostawca systemu AI wysokiego ryzyka i osoba trzecia dostarczająca system AI, który jest wykorzystywany w systemie AI wysokiego ryzyka, wskazują, w drodze pisemnej umowy, informacje, zdolności, dostęp techniczny i innego rodzaju pomoc opartą na powszechnie uznanym stanie wiedzy technicznej wymagane, aby umożliwić dostawcy systemu AI wysokiego ryzyka pełne spełnienie obowiązków ustanowionych w niniejszym rozporządzeniu IA.
- Nie dotyczy modeli AI typu open source.
- Ust. 5 Prawa własności intelektualnej i ochrona tajemnicy przedsiębiorstwa pozostają nienaruszone.



# Regulierung von foundation models wurde auf KI-Modelle mit systemischem Risiko reduziert

- EP wollte noch breiter “foundation models” regeln.
- Definition (Art 3(1)(c)): ‘foundation model’ means an AI system model that is **trained on broad data** at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks;
  - Hintergrund: ChatGPT
  - Vgl. demgegenüber: ‘general purpose AI system’ means an AI system that can be used in and adapted to a wide range of applications for which it was not intentionally and specifically designed (Art 3(1)(d)).
- Unterschied scheint vor allem den Umfang der “training data” und (weniger bedeutsam) das Design “for a generality of output” zu sein.

## Regulacja modeli podstawowych została ograniczona do modeli AI z ryzykiem systemowym

- PE chciał jeszcze szerzej uregulować „modele podstawowe”.
- Definicja (art. 3 (1)(c)): ‘model podstawowy’ oznacza model systemu AI, który został **wytrenowany na obszernych danych** na dużą skalę, zaprojektowany pod kątem ogólności wyników i może zostać zaadaptowany do szerokiego zakresu charakterystycznych zadań;
  - Kontekst: ChatGPT
  - Por. natomiast: ‘system AI ogólnego przeznaczenia’ oznacza system AI, który może być wykorzystywany i dostosowywany do szerokiego zakresu zastosowań, dla których nie został celowo i specjalnie zaprojektowany (art. 3(1)(d)).
- Podstawową różnicą wydaje się być zakres „danych treningowych” oraz (mniej znaczące) zaprojektowanie „dla ogólności wyniku”.



# Art. 28b EP: Pflichten für provider von foundation models

- (1) Pflichten gelten unabhängig von Distributionskanal (auch open source), development methods oder Typus von Trainingsdaten (vgl. auch Art. 2(5)(e)).
- (2)(a): foundation models should assess and mitigate possible risks and harms through appropriate design, testing and analysis,
- (2)(b) process and incorporate only datasets that are subject to appropriate data governance measures (suitability, biases),
- (2)(c) Foundation models have to keep appropriate levels of performance, predictability, interpretability, corrigibility, safety and cybersecurity throughout their lifecycle: independent experts, documented analysis and extensive testing.
- (2)(d) standards to reduce energy use, resource use and waste, and measure energy consumption.
- (2)(e) draw up extensive technical documentation and intelligible instructions for use for downstream users to comply with Art. 28; and (3) provide the relevant documents up to 10 years after the model is launched.
- (2)(f) Foundation model providers have to implement a quality management system to ensure compliance with Art. 28;
- (2)(g) Foundation models have to be registered on the EU database.
- (4) Foundation models that fall in the generative AI category must comply with transparency obligation (Art. 52) and implement adequate safeguards against generating content in breach of EU law.  
Generative AI models would have to make publicly available a sufficiently detailed summary of the use of training data protected under copyright law.

# Art. 28b PE: Obowiązki dla dostawców modeli podstawowych

- (1) Obowiązki mają zastosowanie niezależnie od kanału dystrybucji (w tym open source), metod rozwoju lub rodzaju danych treningowych (zob. również art. 2(5)(e)).
- (2)(a): modele podstawowe powinny oceniać i ograniczać możliwe ryzyko i szkody poprzez odpowiednie projektowanie, testowanie i analizę,
- (2)(b) przetwarzanie i włączanie jedynie zbiorów danych, które podlegają odpowiednim środkom zarządzania danymi (odpowiedniość, stroniczość),
- (2)(c) modele podstawowe muszą utrzymywać odpowiednie poziomy wydajności, przewidywalności, interpretowalności, korygowalności, bezpieczeństwa i cyberbezpieczeństwa przez cały cykl życia: niezależni eksperci, udokumentowana analiza i szeroko zakrojone testy.
- (2)(d) normy mające na celu zmniejszenie zużycia energii, zasobów i odpadów oraz pomiar zużycia energii.
- (2)(e) sporządzanie obszernej dokumentacji technicznej i zrozumiałych instrukcji użytkowania dla dalszych użytkowników w celu zapewnienia zgodności z art. 28; oraz (3) dostarczanie odpowiednich dokumentów do 10 lat po wprowadzeniu modelu na rynek.
- (2)(f) dostawcy modelu podstawowego muszą wdrożyć system zarządzania jakością w celu zapewnienia zgodności z art. 28;
- (2)(g) modele podstawowe muszą być zarejestrowane w bazie danych UE.
- (4) modele podstawowe należące do kategorii generatywnej AI muszą być zgodne z obowiązkiem przejrzystości (art. 52) i muszą wdrażać odpowiednie zabezpieczenia przed generowaniem treści z naruszeniem prawa UE. Generatywne modele AI musiałyby publicznie udostępniać wystarczająco szczegółowe podsumowanie wykorzystania danych treningowych chronionych prawem autorskim.



# Bewertung: Reduzierung auf KI-Modelle mit systemischen Risiken ggü foundation models sinnvoll

- Argument für Regulierung von foundation models im Unterschied zu general purpose AI ist, dass sie eine engere Kategorie mit potentiell sehr breiter Verwendung betreffen. Aber:
  - Der Begriff wird zwar in der Informatik genutzt, aber nicht für die Zwecke juristischer Definitionen, so dass seine Eignung unklar ist („trained on broad data at scale“?).
  - Auch hier stellt sich die Frage, wie angesichts der unterschiedlichen Verwendungen ein Risikomanagementsystem eingerichtet werden soll oder über die Geeignetheit von Trainingsdaten entschieden werden soll.
    - Risiko, dass nur große Unternehmen die Pflichten erfüllen können?
  - Ggf. könnte die eigenständige Regulierung von foundation models unabhängig von ihrem konkreten Einsatz an eine Benennung konkreter Modelle geknüpft werden, deren Anbieter dann strengeren Pflichten unterliegen (vgl. Digital Markets Act).
  - Problematisch ist nach wie vor die Einbeziehung von Open-Source-Modelle mit KI-Systemen mit systemischem Risiko.

## Ocena: Ograniczenie do modeli AI z ryzykiem systemowym w porównaniu do modeli podstawowych jest zasadne

- Argumentem przemawiającym za uregulowaniem modeli podstawowych w odróżnieniu od AI ogólnego przeznaczenia jest to, że dotyczą one węższej kategorii o potencjalnie bardzo szerokim zastosowaniu. Ale:
  - Termin ten jest wprawdzie używany w informatyce, jednakże nie do celów definicji prawnych, więc jego przydatność jest niejasna („trenowany na obszernych danych na dużą skalę“?).
  - Tutaj również pojawia się pytanie, w jaki sposób należy skonfigurować system zarządzania ryzykiem w świetle różnych zastosowań lub w jaki sposób należy podjąć decyzję co do przydatności danych treningowych.
    - Ryzyko, że tylko duże firmy będą w stanie spełnić te obowiązki?
  - W razie potrzeby niezależna regulacja dotycząca modeli podstawowych mogłaby być powiązana ze wskazaniem konkretnych modeli, niezależnie od ich konkretnego wykorzystania, których dostawcy podlegaliby wówczas bardziej rygorystycznym obowiązkom (por. ustawa o rynkach cyfrowych).
  - W dalszym ciągu problematyczne jest włączenie modeli typu open source z systemami AI z ryzykiem systemowym.



# Content Moderation bei KI-Systemen?

- Brauchen wir eine Content Moderation bei KI-Systemen wie beim Digital Services Act?
  - M.E. schwierig, weil so schnell wie beim DSA nicht reagiert werden kann. Auch keine unmittelbare Breitenwirkung der Ausgaben (anders als bei Plattformen). Daher allenfalls bei sehr verbreiteten Modellen.
  - Wichtiger ist m.E. die Kennzeichnungspflicht für die Erzeugnisse und die Information über Missbräuche.

## Moderacja treści w systemach AI?

- Czy potrzebna jest nam moderacja treści w systemach AI, jak w przypadku ustawy o rynkach cyfrowych?
  - Moim zdaniem jest to trudne, ponieważ nie można reagować tak szybko, jak w przypadku DSA. Brak również bezpośredniego szerokiego oddziaływania wyników (w przeciwieństwie do platform). Stąd też tylko w przypadku bardzo popularnych modeli.
  - Moim zdaniem ważniejsze jest obowiązkowe oznaczanie produktów i informowanie o nadużyciach.



# Allgemeine Prinzipien für alle KI-Systeme?

- Nicht aufgenommen wurden allgemeine Prinzipien für alle KI-Systeme (Art. 4a EP-Vorschlag: General principles applicable to all AI systems):
  - (1) All operators falling under this Regulation shall make their best efforts to develop and use AI systems or foundation models in accordance with the following general principles establishing a high-level framework that promotes a coherent human-centric European approach to ethical and trustworthy Artificial Intelligence, which is fully in line with the Charter as well as the values on which the Union is founded:
  - a) human agency and oversight,
  - b) technical robustness and safety,
  - c) privacy and data governance,
  - d) transparency,
  - e) diversity, non-discrimination and fairness,
  - f) social and environmental well-being.

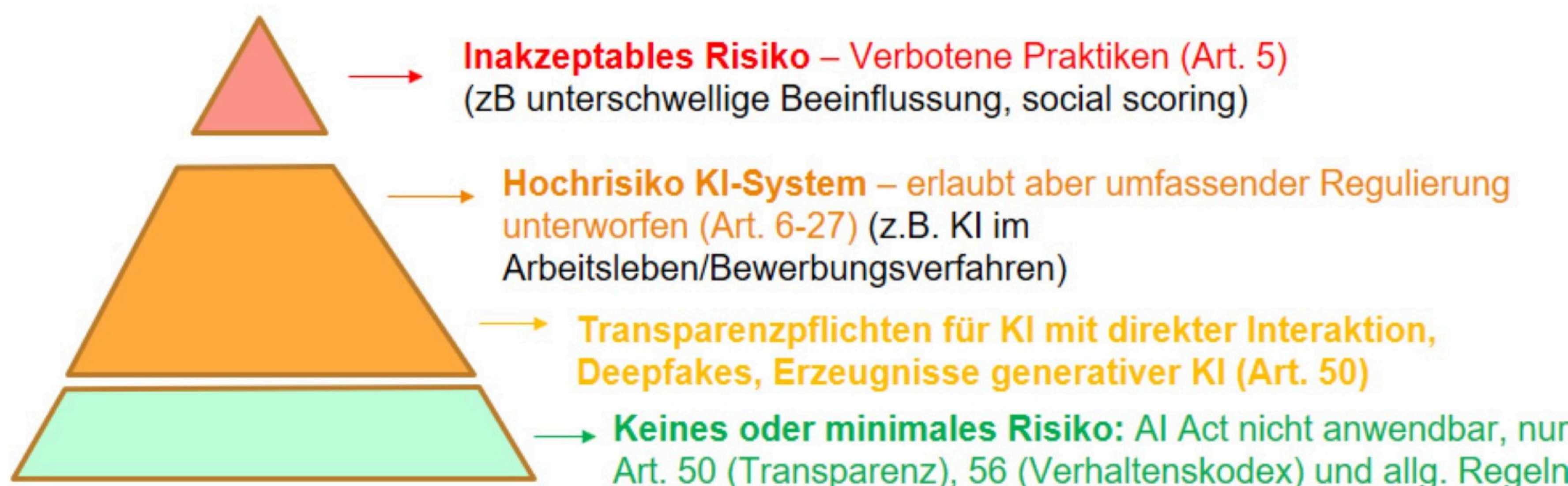
## Ogólne zasady dla wszystkich systemów AI?

- Nie uwzględniono ogólnych zasad dla wszystkich systemów AI (art. 4a wniosku PE): Ogólne zasady mające zastosowanie do wszystkich systemów AI:
  - (1) Wszystkie podmioty objęte zakresem niniejszego rozporządzenia dokładają wszelkich starań, aby rozwijać i wykorzystywać systemy AI lub modele podstawowe zgodnie z następującymi zasadami ogólnymi, ustanawiającymi ramy wysokiego szczebla, które promują spójne, zorientowane na człowieka europejskie podejście do etycznej i godnej zaufania sztucznej inteligencji, które jest w pełni zgodne z Kartą, a także z wartościami, na których opiera się Unia:
  - a) przewodnia i nadzorczą rolę człowieka,
  - b) solidność techniczna i bezpieczeństwo,
  - c) ochrona prywatności i zarządzanie danymi,
  - d) przejrzystość,
  - e) różnorodność, niedyskryminacja i sprawiedliwość,
  - f) dobrostan społeczny i środowiskowy.



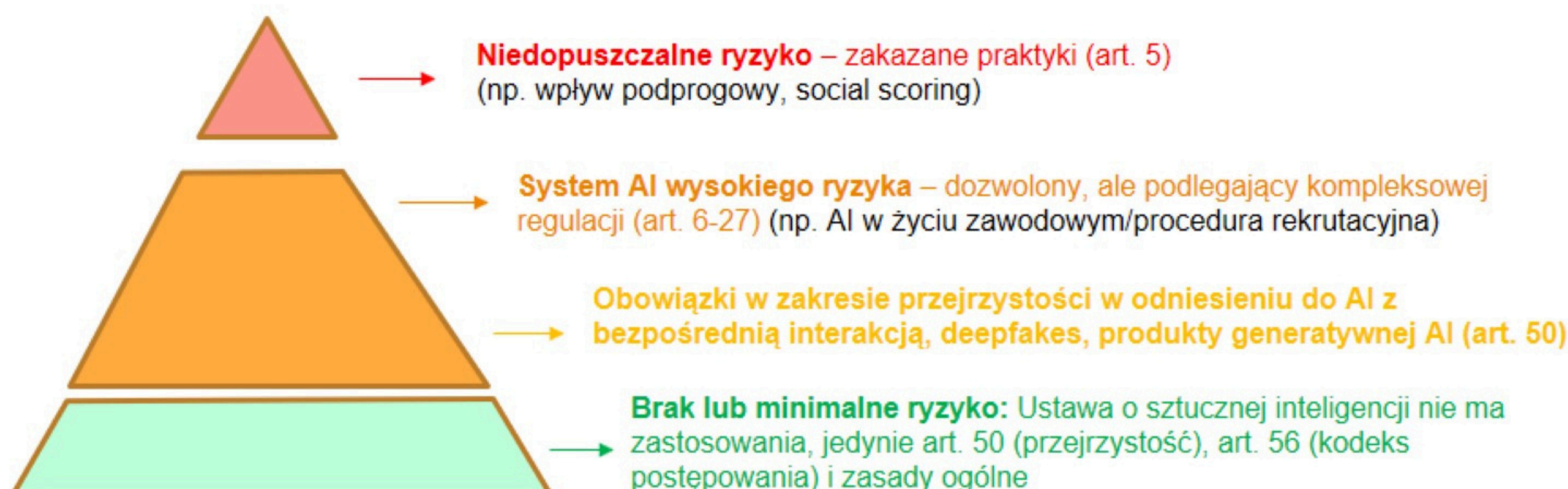
# Wie wird geregelt? – Ursprünglich: Risikobasierte Regulierung

- KOM-Vorschlag: Je höher das Risiko, desto strenger die Regeln.
- Keine Regulierung von KI als solcher, sondern nur konkreter Anwendungen.



## Sposób regulacji? – Początkowo: Regulacja w oparciu o ryzyko

- Wniosek Komisji: Im wyższe ryzyko, tym surowsze reguły.
- Brak regulacji dotyczących AI jako takiej, tylko regulacje dotyczące konkretnych zastosowań.





# Nun: hybrider Ansatz

- Risikobasierter Ansatz problematisch bei KI mit allgemeinem Verwendungszweck?
- Lösung (1): "Aufrücken zum Hersteller" : Bei "substantial modification", die ein High risk AI system erzeugt, wird der "Modifizierer" zum Hersteller (Art. 25 Abs. 1).
  - Zudem Vorgaben für Vereinbarungen zwischen Teilehersteller und Herstellern von High-risk-AI, aber ohne Klauselkontrolle (Art. 25 Abs. 2, 4; anders noch Art. 28a EP-Vorschlag).
- Lösung (2): Eigene Pflichten für Hersteller von "foundation models" (Art. 28b)



## Obecnie: podejście hybrydowe

- Podejście oparte na ryzyku problematyczne w przypadku AI ogólnego przeznaczenia?
- Rozwiązanie (1): „Awans na producenta”: W przypadku „istotnej modyfikacji”, która tworzy system AI wysokiego ryzyka, „modyfikujący” staje się producentem (art. 25 ust. 1).
  - Ponadto wytyczne dotyczące porozumień między producentami części a producentami AI wysokiego ryzyka, ale bez kontroli klauzul (art. 25 ust. 2, 4; inaczej art. 28a wniosku PE).
- Rozwiązanie (2): Szczególne obowiązki dla producentów „modeli podstawowych” (art. 28b)





# Persönlicher Anwendungsbereich (Wer?)

- AI Act regelt v.a. die Pflichten von Anbietern und Betreibern:
  - Art 3 Nr. 3: „Anbieter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich;
  - Art 3 Nr. 4: „Betreiber“ 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
  - Außerdem erfasst werden Importeure, Händler, Hersteller, Produkthersteller KI-eingebetteter Produkte und Bevollmächtigte von Anbietern außerhalb der EU.
  - Die von KI-Systemen **betroffenen Personen** wurden zunächst im AI Act nicht angesprochen (anders in der DSGVO). Aber nun Art. 86: Recht auf Erläuterung der Entscheidungsfindung im Einzelfall, aber gesetzlich abdingbar und subsidiär zu anderen Rechten auf Erläuterung (zB nach DSGVO, soweit diese ein solches Recht eröffnet).

# Osobowy zakres stosowania (kto?)

- AI Act reguluje przede wszystkim obowiązki dostawców i podmiotów stosujących:
  - Art. 3 nr 3: „dostawca” oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które rozwijają system AI lub model AI ogólnego przeznaczenia lub zlecają rozwój systemu AI lub modelu AI ogólnego przeznaczenia oraz które – odpłatnie lub nieodpłatnie – pod własną nazwą lub własnym znakiem towarowym wprowadzają do obrotu lub oddają do użytku system AI;
  - Art. 3 nr 4: „podmiot stosujący” oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które wykorzystują system AI, nad którym sprawują kontrolę, z wyjątkiem sytuacji, gdy system AI jest wykorzystywany w ramach osobistej działalności pozazawodowej;
  - Uwzględniono również importerów, dystrybutorów, producentów, producentów produktów z wbudowaną AI oraz upoważnionych przedstawicieli dostawców spoza UE.
  - **Osoby, których dotyczą systemy AI**, nie zostały początkowo uwzględnione w AI Act (w przeciwieństwie do RODO). Ale obecnie art. 86: Prawo do uzyskania wyjaśnienia procesu decyzyjnego w indywidualnych przypadkach, jednak z możliwością odstąpienia zgodnie z prawem i pomocnicze w stosunku do innych praw do uzyskania wyjaśnienia (np. zgodnie z RODO, o ile zapewnia takie prawo).



## Räumlicher Anwendungsbereich (Wo?)

- Art. 2 Abs. 1: Diese Verordnung gilt für Folgende:
- a) Anbieter, die in der Union KI-Systeme in Verkehr bringen oder in Betrieb nehmen oder KI-Modelle mit allgemeinem Verwendungszweck in Verkehr bringen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind;
- b) Betreiber von KI-Systemen, die ihren Sitz in der Union haben oder sich in der Union befinden;
- c) Anbieter und Betreiber von KI-Systemen, die ihren Sitz in einem Drittland haben oder sich in einem Drittland befinden, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird;
- → **Weiter räumlicher Anwendungsbereich zwingend, um Nachteile für EU-Unternehmen zu vermeiden.**

## Przestrzenny zakres stosowania (gdzie?)

- Art. 2 ust. 1 Niniejsze rozporządzenie stosuje się do:
- a) dostawców wprowadzających do obrotu lub oddających do użytku systemy AI lub wprowadzających do obrotu modele AI ogólnego przeznaczenia w Unii, niezależnie od tego, czy dostawcy ci mają siedzibę lub znajdują się w Unii czy w państwie trzecim;
- b) podmiotów stosujących systemy AI, które to podmioty mają siedzibę lub znajdują się w Unii;
- c) dostawców systemów AI i podmiotów stosujących systemy AI, którzy mają siedzibę lub znajdują się w państwie trzecim, w przypadku gdy wyniki wytworzone przez system AI są wykorzystywane w Unii;
- → **Szeroki geograficzny zakres stosowania jest obowiązkowy w celu uniknięcia niedogodności dla przedsiębiorstw z UE.**



# Anwendungsbereich: Abgrenzung zu anderen Materien

- Ausgenommene Bereiche:
  - Sektorielle Vorschriften für Hochrisiko-KI-Systeme sind vorrangig, Art 2 Abs. 2
  - Verteidigung und nationale Sicherheit, Art 2 Abs. 3
  - KI-Systeme für alleinigen Zweck wissenschaftlicher Forschung, Art. 2 Abs. 6
  - Forschungs-, Test- und Entwicklungstätigkeit vor Inverkehrbringen, soweit nicht Test unter realen Bedingungen (Art. 2 Abs. 8)
  - Einsatz von KI-Systemen durch natürliche Personen im Rahmen einer ausschließlich persönlichen und nicht beruflichen Tätigkeit verwenden, Art 2 Abs. 10 (selbst Transparenzpflicht für Deep Fakes nicht ausgenommen).
  - KI-Systeme unter Open Source-Lizenzen, soweit diese nicht als Hochrisiko-System oder als KI-System iSd Art. 5 (verbotene Praktiken) oder Art. 50 (Transparenzpflicht)

# Zakres stosowania: Odgraniczenie od innych obszarów

- Wyłączone zakresy:
  - Przepisy sektorowe dla systemów AI wysokiego ryzyka są priorytetem, art. 2 ust. 2
  - Obrona i bezpieczeństwo narodowe, art. 2 ust. 3
  - Systemy AI wyłącznie do celów badań naukowych, art. 2 ust. 6
  - Działalność badawcza, testowa i rozwojowa przed wprowadzeniem do obrotu, chyba że testy odbywają się w warunkach rzeczywistych (art. 2 ust. 8)
  - Korzystanie z systemów AI przez osoby fizyczne w ramach czysto osobistej działalności pozazawodowej, art. 2 ust. 10 (nawet nie wyłączając obowiązku przejrzystości w przypadku deep fakes).
  - Systemy AI na licencjach open source, chyba że są one sklasyfikowane jako systemy wysokiego ryzyka lub jako systemy AI w rozumieniu art. 5 (zakazane praktyki) lub art. 50 (obowiązek przejrzystości)



# Anwendungsbereich: Abgrenzung zu anderen Materien

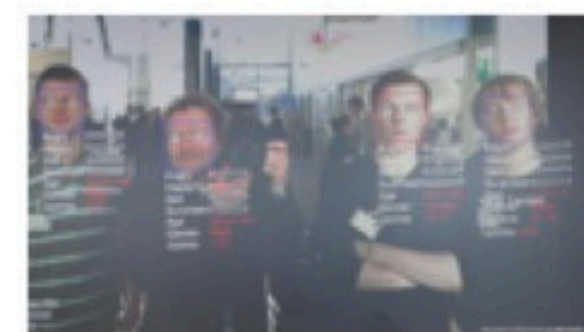
- AI Act berührt nicht andere EU-Rechtsvorschriften (EG 9, 10), insbesondere im Bereich Datenschutz (Art. 2 Abs. 7), Verbraucherschutz + Produktsicherheit (Art. 2 Abs. 9), Grundrechte, Beschäftigung, Arbeitnehmerschutz und Produktsicherheit.
- KI-VO zielt darauf ab, die Wirksamkeit dieser bestehenden Rechte und Rechtsbehelfe zu stärken, indem sie spezifische Anforderungen und Verpflichtungen festlegt, u. a. in Bezug auf Transparenz, technische Dokumentation und das Führen von Aufzeichnungen von KI-Systemen (EG 9 aE).
  - Beispiele: Rechtsbehelfe aus Produkthaftungsrecht (vgl. Reform) oder DSGVO.
  - Was bedeutet das für das Recht auf Dokumentenzugang?

# Zakres stosowania: Odgraniczenie od innych obszarów

- AI Act nie ma wpływu na pozostałe przepisy UE (motyw 9, 10), w szczególności w zakresie ochrony danych (art. 2 ust. 7), ochrony konsumentów + bezpieczeństwa produktów (art. 2 ust. 9), praw podstawowych, zatrudnienia, ochrony pracowników i bezpieczeństwa produktów.
- Rozporządzenie AI ma na celu wzmocnienie skuteczności tych istniejących praw i środków prawnych poprzez ustanowienie szczegółowych wymogów i obowiązków, m.in. w odniesieniu do przejrzystości, dokumentacji technicznej i prowadzenia rejestrów systemów AI (motyw 9 w zast.).
  - Przykłady: Środki prawne na mocy przepisów dotyczących odpowiedzialności za produkt (por. reforma) lub RODO.
  - Co to oznacza dla prawa dostępu do dokumentów?

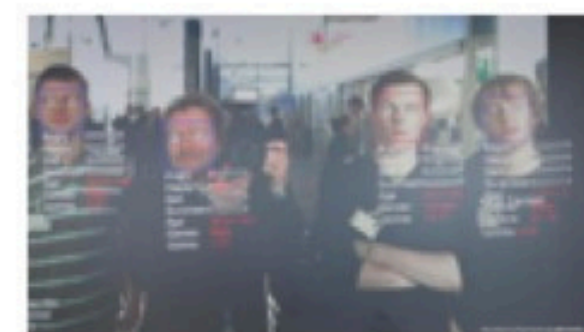


# Verbote (Art. 5)



- **Unterschwellige Beeinflussung durch KI-System, (1)(a):** KI-VO folgt EP: Fähigkeit, informierte Entscheidung zu treffen, muss spürbar beeinträchtigt werden, so dass dies erheblichen Schaden zufügen kann.
- **Ausnutzen der Schwäche/Schutzbedürftigkeit, (1)(b):** Verhaltensbeeinflussung vulnerabler Personen mit der Folge, dass erheblicher Schaden (nicht nur körperlich/psychologisch) mit hinreichender Wahrscheinlichkeit zugefügt wird
- **Social Scoring (sowohl durch Staat wie durch Private) (1)(c):** biometrische Kategorisierungssysteme auf Grundlage der Verhaltensbeobachtung oder persönlicher Eigenschaften, wenn dies zur Schlechterstellung ohne Zusammenhang mit den ursprünglich erzeugten oder erfassten Daten steht oder wenn die Schlechterstellung im Hinblick auf Verhalten ungerechtfertigt oder unverhältnismäßig ist
- **Strafbarkeitsprognosen, (1)(d)** (soweit nicht objektive und überprüfbare Tatsachen)
- Datenbanken zur **Gesichtserkennung** durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet, (1)(e) (Clearview)
- **Emotionserkennungssysteme** am Arbeitsplatz oder in Bildungseinrichtungen, 1(f)
- **Biometrische Kategorisierung**, um verbotene Merkmale (Rasse, pol. Einstellung, sexuelle Ausrichtung etc) zu erschließen, 1(g)
- **Biometrische Echtzeit-Identifizierung, (1)(h)** (mit Ausnahmen für Strafverfolgung und Terrorabwehr) (Hauptdiskussionspunkt)

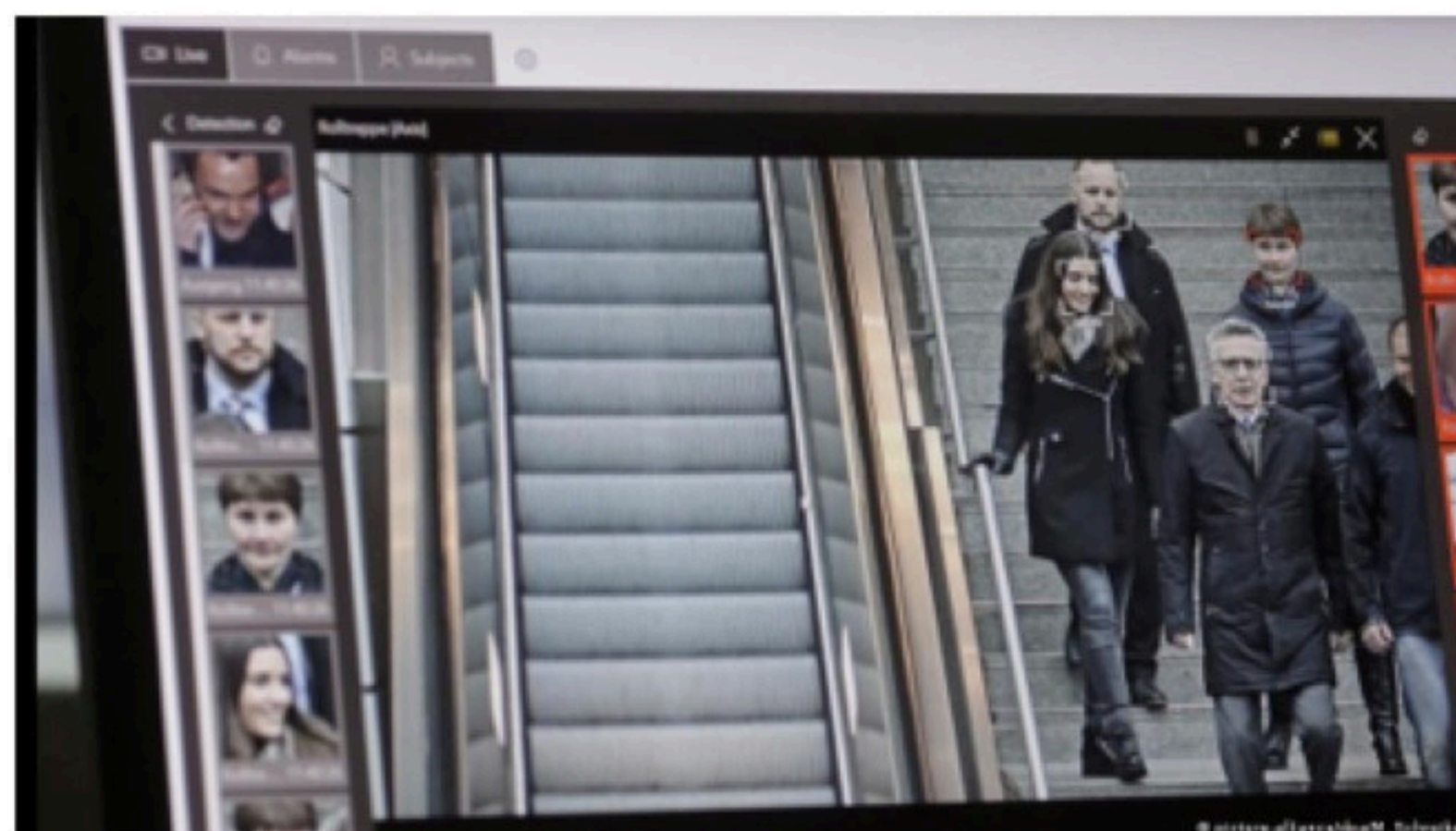
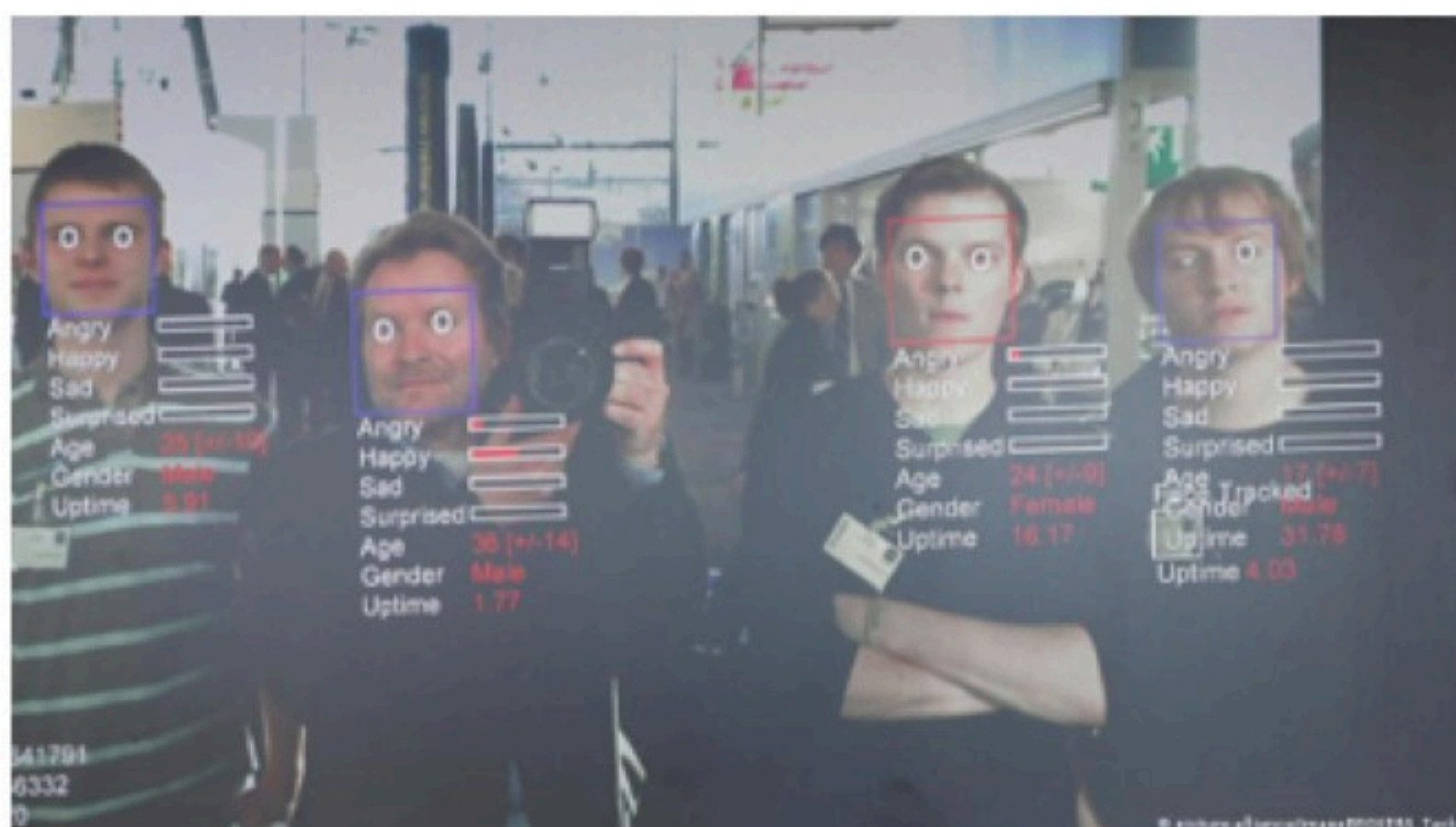
# Zakazy (art. 5)



- **Podprogowy wpływ systemu AI, (1)(a):** Rozporządzenie AI podąża za PE: Zdolność do podejmowania świadomych decyzji musi być odczuwalnie ograniczona, aby mogło to spowodować znaczną szkodę.
- **Wykorzystywanie słabości/potrzeby ochrony, (1)(b):** Wywieranie wpływu na zachowanie osób szczególnie narażonych z takim skutkiem, że z wystarczającym prawdopodobieństwem zostanie im wyrządzona znaczna szkoda (nie tylko fizyczna/psychiczna)
- **Scoring społeczny (zarówno przez państwo, jak i podmioty prywatne) (1)(c):** biometryczne systemy kategoryzacji na podstawie obserwacji zachowań lub cech osobistych, jeżeli prowadzi to do krzywdzącego traktowania bez związku z pierwotnie wygenerowanymi lub zgromadzonymi danymi, lub jeśli krzywdzące traktowanie jest nieuzasadnione lub niewspółmierne w stosunku do zachowania
- **Przewidywanie odpowiedzialności karnej, (1)(d)** (chyba że obiektywne i możliwe do zweryfikowania fakty stanowią inaczej)
- Bazy danych do **rozpoznawania twarzy** poprzez nieukierunkowany odczyt obrazów twarzy z Internetu, (1)(e) (Clearview)
- **Systemy rozpoznawania emocji** w miejscu pracy lub w placówkach edukacyjnych, 1(f)
- **Kategoryzacja biometryczna** w celu identyfikacji cech zabronionych (rasa, poglądy polityczne, orientacja seksualna itp.), 1(g)
- **Identyfikacja biometryczna w czasie rzeczywistym, (1)(h)** (z wyjątkami dotyczącymi ścigania przestępstw i zwalczania terroryzmu) (główny punkt dyskusji)

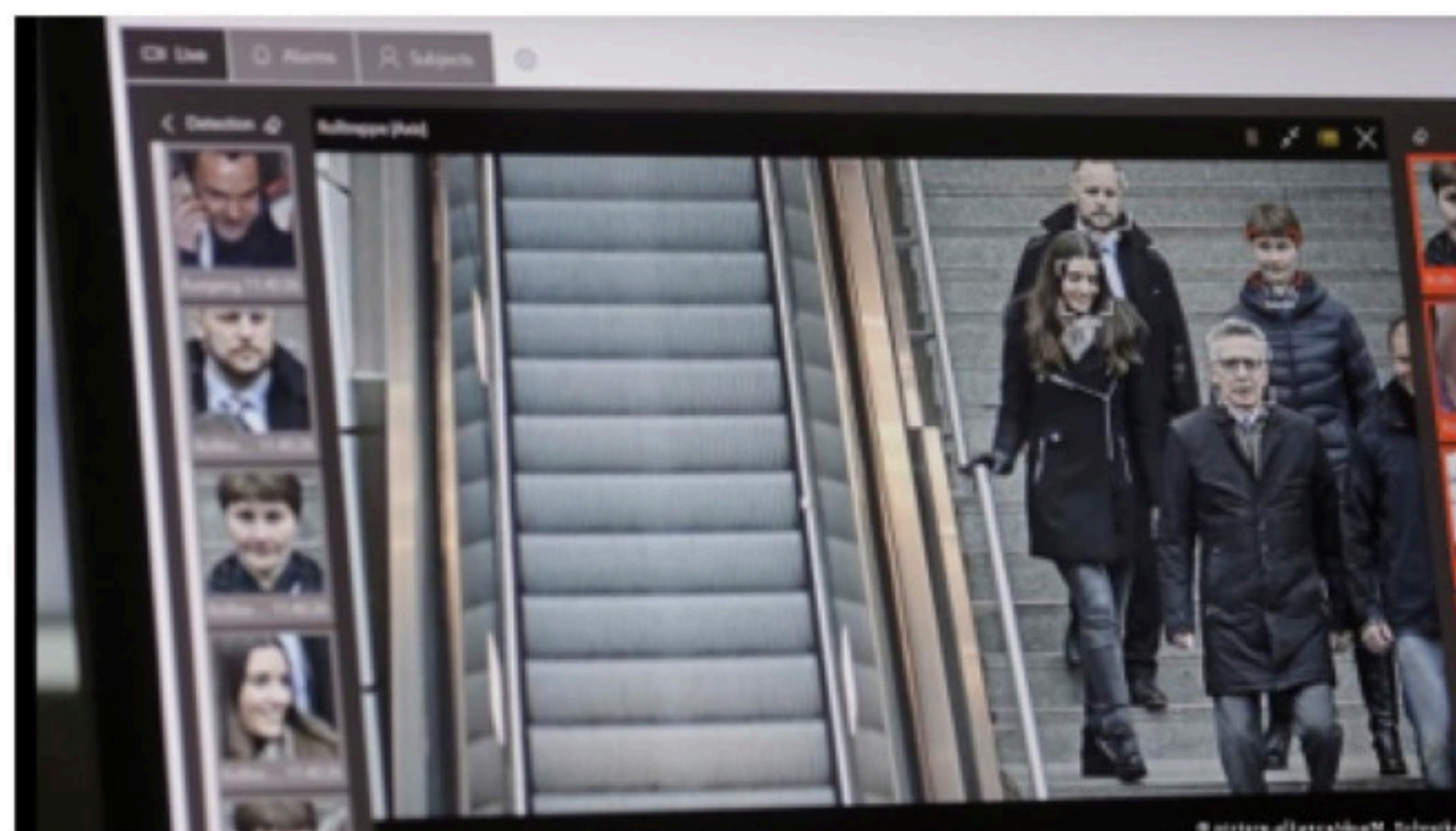
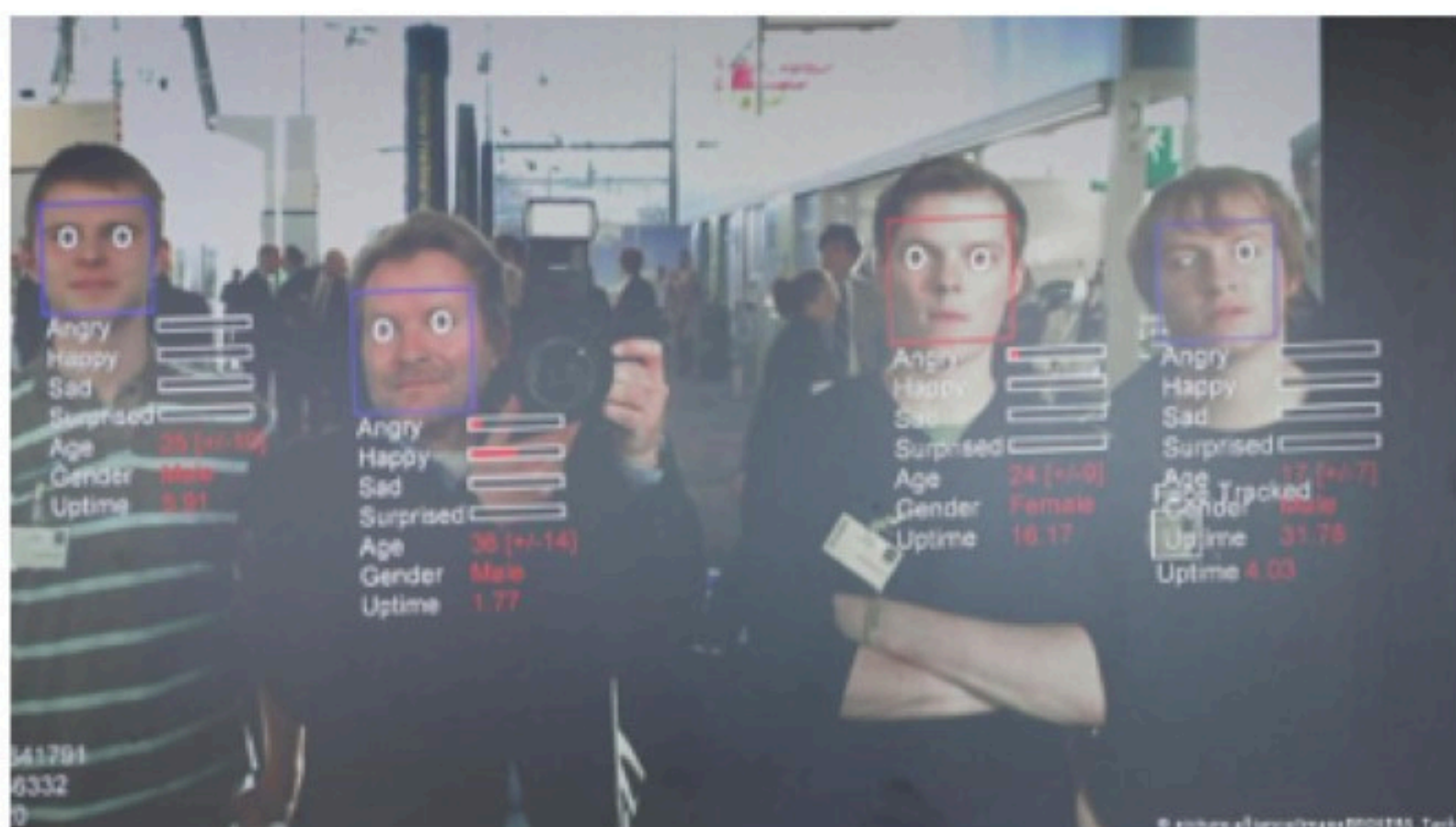


# Echtzeit-Fernidentifizierung



- Nur Echtzeit-Fernidentifizierung ist verboten, nicht nachträgliche Identifizierung
- Unzulässige Vorratsdatenspeicherung?

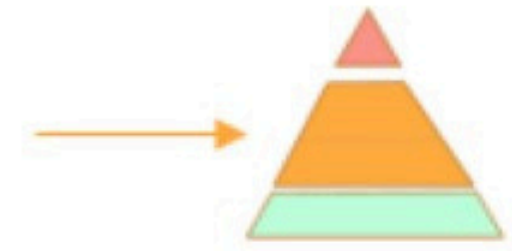
## Zdalna identyfikacja w czasie rzeczywistym



- Zabroniona jest jedynie zdalna identyfikacja w czasie rzeczywistym, nie zaś późniejsza identyfikacja
- Niedopuszczalna retencja danych?



# Hochrisiko-KI-Systeme (Art. 6): Definition



## Was sind Hochrisiko-KI-Systeme? Zwei Fälle

- **Abs. 1:** KI-Systeme, die entweder eine Sicherheitskomponente eines Produkts sind, das bereits einer Konformitätsbewertung durch einen Dritten in Bezug auf Gesundheits- und Sicherheitsrisiken unterliegt oder das KI-System ist selbst ein solches Produkt UND das Produkt oder das KI-System als Teil eines solchen Produkts unterliegt einer Konformitätsbewertung durch Dritte aufgrund der in Anhang II genannten Harmonisierungsrechtsakte der Union
- **Abs. 2:** KI-Systeme, die auf den in Anhang III genannten Feldern eingesetzt werden.
- **Abs. 3 Neu (EP):** KI-System gilt im Fall von Abs. 2 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. (+), wenn
  - Nur Durchführung eng gefasster Verfahrensaufgabe
  - Nur Verbesserung zuvor ausgeführter menschlicher Tätigkeit
  - Nur Erkennen von Entscheidungsmustern oder Abweichungen von früheren Entscheidungsmustern, ohne zuvor abgeschlossene menschliche Bewertung zu ersetzen
  - Nur vorbereitende Aufgabe für eine Bewertung im Bereich des Gebiete des Anhangs III

# Systemy AI wysokiego ryzyka (art. 6): Definicja



## Czym są systemy AI wysokiego ryzyka? Dwa przypadki

- **Ust. 1:** Systemy AI, które są albo elementem bezpieczeństwa produktu, podlegającego już ocenie zgodności przez podmiot trzeci pod kątem zagrożeń dla zdrowia i bezpieczeństwa, albo system AI sam w sobie jest takim produktem ORAZ produkt lub system AI jako część takiego produktu podlega ocenie zgodności przez podmioty trzecie na podstawie unijnych aktów harmonizacyjnych, o których mowa w załączniku II
- **Ust. 2:** Systemy AI wykorzystywane w dziedzinach wymienionych w załączniku III.
- **Ust. 3 nowy (PE):** System AI w przypadku ust. 2 nie jest uważany za wysoce ryzykowny, jeżeli nie stwarza znaczącego ryzyka szkody dla zdrowia, bezpieczeństwa lub praw podstawowych osób fizycznych, między innymi poprzez brak znaczącego wpływu na wynik procesu podejmowania decyzji. (+) jeżeli
  - Tylko realizacja wąsko zdefiniowanego zadania proceduralnego
  - Tylko usprawnienie czynności uprzednio wykonywanych przez człowieka
  - Tylko rozpoznawanie wzorców podejmowania decyzji lub odstępstw od wzorców podjętych uprzednio decyzji, bez zastąpienia zakończonej uprzednio oceny dokonanej przez człowieka
  - Tylko zadanie przygotowawcze do oceny w zakresie obszarów wymienionych w załączniku III



## Hochrisiko-KI (Art. 6): Bewertung

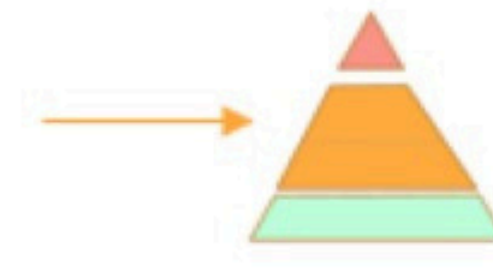
- Der Einsatz von KI durch den Staat wird relative umfassend als Hochrisiko-System eingestuft.
  - Das wird absehbar die Kosten treiben und den Einsatz insgesamt verhindern, obwohl durchaus erheblicher Nutzen gerade durch den Einsatz von KI in der Verwaltung zu erwarten ist.
  - M.E. zeigt sich, dass öffentliche Einrichtungen – etwa Hochschulen, aber auch die Justiz – schlicht keine Fürsprecher hatten, um Ausnahmen durchzusetzen.
- Positiv sind die neuen Ausnahmen nach Art. 6 Abs. 3 KI-VO zu bewerten.
- Ggf. hätte Hochrisiko-Einsatz ausgeschlossen werden können, wenn der Betroffene eine (echte) Wahl hat, ob er dem KI-System unterworfen wird und zudem ein Recht auf Beschwerde zu einem menschlichen Entscheider hat.

## AI wysokiego ryzyka (art. 6): Ocena

- Wykorzystanie AI przez państwo jest stosunkowo szeroko klasyfikowane jako system wysokiego ryzyka.
  - Przewiduje się, że spowoduje to wzrost kosztów i uniemożliwi korzystanie z AI w ogóle, mimo iż można spodziewać się znacznych korzyści z wykorzystania AI, zwłaszcza w administracji.
  - Moim zdaniem pokazuje to, że instytucje publiczne – takie jak uniwersytety, ale także sądownictwo – po prostu nie miały swoich orędowników, którzy wyegzekwowaliby wyłączenia.
- Nowe wyłączenia na mocy art. 6 ust. 3 rozporządzenia AI należy oceniać pozytywnie.
- W razie potrzeby zastosowanie wysokiego ryzyka można było wykluczyć, gdyby dana osoba miała (rzeczywisty) wybór, czy zostanie poddana systemowi AI, a ponadto miała prawo złożenia skargi u ludzkiego decydenta.

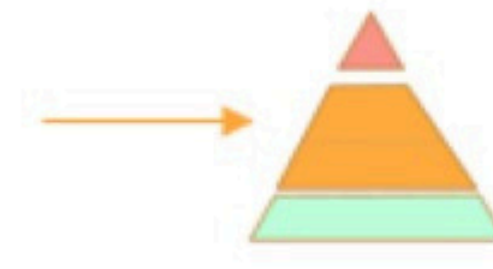


# Hochrisiko KI (Art. 8-15): Anforderungen



- Art. 8 Abs. 1: Begrenzung durch „Zweckbestimmung sowie dem allgemein anerkannten Stand der Technik“.
- Art. 9: Einrichtung eines Risikomanagementsystems, das eine angemessene Risikobewertung und Risikominimierung/-beseitigung gewährleistet im Hinblick auf den beabsichtigten Zweck während des gesamten Lebenszyklus.
- Art. 10: Datenqualität, die für die Zweckbestimmung des Hochrisiko-KI-Systems geeignet sind (Art. 10). Für Trainings-, Validierungs- und Testdatensätze weitere Vorgaben (Art. 10(2)-(5)).
- Art. 11: Technische Dokumentation
- Art. 12: Aufzeichnungspflichten (Logging)
- Art. 13: Transparenzpflichten und Verpflichtung auf Gebrauchsanweisungen. Beachte auch das Recht auf Erklärung (Art. 86).
- Art. 14: Menschliche Aufsicht.
- Art. 15: Genauigkeit, Robustheit und Cybersicherheit

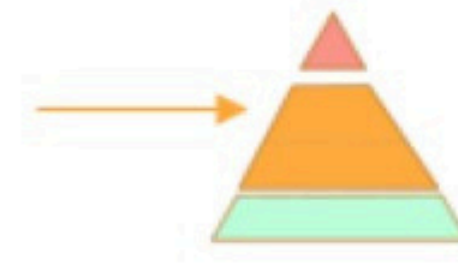
# AI wysokiego ryzyka (art. 8-15): Wymogi



- Art. 8 ust. 1: Ograniczenie przez „przeznaczenie oraz powszechnie uznawany stan wiedzy technicznej”.
- Art. 9: Ustanowienie systemu zarządzania ryzykiem, który zapewnia odpowiednią ocenę ryzyka i minimalizację/eliminację ryzyka w odniesieniu do zamierzonego celu podczas całego cyklu życia.
- Art. 10: Jakość danych odpowiednia do przeznaczenia systemu AI wysokiego ryzyka (art. 10). Dalsze wytyczne dotyczące zestawów danych treningowych, walidacyjnych i testowych (art. 10 ust. 2-5).
- Art. 11: Dokumentacja techniczna
- Art. 12: Rejestrowanie zdarzeń (logowanie)
- Art. 13: Obowiązki w zakresie przejrzystości i obowiązek dostarczenia instrukcji użytkowania. Należy również zwrócić uwagę na prawo do uzyskania wyjaśnienia (art. 86).
- Art. 14: Nadzór ze strony człowieka.
- Art. 15: Dokładność, solidność i cyberbezpieczeństwo



# Hochrisiko-KI: Adressat der Pflichten



## Anbieter

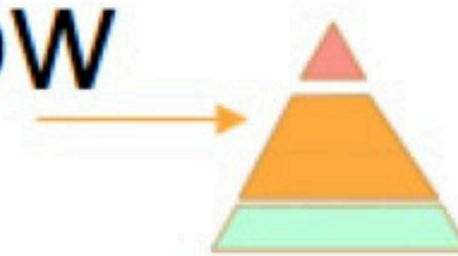
- Einhaltung der Art. 8-15 (Art. 16) und entsprechendes Qualitätsmanagement (Art. 17).
- Aufbewahrung der Dokumentation (Art. 18) und der automatischen Logging-Daten (Art. 19)
- Produktüberwachung, Korrekturmaßnahmen, Informationspflicht (EP) (Art. 20).
- Information und Kooperation mit den Aufsichtsbehörden (Art. 21)
- Bestellung eines Bevollmächtigten (Art. 22).
- Konformitätsbewertung (Art. 43).
- Registrierung des Hochrisiko-KI-Systems (Art. 49).

**Zudem Pflichten für Importeure (Art. 23), Händler (Art. 24), Verantwortlichkeit entlang der Wertschöpfungskette (Art. 25)**

## Betreiber (EP, vorher: Nutzer) (Art. 26):

- Abs. 1: Verwendung im Einklang mit Gebrauchsanweisungen.
- Abs. 2: ausreichend kompetentes Personal
- Abs. 4: Eingabedaten müssen Zweck des Systems entsprechen und ausreichend repräsentativ sein.
- Abs. 5: Ausführung des Systems überwachen; Anbieter und Behörden über bekannt gewordene Risiken informieren.
- Abs. 6: Aufbewahrung der Nutzungsprotokolle
- Abs. 7: Beteiligung der AN-Vertreter
- Abs. 11: Information der Betroffenen
- Abs. 12: Zusammenarbeit mit Behörden
- Art. 27: in einigen Fällen: Grundrechte-Folgenabschätzung (EP, dort Anbieterpflicht)
- Pflichten nach anderen Vorschriften unberührt.

# AI wysokiego ryzyka: Adresat obowiązków



## Dostawca

- Zgodność z art. 8-15 (art. 16) i odpowiednie zarządzanie jakością (art. 17).
- Przechowywanie dokumentacji (art. 18) i automatycznych danych logowania (art. 19)
- Monitorowanie produktów, działania naprawcze, obowiązek informacyjny (PE) (art. 20).
- Informowanie i współpraca z organami nadzoru (art. 21)
- Ustanowienie upoważnionego przedstawiciela (art. 22).
- Ocena zgodności (art. 43).
- Rejestracja systemu AI wysokiego ryzyka (art. 49).

**Ponadto obowiązki importerów (art. 23), dystrybutorów (art. 24), odpowiedzialność w całym łańcuchu wartości (art. 25)**

## Podmiot stosujący (PE, poprzednio: użytkownik) (art. 26):

- Ust. 1: Wykorzystanie zgodnie z instrukcjami obsługi.
- Ust. 2: Personel posiadający wystarczające kompetencje
- Ust. 4: Dane wejściowe muszą odpowiadać celowi systemu i być wystarczająco reprezentatywne.
- Ust. 5: Monitorowanie wdrażania systemu; informowanie dostawców i organów o wszelkich znanych zagrożeniach.
- Ust. 6: Przechowywanie rejestrów zdarzeń
- Ust. 7: Udział przedstawicieli pracowników
- Ust. 11: Informowanie osób dotkniętych
- Ust. 12: Współpraca z organami
- Art. 27: w niektórych przypadkach: Ocena skutków dla praw podstawowych (PE, tam obowiązek dostawcy)
- Obowiązki wynikające z innych przepisów pozostają nienaruszone.



## Hochrisiko-KI: Recht auf Erklärung



- Art. 86 begründet ein Recht auf Erklärung individueller Entscheidungen (angelehnt an Art. 22 DSGVO):
- Personen, die von einer Entscheidung betroffen sind, die der Betreiber auf der Grundlage der Daten aus einem in Anhang III aufgeführten Hochrisiko-KI-System (...) getroffen hat und die rechtliche Auswirkungen hat oder sie in ähnlicher Art erheblich auf eine Weise beeinträchtigt, die ihrer Ansicht nach ihre Gesundheit, ihre Sicherheit oder ihre Grundrechte beeinträchtigt, haben das Recht, vom Betreiber eine klare und aussagekräftige Erläuterung zur Rolle des KI-Systems im Entscheidungsprozess und zu den wichtigsten Elementen der getroffenen Entscheidung zu erhalten.
- Kann gesetzlich ausgeschlossen werden (Abs. 2).

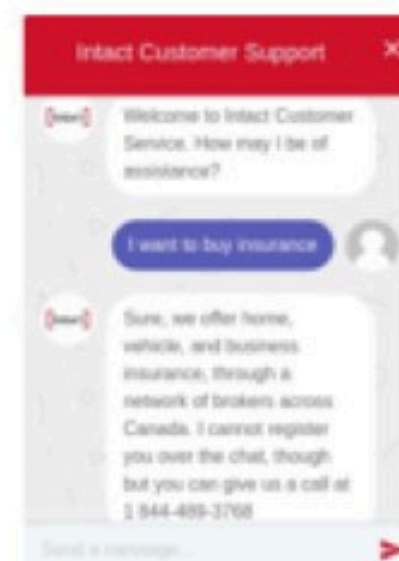
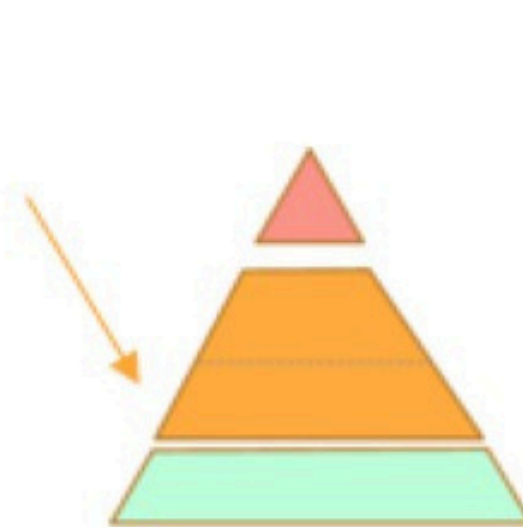
## AI wysokiego ryzyka: Prawo do uzyskania wyjaśnienia



- Art. 86 ustanawia prawo do uzyskania wyjaśnienia indywidualnych decyzji (na podstawie art. 22 RODO):
- Każda osoba, będąca przedmiotem decyzji podjętej przez podmiot stosujący na podstawie wyników systemu AI wysokiego ryzyka wymienionego w załączniku III, (...), która to decyzja wywołuje skutki prawne lub w podobny sposób oddziałuje na tę osobę na tyle znacząco, że uważa ona, iż ma to niepożądany wpływ na jej zdrowie, bezpieczeństwo lub prawa podstawowe, ma prawo uzyskania od podmiotu stosującego jasnego i merytorycznego wyjaśnienia roli tego systemu AI w procedurze podejmowania decyzji oraz głównych elementów podjętej decyzji.
- Możliwość wykluczenia przez ustawę (ust. 2).

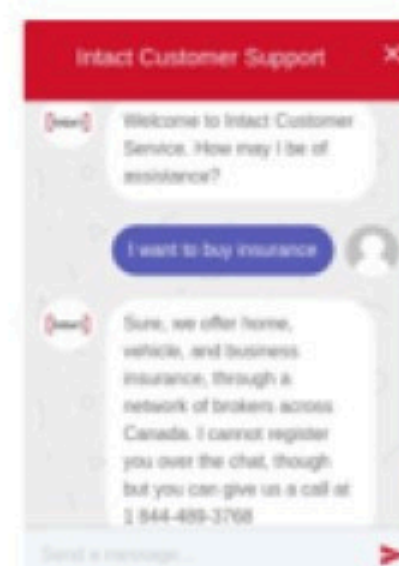
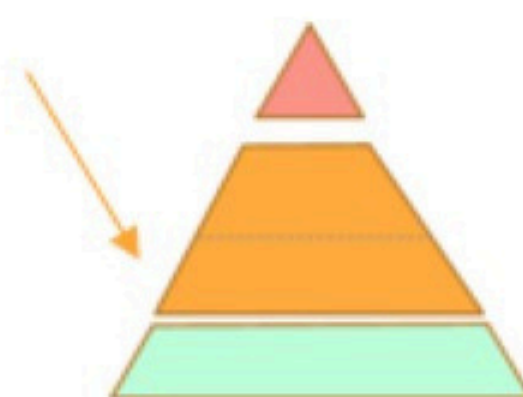


# Transparenzpflicht für Anbieter und Nutzer (Art. 50)



- **KI Systeme, die mit Menschen interagieren** (z.B. Chatbots) müssen über die Interaktion mit KI informieren (Abs. 1).
- **Generative KI-Systeme** müssen Erzeugnisse kennzeichnen (Abs. 2)
- Betreiber eines Emotionserkennungssystems müssen Betroffene informieren (Abs. 3)
- Deep-Fakes müssen gekennzeichnet werden (Abs. 4)

## Obowiązek przejrzystości dla dostawców i użytkowników (art. 50)



- **Systemy AI, które wchodzą w interakcje z ludźmi** (np. chatboty) mają obowiązek informować o interakcjach z udziałem AI (ust. 1).
- **Systemy generatywnej AI** muszą oznakowywać produkty (ust. 2)
- Podmioty stosujące system rozpoznawania emocji muszą informować osoby, których to dotyczy (ust. 3)
- Deep fakes należy odpowiednio oznakować (ust. 4)

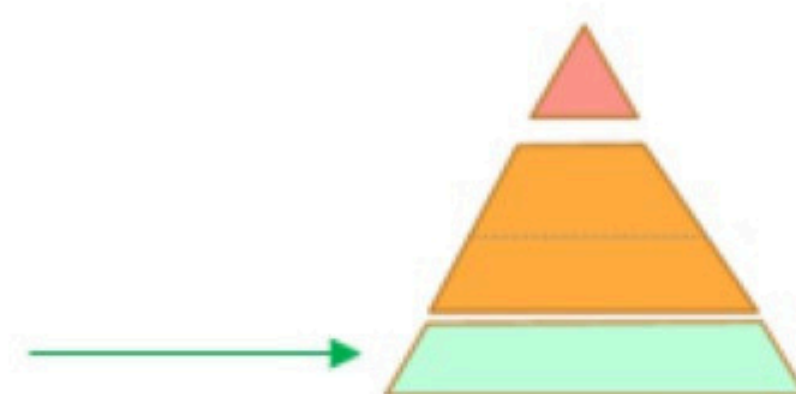


## Andere KI-Systeme: Nur Art. 28, 52 und 69



- Andere als verbotene Systeme iSd Art. 5, Hochrisikosysteme iSd Art. 6, KI-Modelle mit allgemeinem Verwendungszweck (mit oder ohne systemisches Risiko) iSd Art. 51, 53, 55 werden von der KI-VO grds. nicht erfasst.
- Abgesehen von den Transparenzpflichten nach Art. 50 und dem “Aufrücken zum Hersteller” bei Einsatz in Hochrisikosystemen (Art. 25 Abs. 1) unterliegen sie nur freiwilligen codes of conduct nach Art. 56 (und den Regeln außerhalb der KI-VO, v.a. der DSGVO).

## Inne systemy AI: Tylko art. 28, 52 i 69



- Systemy inne niż systemy zakazane w rozumieniu art. 5, systemy wysokiego ryzyka w rozumieniu art. 6, modele AI ogólnego przeznaczenia (z ryzykiem systemowym lub bez) w rozumieniu art. 51, 53, 55 co do zasady nie są objęte rozporządzeniem AI.
- Oprócz obowiązków w zakresie przejrzystości zgodnie z art. 50 i „awansu na producenta” w przypadku wykorzystania w systemach wysokiego ryzyka (art. 25 ust. 1), podlegają one jedynie dobrowolnym kodeksom postępowania zgodnie z art. 56 (i przepisom spoza rozporządzenia AI, w szczególności RODO).



# Folgen des AI Act für das geistige Eigentum

- Geistiges Eigentum ist grundrechtlich fundiert (Art. 17 GRCh).
  - Relevant für die Grundrechtefolgenabschätzung (Art. 27 KI-VO iVm ErwG 48)
- Geistiges Eigentum muss bei Dokumentationspflicht gewahrt werden
  - Vorbehalt geistigen Eigentums für die Vereinbarung entlang der KI-Wertschöpfungskette (Art. 25 Abs. 5 und ErwG 88)
  - Schutz geistigen Eigentums bei Erfüllung von Dokumentationspflichten (Art. 52 Abs. 6, Art. 53 Abs. 1 lit. b, Art. 78 Abs. 1 lit. a, EG 167)
  - Schutz geistigen Eigentums beim Zugang zu Trainingsdaten (Anhang VII zur Konformitätsbewertung Ziffer 4.5)

## Konsequenzen der Gesetzgebung über künstliche Intelligenz für das geistige Eigentum

- Własność intelektualna opiera się na prawach podstawowych (art. 17 Karty praw podstawowych).
  - Istotne dla oceny skutków dla praw podstawowych (art. 27 rozporządzenia AI w zw. z motywem 48)
- Własność intelektualna musi być chroniona w przypadku obowiązków dokumentacyjnych
  - Zastrzeżenie własności intelektualnej na potrzeby porozumienia w całym łańcuchu wartości AI (art. 25 ust. 5 i motyw 88)
  - Ochrona własności intelektualnej przy wypełnianiu obowiązków dokumentacyjnych (art. 52 ust. 6, art. 53 ust. 1 lit. b, art. 78 ust. 1 lit. a, motyw 167)
  - Ochrona własności intelektualnej przy dostępie do danych treningowych (załącznik VII do oceny zgodności, pkt 4.5)



# Folgen des AI Act speziell für das Patentrecht

- Vielfach werden KI-Modelle mit allgemeinen Verwendungszweck mangels technischer Lösung nicht patentierbar sein
  - Vgl. EPA T 702/20, GRUR-RS 2022, 40533 (EP 3 089 081 A1).
  - Aber: Emotional Perception AI Ltd v Comptroller-General of Patents, Designs and Trade Marks [2023] EWHC 2948 (Ch)
- Sind in KI-Systemen verbotene Praktiken zugleich die Patentierung wegen Verstoßes gegen die öffentliche Ordnung aus?
- Etwaige Patentverletzungen von Hochrisiko-KI-Systemen müssen (streng genommen) in die Grundrechtfolgenabschätzung eingestellt werden.
- Wahrung von Patentrechten bei Dokumentationspflichterfüllung wohl weniger relevant, da Inhalt ohnehin offenbart und deshalb kaum vertraulich.
  - Aber relevant für Schutz von Geschäftsgeheimnissen.
  - Zugang zu KI-Dokumentationen kann Aufschluss über Funktionsweise der Systeme geben, was ggf. für die Aufdeckung von Patentverletzungen relevant sein kann.

## Szczególne konsekwencje ustawy o sztucznej inteligencji dla prawa patentowego

- W wielu przypadkach modele AI ogólnego przeznaczenia nie będą podlegały opatentowaniu ze względu na brak rozwiązania technicznego
  - Por. EPA T 702/20, GRUR-RS 2022, 40533 (EP 3 089 081 A1).
  - Ale: Emotional Perception AI Ltd v Comptroller-General of Patents, Designs and Trade Marks [2023] EWHC 2948 (Ch)
- Czy w systemach AI zakazane praktyki jednocześnie są wyłączone z opatentowania z powodu naruszenia porządku publicznego?
- Wszelkie naruszenia patentów przez systemy AI wysokiego ryzyka muszą (ściśle rzecz biorąc) zostać uwzględnione w ocenie skutków dla praw podstawowych.
- Ochrona praw patentowych jest prawdopodobnie mniej istotna przy wypełnianiu obowiązków dokumentacyjnych, ponieważ treść i tak jest ujawniana, a zatem nie jest poufna.
  - Jest to jednak istotne dla ochrony tajemnic przedsiębiorstwa.
  - Dostęp do dokumentacji AI może dostarczyć informacji o sposobie funkcjonowania systemów, co może być istotne dla wykrywania naruszeń patentów.



# Folgen des AI Act speziell für das Urheberrecht

- Anbieter, die KI-Modelle mit allgemeinem Verwendungszweck in der EU in Verkehr bringen, müssen darlegen, wie die Einhaltung des Urheberrechts und v.a. der TDM-Schranken-Schranke (Art. 4 Abs. 3 RL 2019/790) sicherstellt wird (Art. 53 Abs. 1 c, EG 104, 106).
  - Dies gilt unabhängig von dem Ort, wo die urheberrechtlich relevanten Handlungen erfolgt sind (EG 106), um „Race to the Bottom“ zu verhindern.
  - Einhaltung des Urheberrechts wird damit durch die KI-Aufsichtsbehörden in gewissem Umfang durchgesetzt.
  - Zudem Pflicht zur Erstellung und Veröffentlichung einer Zusammenfassung der für das Training verwendeten Inhalte.
  - Überwachung durch das Amt für künstliche Intelligenz (EG 108).
- Klarstellung, dass TDM-Schranke (Art. 4 RL 2019/790 = §§ 44b, 69d UrhG) auch für das Training von (generativen) KI-Systemen gilt (EG 105).

## Szczególne konsekwencje ustawy o sztucznej inteligencji dla prawa autorskiego

- Dostawcy, którzy wprowadzają modele AI ogólnego przeznaczenia do obrotu w UE, muszą przedstawić, w jaki sposób zapewniona jest zgodność z prawem autorskim, a w szczególności z ograniczeniem ograniczeń w odniesieniu do eksploracji tekstów i danych (TDM) (art. 4 ust. 3 dyrektywy 2019/790) (art. 53 ust. 1 lit. c, motyw 104, 106).
  - Ma to zastosowanie niezależnie od miejsca, w którym miały miejsce działania istotne z punktu widzenia praw autorskich (motyw 106), aby uniknąć „wyścigu na dno”.
  - Zgodność z prawem autorskim jest zatem do pewnego stopnia egzekwowana przez organy nadzoru AI.
  - Ponadto obowiązek stworzenia i opublikowania podsumowania treści wykorzystanych do trenowania.
  - Monitorowanie przez Urząd ds. Sztucznej Inteligencji (motyw 108).
- Wyjaśnienie, że ograniczenie TDM (art. 4 dyrektywy 2019/790 = §§ 44b, 69d UrhG) ma również zastosowanie do trenowania (generatywnych) systemów AI (motyw 105).