Der AI Act: State of play

Univ.-Prof. MMMag. Dr. Rainer Palmstorfer, LL.M.
Institut für Europarecht, JKU
rainer.palmstorfer@jku.at

JOHANNES KEPLER UNIVERSITÄT LINZ
Altenberger Straße 69
4040 Linz, Österreich
jku.at

Überblick

- COM (2021) 206 final, veröffentlicht am 21.04.2021
- Rechtsgrundlagen: Art 114 AEUV und Art 16 AEUV
- Rechtsnatur: Verordnung
- Typus: Produktsicherheitsrecht
- Nicht alle Rechtsfragen iZm KI erfasst (geplant: ProduktHaftungsRL, KI-HaftungsRL)
- Umfang: 85 Artikel und 9 Anhänge
- Dezember 2022: Gemeinsamer Standpunkt des Rates (14954/22)
- Juni 2023: Position des EP (P9_TA(2023)0236, 771 Abänderungen)

Ziele des AI Act EP

ErwGr (1a): „Diese Verordnung soll die Werte der Union wahren, dazu beitragen, dass die mit der KI verbundenen Vorteile der gesamten Gesellschaft zugutekommen, Einzelpersonen, Unternehmen, Demokratie und Rechtsstaatlichkeit sowie die Umwelt vor Risiken schützen und zugleich Innovation und Beschäftigung fördern und der Union eine Führungsrolle in diesem Bereich verschaffen.“

Weiter territorialer Anwendungsbereich (Art 2 Abs 1)

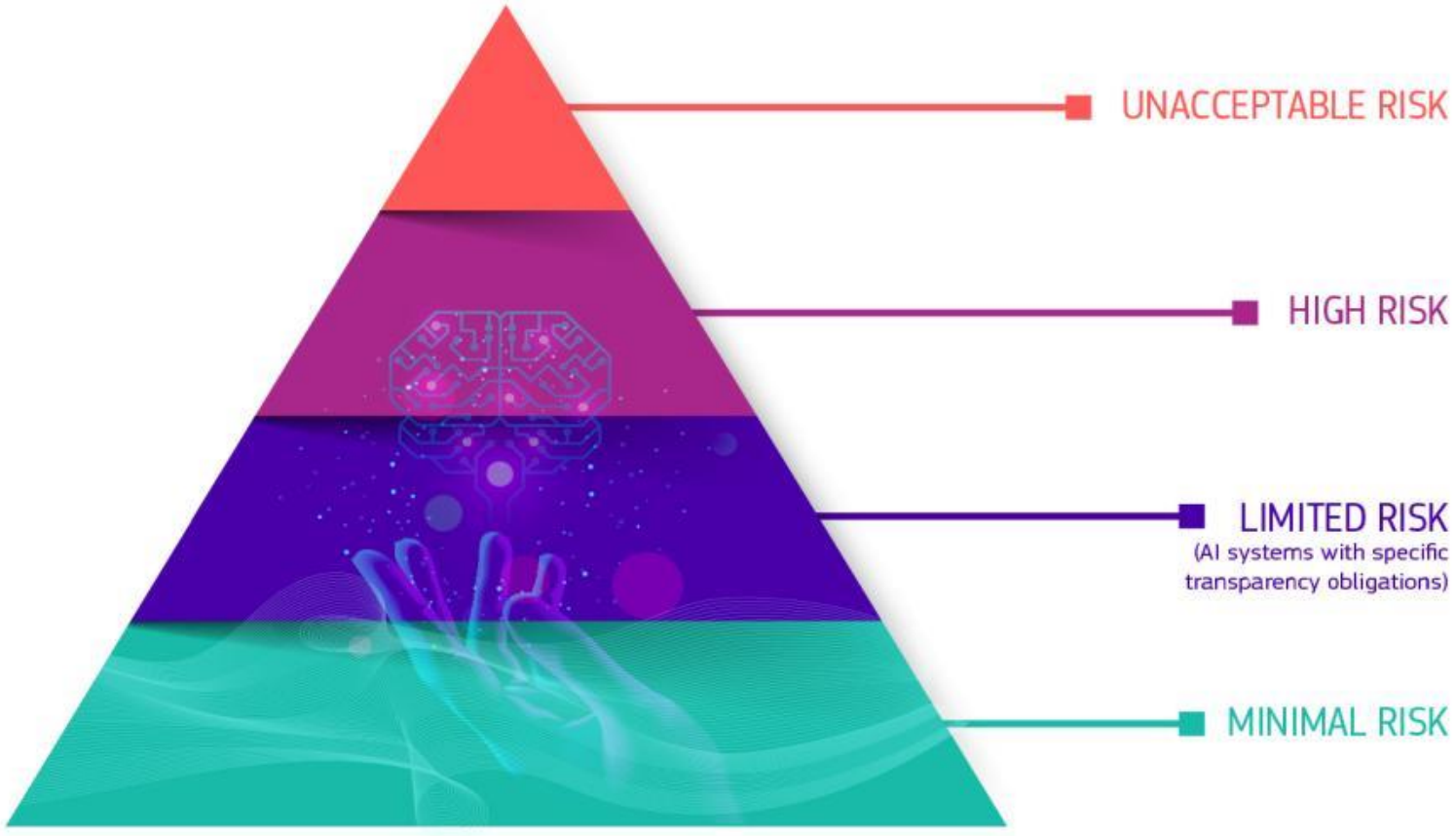
- Anbieter [= private/öffentliche KI-Entwickler], die KI-Systeme in der Union in Verkehr bringen oder in Betrieb nehmen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind.
- Nutzer [= berufliche Nutzung!] von KI-Systemen, die sich in der Union befinden.
- Anbieter und Nutzer von KI-Systemen, die in einem Drittland niedergelassen oder ansässig sind, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird.

Weiter territorialer Anwendungsbereich (Art 2 Abs 1) EP

- Anbieter [= private/öffentliche KI-Entwickler], die KI-Systeme 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 [= berufliche Nutzung!] von KI-Systemen, die sich in der Union befinden.
- Anbieter und Betreiber von KI-Systemen, die in einem Drittland niedergelassen oder ansässig sind, wenn das vom System hervorgebrachte Ergebnis in der Union verwenden soll.
- **Betroffene Personen** [= jede natürliche Personen oder Personengruppe, die einem KI-System unterliegt oder anderweitig davon betroffen ist], die in der Union ansässig sind und deren Gesundheit, Sicherheit oder Grundrechte durch die Verwendung eines KI-Systems, das in der Union in Verkehr gebracht oder in Betrieb genommen wird, beeinträchtigt werden.

Nach Risiko differenzierender Regelungsansatz

ErwGr 14: „Um ein verhältnismäßiges und wirksames verbindliches Regelwerk für KI-Systeme einzuführen, sollte ein klar definierter [horizontaler] risikobasierter Ansatz verfolgt werden. Bei diesem Ansatz sollten Art und Inhalt solcher Vorschriften auf die Intensität und den Umfang der Risiken zugeschnitten werden, die von KI-Systemen ausgehen können. Es ist daher notwendig, [i] bestimmte Praktiken im Bereich der künstlichen Intelligenz zu verbieten [unannehmbares Risiko, verbotene Praktiken] und [ii] Anforderungen an Hochrisiko-KI-Systeme und Verpflichtungen für die betreffenden Akteure sowie [iii] Transparenzpflichten für bestimmte KI-Systeme [geringes Risiko] festzulegen.“



https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_de

Risiko?

- Schlüsselbegriff des KI-Gesetzes, Rechtsbegriff
- Keine Legaldefinition im Kommissionsvorschlag (siehe Art 3)
- Risiko für wen?
  - „hohes Risiko für die Gesundheit und Sicherheit oder für die Grundrechte natürlicher Personen“ (COM(2021) 206 final, 15)

Art 3 Abs 1 (EP)

- 1a. „ ‚**Risiko**‘ die Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens;“
- 1b. „ ‚**erhebliches Risiko**‘ ein Risiko, das aufgrund der Kombination von Schwere, Intensität, Eintrittswahrscheinlichkeit und Dauer seiner Auswirkungen sowie seiner Eigenschaft, eine Einzelperson, eine Vielzahl von Personen oder eine bestimmte Personengruppe zu beeinträchtigen, erheblich ist;“

(Zu?) weiter KI-Begriff (→ Art 3)

„ ‚System der künstlichen Intelligenz' (KI-System) eine Software, die mit einer oder mehreren der in **Anhang I** aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren;"

(Zu?) weiter KI-Begriff (→ Art 3)

„ ‚System der künstlichen Intelligenz' (KI-System) eine Software, die mit einer oder mehreren der in **Anhang I** aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren;" **KOM**

„System der künstlichen Intelligenz" (KI-System) ein System, das so konzipiert ist, dass es mit Elementen der Autonomie arbeitet, und das auf der Grundlage maschineller und/oder vom Menschen erzeugter Daten und Eingaben durch **maschinelles Lernen und/oder logik- und wissensgestützte Konzepte** ableitet, wie eine Reihe von Zielen erreicht wird, und systemgenerierte Ergebnisse wie Inhalte (generative KI-Systeme), Vorhersagen, Empfehlungen oder Entscheidungen hervorbringt, die das Umfeld beeinflussen, mit dem die KI-Systeme interagieren;" **RAT**

„System der künstlichen Intelligenz" (KI-System) ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren kann und das für explizite oder implizite Ziele Ergebnisse wie Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das physische oder virtuelle Umfeld beeinflussen;" **EP (= OECD)**

Verbotene Praktiken

Verbotene Praktiken (Art 5)

- **Techniken der unterschwelligen Beeinflussung**
- **Ausnützung der Schwäche/Schutzbedürftigkeit bestimmter Personengruppen (zB Alter)**
- **Social Scoring** (Bewertung der Vertrauenswürdigkeit natürlicher Personen durch Behörden)
- **Biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken**

Verbotene Praktiken (Art 5) RAT

- **Techniken der unterschwelligen Beeinflussung**
- **Ausnützung der Schwäche/Schutzbedürftigkeit bestimmter Personengruppen (zB Alter)**
- **Social Scoring** (Bewertung der Vertrauenswürdigkeit natürlicher Personen durch Behörden)
- **Biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken**

Verbotene Praktiken (Art 5) RAT

- **Techniken der unterschwelligen Beeinflussung**
- **Ausnützung der Schwäche/Schutzbedürftigkeit bestimmter Personengruppen (zB Alter, auch soziale/wirtschaftliche Lage)**
- **Social Scoring** (Bewertung der Vertrauenswürdigkeit natürlicher Personen durch Behörden und Private)
- **Biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken**

Verbotene Praktiken (Art 5) RAT EP

- **Techniken der unterschwelligen Beeinflussung**
- **Ausnützung der Schwäche/Schutzbedürftigkeit bestimmter Personengruppen (zB Alter, auch soziale/wirtschaftliche Lage)**
- **Social Scoring** (Bewertung der Vertrauenswürdigkeit natürlicher Personen durch Behörden und Private)
- **Biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken**

Verbotene Praktiken (Art 5) RAT EP

- **Techniken der unterschwelligen Beeinflussung**
- **Ausnützung der Schwäche/Schutzbedürftigkeit bestimmter Personengruppen (zB Alter, auch soziale/wirtschaftliche Lage)**
- **Social Scoring** (Bewertung der Vertrauenswürdigkeit natürlicher Personen durch Behörden und Private)
- **Biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen ~~zu Strafverfolgungszwecken~~**

Verbotene Praktiken (Art 5) RAT EP

- **Techniken der unterschwelligen Beeinflussung**
- **Ausnützung der Schwäche/Schutzbedürftigkeit bestimmter Personengruppen (zB Alter, auch soziale/wirtschaftliche Lage)**
- **Social Scoring** (Bewertung der Vertrauenswürdigkeit natürlicher Personen durch Behörden und Private)
- **Biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen ~~zu Strafverfolgungszwecken~~**
- **Einfügung weiterer Verbote (zB Predictive policing, Emotionserkennung in bestimmten Bereichen ua)**

„Zankapfel“ Verbotene Praktiken (Art 5)

Die Erweiterung der Verbotstatbestände (insb das gänzliche Verbot biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen) durch das EP wird als der Hauptkonfliktpunkt im Trilog angesehen. Es wird aber nicht damit gerechnet, dass dies zum Scheitern des Trilogs führt.

Hochrisiko-KI

Hochrisiko-KI

- Hauptteil des AI Act: Titel III (Art 6-51l)
- Zweck: KI-Systeme in sensiblen Bereichen sollen vor Marktzulassung bestimmte Vorgaben erfüllen
  - Art 6 Abs 1: KI-Systeme als Produkt oder Sicherheitskomponente eines Produktes nach bestimmten Harmonisierungsvorschriften (New Legislative Framework)
  - Art 6 Abs 2: KI-Systeme, die bestimmungsgemäß in bestimmten Sektoren eingesetzt werden sollen (Bildung, Strafverfolgung, Beschäftigung, kritische Infrastruktur, Migration ua)
- Vorgaben: Risikomanagement (dh Risikominimierung), Daten/Daten-Governance, Dokumentation, Aufzeichnungspflichten, Transparenz, menschliche Aufsicht, Genauigkeit/Robustheit/Cybersicherheit

Hochrisiko-KI

- Hauptteil des AI Act: Titel III (Art 6-51l)
- Zweck: KI-Systeme in sensiblen Bereichen sollen vor Marktzulassung bestimmte Vorgaben erfüllen
  - Art 6 Abs 1: KI-Systeme als Produkt oder Sicherheitskomponente eines Produktes nach bestimmten Harmonisierungsvorschriften (New Legislative Framework)
  - KI-Systeme, die bestimmungsgemäß in bestimmten Sektoren eingesetzt werden sollen (Bildung, Strafverfolgung, Beschäftigung, kritische Infrastruktur, Migration, Beeinflussung der Wahl, Empfehlungssysteme von sehr großen Onlineplattformen iSd DSA ua), zusätzliches Abstellen auf Gefährdungsgrad
- Vorgaben: Risikomanagement (dh Risikominimierung), Daten/Daten-Governance, Dokumentation, Aufzeichnungspflichten, Transparenz, menschliche Aufsicht, Genauigkeit/Robustheit/Cybersicherheit) Konkretisierung

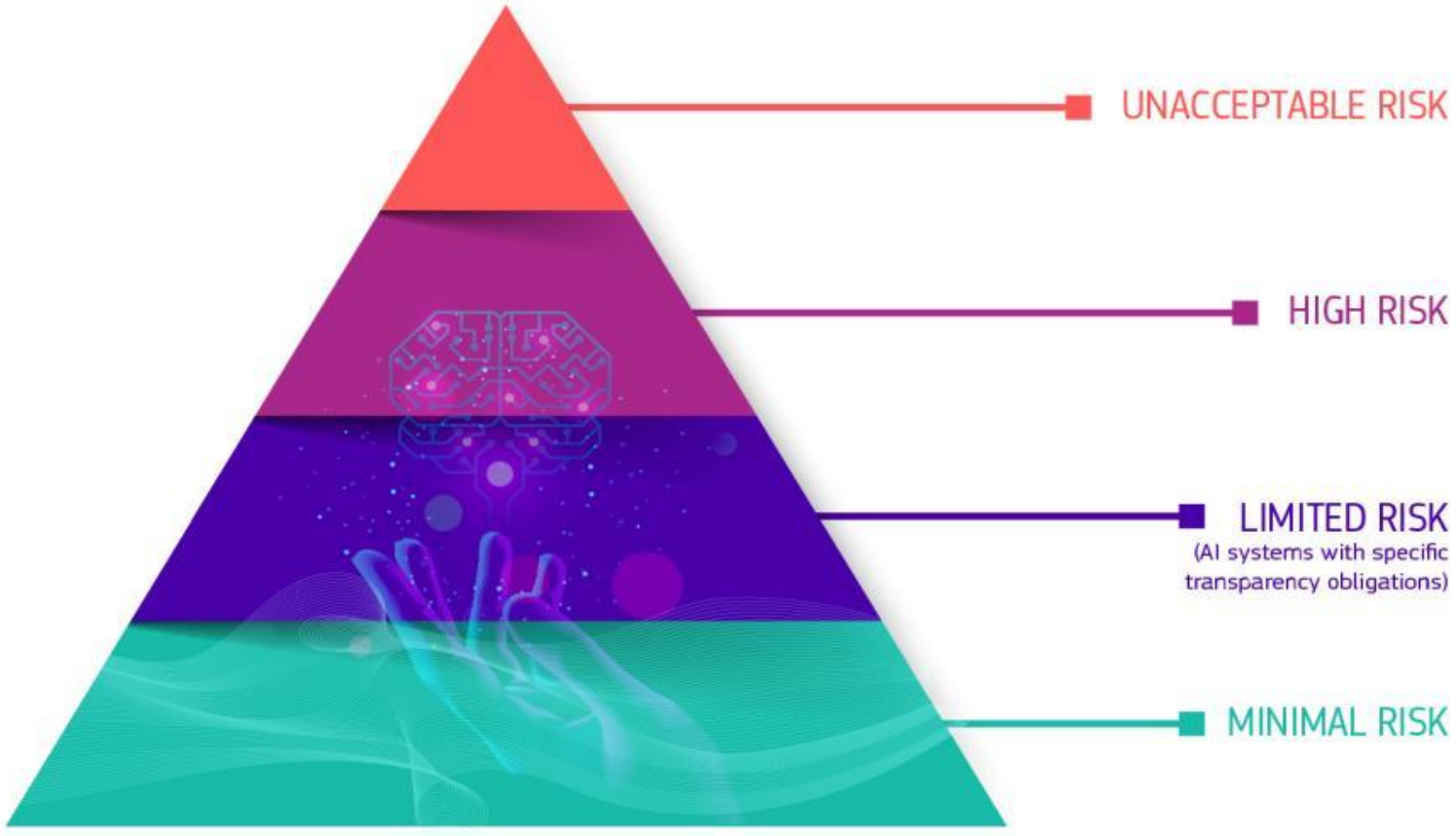
Art 6 Abs 2 EP

„**Zusätzlich** zu den in Absatz 1 genannten Hochrisiko-KI-Systemen gelten KI-Systeme, die unter einen oder mehrere der in Anhang III genannten kritischen Bereiche und Anwendungsfälle fallen, als hochriskant, **wenn sie ein erhebliches Risiko für die Gesundheit, die Sicherheit oder die Grundrechte von natürlichen Personen darstellen**. Fällt ein KI-System unter Anhang III Nummer 2, so gilt es als hochriskant, wenn es ein erhebliches Risiko für die Umwelt birgt.

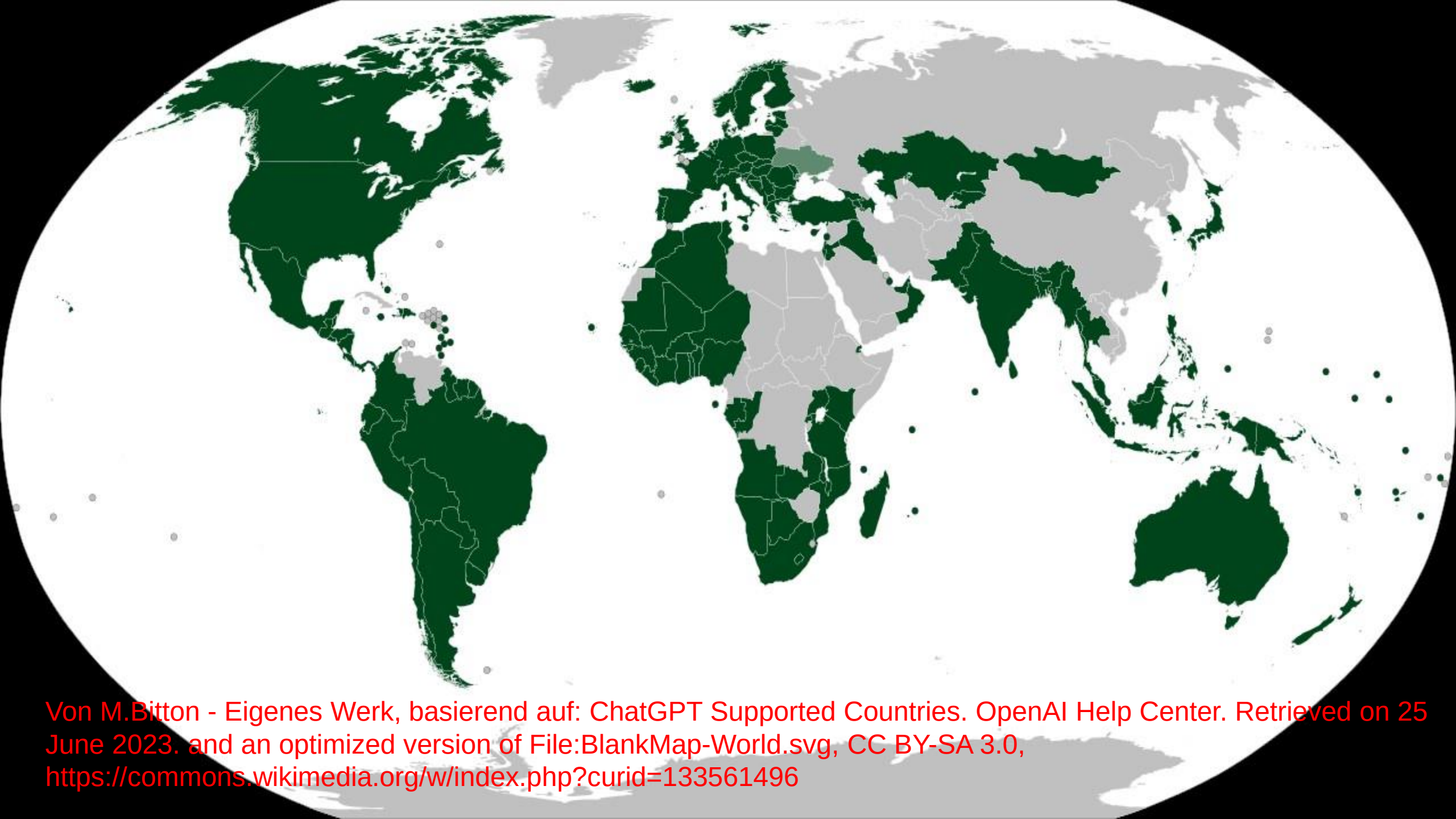
Die Kommission legt sechs Monate vor Inkrafttreten dieser Verordnung nach Anhörung des Amtes für künstliche Intelligenz und der einschlägigen Interessenträger Leitlinien vor, in denen eindeutig festgelegt ist, unter welchen Umständen die Ergebnisse der in Anhang III genannten Systeme der künstlichen Intelligenz ein erhebliches Risiko für die Gesundheit, die Sicherheit oder die Grundrechte natürlicher Personen darstellen und in welchen Fällen dies nicht der Fall ist.“

Förderung?

- Titel VIII: Maßnahmen zur Investitionsförderung
- Art 53-55 AI Act: KI-Reallabore
- AI Act als Rechtsgrundlage für die Verwendung personenbezogener Daten, die für andere Zwecke erhoben werden, zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse.
- Art 54a-b Testen unter realen Bedingungen außerhalb von KI-Reallaboren
- Art 55a Ausnahmen für KMU
- Art 53 Abs 1: Pflicht der MS zur Errichtung eines nationalen Reallabors



https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_de



Von M.Bitton - Eigenes Werk, basierend auf: ChatGPT Supported Countries. OpenAI Help Center. Retrieved on 25 June 2023. and an optimized version of File:BlankMap-World.svg, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=133561496

Artikel 4b RAT

„(1) KI-Systeme mit allgemeinem Verwendungszweck, die als Hochrisiko-KI-Systeme oder als Komponenten von Hochrisiko-KI-Systemen im Sinne von Artikel 6 verwendet werden können, erfüllen die in Titel III Kapitel 2 dieser Verordnung festgelegten Anforderungen ab dem Datum der Anwendung der Durchführungsrechtsakte, die von der Kommission im Einklang mit dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen werden, spätestens jedoch 18 Monate nach Inkrafttreten dieser Verordnung. In diesen Durchführungsrechtsakten wird die Anwendung der in Titel III Kapitel 2 festgelegten Anforderungen präzisiert und an KI-Systeme mit allgemeinem Verwendungszweck angepasst, (…)“

Art 28 b EP
Pflichten des Anbieters eines Basismodells

„(1) Ein Anbieter eines Basismodells muss, bevor er es auf dem Markt bereitstellt oder in Betrieb nimmt, sicherstellen, dass es den in diesem Artikel festgelegten Anforderungen entspricht, unabhängig davon, ob es als eigenständiges Modell oder eingebettet in ein KI-System oder ein Produkt oder unter freien und Open-Source-Lizenzen als Dienstleistung sowie über andere Vertriebskanäle bereitgestellt wird.

(2) Für die Zwecke von Absatz 1 muss der Anbieter eines Basismodells

a) durch geeignete Planung, Erprobung und Analyse die Identifizierung, Verringerung und Abschwächung von vernünftigerweise vorhersehbaren Risiken für Gesundheit, Sicherheit, Grundrechte, Umwelt sowie Demokratie und Rechtsstaatlichkeit vor und während der Entwicklung mit geeigneten Methoden, z. B. unter Einbeziehung unabhängiger Experten, sowie die Dokumentation der verbleibenden nicht abwendbaren Risiken nach der Entwicklung nachweisen; (…)“

Art 28 b EP
Pflichten des Anbieters eines Basismodells

„(4) Anbieter von Basismodellen, die in KI-Systemen verwendet werden, die speziell dazu bestimmt sind, mit unterschiedlichem Grad an Autonomie Inhalte wie komplexe Texte, Bilder, Audio- oder Videodateien zu generieren (‚generative KI'), sowie Anbieter, die ein Basismodell in ein generatives KI-System integrieren, müssen zusätzlich

a) (…) Transparenzpflichten nachkommen;

b) das Basismodell so gestalten und gegebenenfalls weiterentwickeln, dass ein angemessener Schutz gegen die Erzeugung von Inhalten, die gegen das Unionsrecht verstoßen, nach dem allgemein anerkannten Stand der Technik und unbeschadet der Grundrechte, einschließlich des Rechts auf freie Meinungsäußerung, sichergestellt ist; (…)"

Überwachung

- Durch Marktüberwachungsbehörden der MS bzw durch Europäischen Datenschutzbeauftragten (bei Unionshandeln)
- Europäischer Ausschuss für Künstliche Intelligenz (Beratung)
- Sanktionsregelungen durch MS zu erlassen (Art 71: Geldbußen)
- Keine Regelung der Rechte der Betroffenen
  - AI Act soll Einzelne schützen (Grundrechtsschutz!)
  - Keine Regelungen zum Rechtsschutz (kein Recht auf Beschwerde analog DSGVO)
- Keine Regelungen zu Haftungsfragen (Vorschlag für Produkthaftungs-RL, COM(2022) 495 final; Vorschlag für KI-Haftungs-RL, COM(2022) 496 final)

Überwachung RAT

- Durch Marktüberwachungsbehörden der MS bzw durch Europäischen Datenschutzbeauftragten (bei Unionshandeln)
- Europäischer Ausschuss für Künstliche Intelligenz (Beratung)
- Sanktionsregelungen durch MS zu erlassen (Art 71: Geldbußen)
- Keine Regelung der Rechte der Betroffenen
  - AI Act soll Einzelne schützen (Grundrechtsschutz!)
  - Keine Regelungen zum Rechtsschutz (Recht auf Beschwerde bei Marktüberwachungsbehörde, siehe Art 63 Abs 11)
- Keine Regelungen zu Haftungsfragen (Vorschlag für Produkthaftungs-RL, COM(2022) 495 final; Vorschlag für KI-Haftungs-RL, COM(2022) 496 final)

Überwachung EP

- Durch eine nationale Aufsichtsbehörde der MS bzw durch Europäischen Datenschutzbeauftragten (bei Unionshandeln)
- Europäisches Amt für Künstliche Intelligenz (Rechtspersönlichkeit, Beratung und Koordinierung)
- Sanktionsregelungen durch MS zu erlassen (Art 71: höhere Geldbußen)
- Keine Regelung der Rechte der Betroffenen
  - AI Act soll Einzelne schützen (Grundrechtsschutz!)
  - Keine Regelungen zum Rechtsschutz (Art 68a: Recht auf Beschwerde bei einer nationalen Aufsichtsbehörde, Art 68b: Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen eine nationale Aufsichtsbehörde, Art 68c: Recht auf Erläuterung der individuellen Entscheidungsfindung)

Art 68a EP

(1) „Jede natürliche Person oder Gruppe von natürlichen Personen hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer nationalen Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn sie der Ansicht ist, dass das sie betreffende KI-System gegen diese Verordnung verstößt.“ [vgl Art 77 DSGVO]

Fazit

- Keine unüberwindbaren Hindernisse zum Abschluss des AI Act noch 2023, Inkrafttreten wohl Ende 2025
- Trotz seines Umfangs gibt der AI Act nicht sämtliche Antworten auf das Phänomen KI
- Stärkung des Rechtsschutzes für Individuen ist konsequent und zu begrüßen
- Es bleibt abzuwarten, wie sich der AI Act in das vorgefundene Regelungsgefüge (ua DSGVO) einfügt
- Zentral wird die Konkretisierung seiner Vorgaben durch die KOM und Normungsorganisationen sein
- Ob der AI Act in der Lage ist, Europa eine Führungsrolle im Bereich der KI zu sichern, bleibt abzuwarten


JOHANNES KEPLER
UNIVERSITÄT LINZ
Vielen Dank für
Ihre
Aufmerksamkeit!
© Johannes Kepler Universität Linz