universität wien

Der AI Act – praxistauglicher Verbraucherschutz(?)

Univ.-Prof. Dr. Christiane Wendehorst, LL.M. (Cambridge)

RTR, 7. Oktober 2024

universität wien

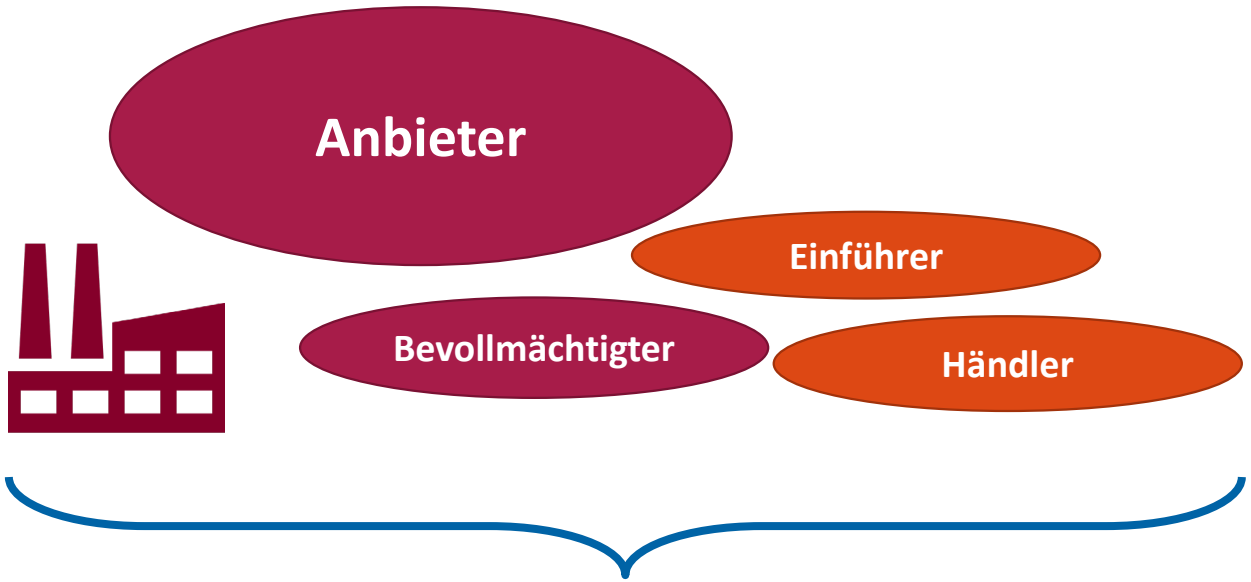
1 Das Regulierungskonzept des AI Act

2 Der AI Act als Verbraucherschutzrecht

3 Verbleibende Probleme – das Beispiel der KI-Definition

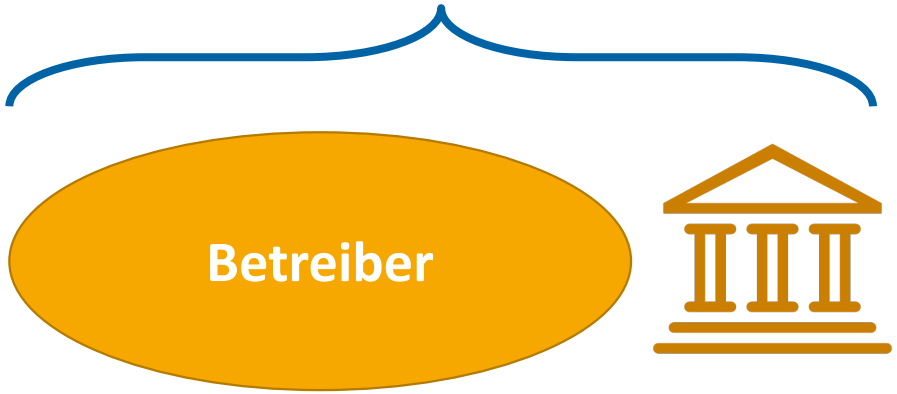
1 Das Regulierungskonzept des AI Act

AI Act als Produktsicherheitsrecht



Klassische Wirtschaftsakteure nach Produktsicherheits- und Marktüberwachungsrecht („neuer Rechtsrahmen“)

Neu: Betreiber als Person mit ähnlichen Pflichten wie Akteure in der Vertriebskette



universität wien

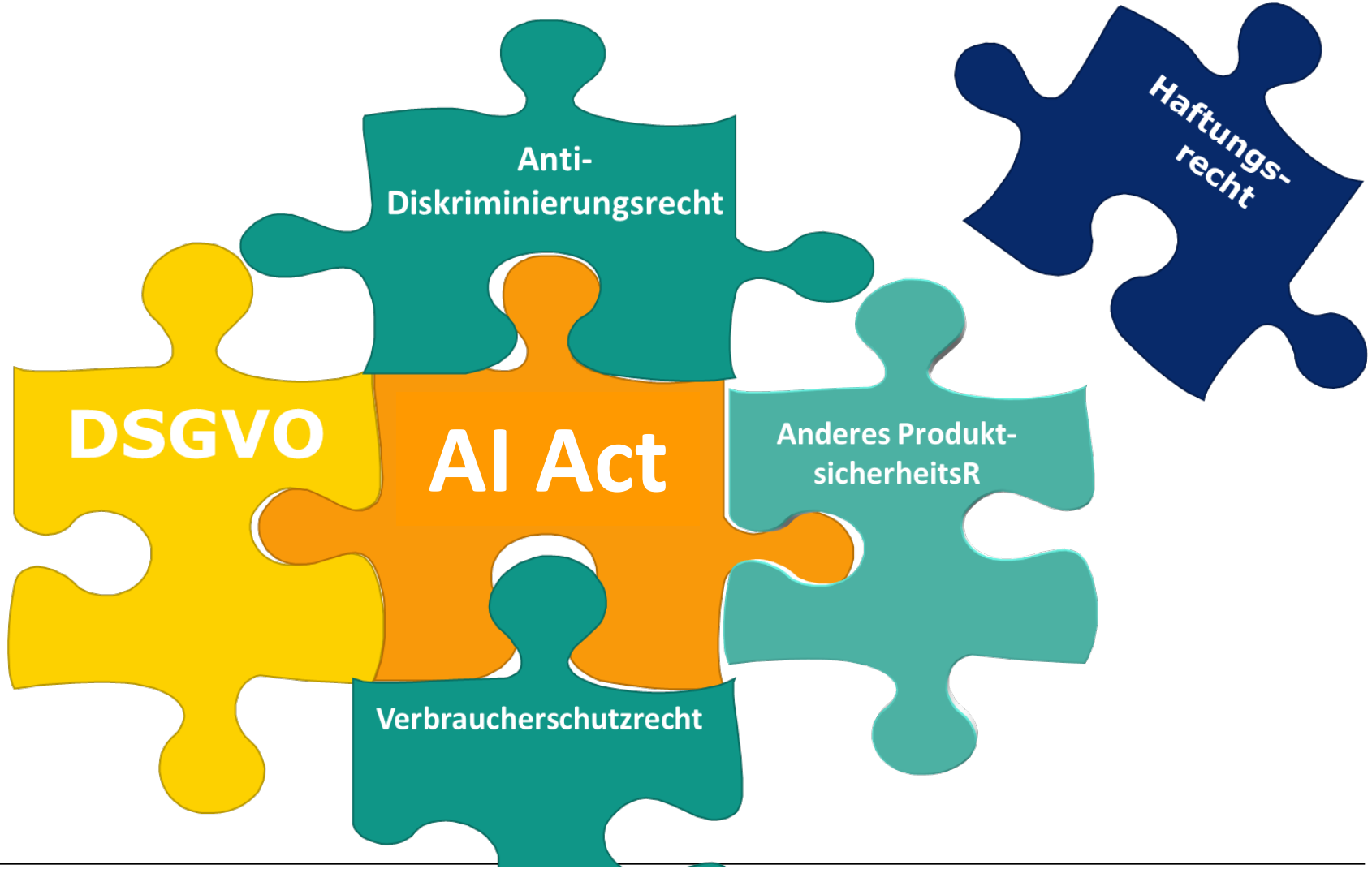
AI Act als Produktsicherheitsrecht

- AI Act enthält KEINE Haftungsbestimmungen
  - aber KI-Systeme von neuer Produkthaftungs-RL erfasst (Problem: gilt nur für bestimmte Schadenstypen)
  - Schicksal des Entwurfs für eine KI-Haftungs-RL unsicher (baut auf Tatbeständen der Verschuldenshaftung nach nationalem Recht auf)
  - viele Vorschriften des AI Act sind als Schutzgesetze zu qualifizieren, so dass ihre Verletzung über §§ 1295, 1311 ABGB ohnehin zur Haftung führt
- AI Act enthält KAUM Individualrechte (aber: Recht auf Erläuterung, Beschwerderecht)
- Whistleblowing-RL und Verbandsklagen-RL anwendbar

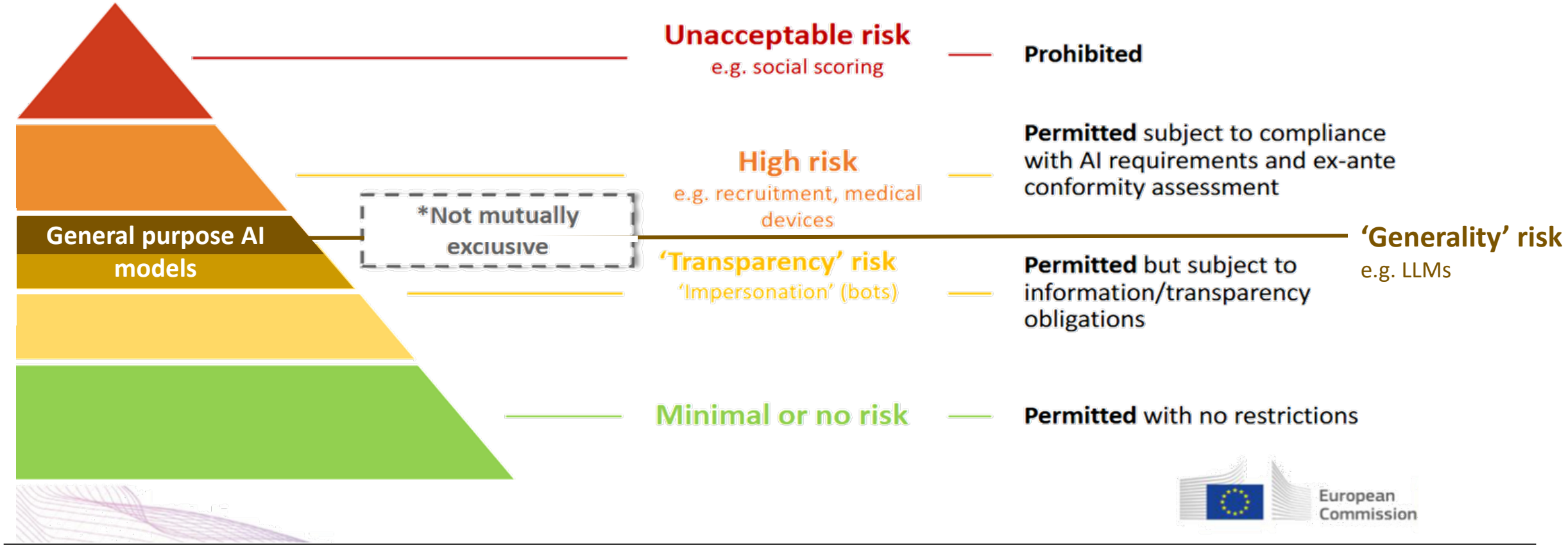
Zusammenspiel mit anderen Rechtsakten

Problem:

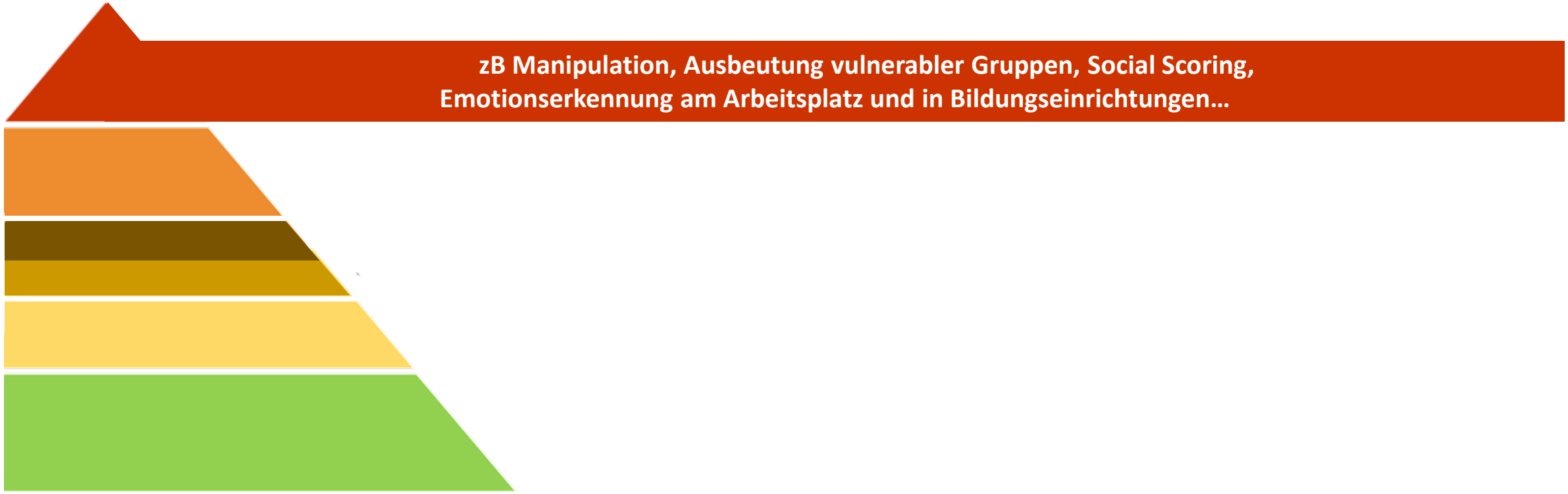
Fehlen einer allgemeinen Zurechnungsnorm, welche das „Verhalten“ von KI ihrem Betreiber strikt zurechnen würde!



Risikobasierter Regulierungsansatz



Verbotene KI-Praktiken



Hochrisiko-KI-Systeme

KI als Produkt oder Sicherheitskomponente für Produkt, das nach ProdSicherheitsR Konformitätsbewertung durch Dritte unterliegt

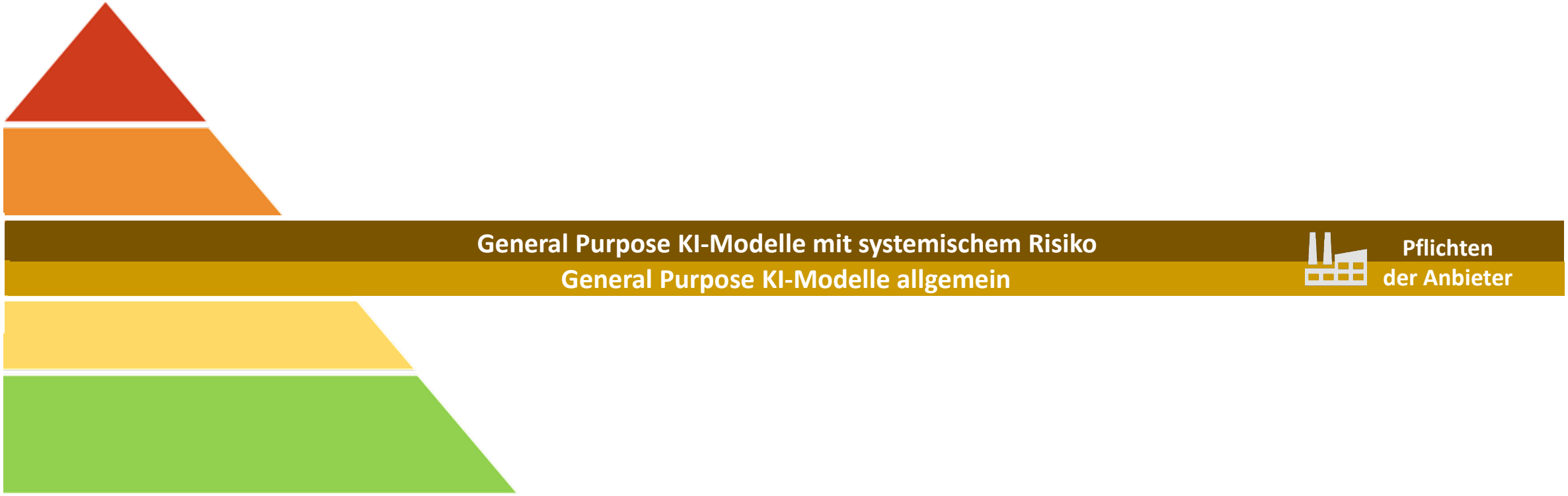
zB Medizinprodukte oder Maschinenprodukte mit KI-Komponenten

In Anhang III angeführte KI-Systeme, sofern Risiko nicht ausnahmsweise nicht erheblich

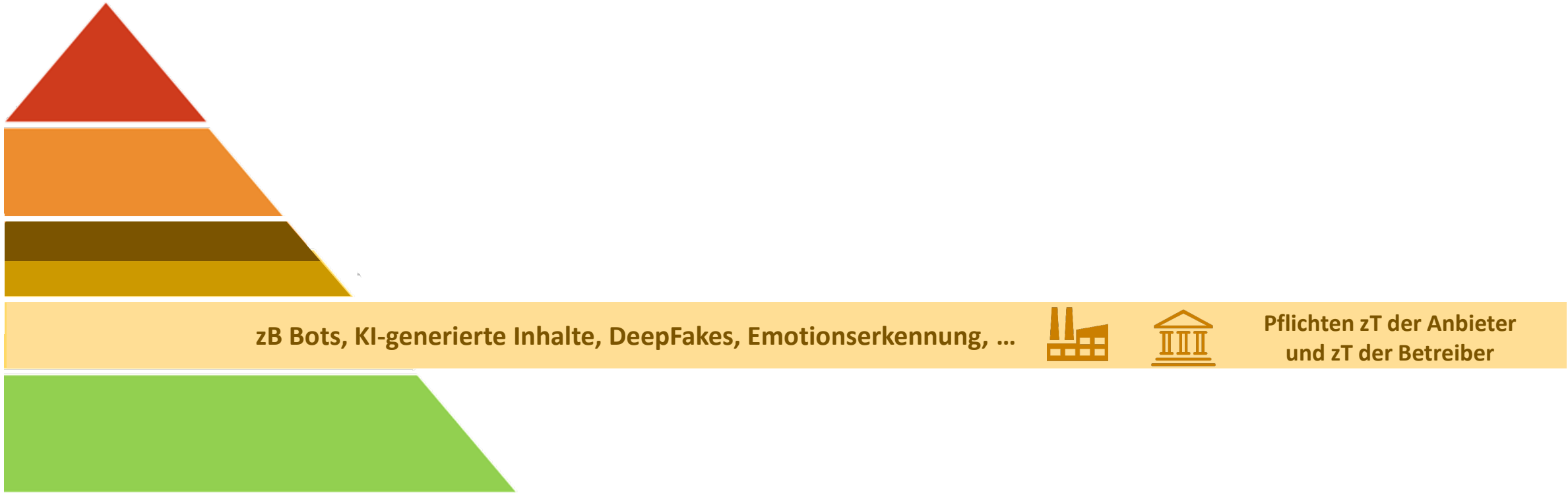
zB viele biometrische KI-Anwendungen, Credit Scoring, Recruitment, Risikobewertung bei Lebens- und Krankenversicherungen …

Hochrisiko-KI-Systeme

KI-Modelle mit allgemeinem Verwendungszweck



KI-Systeme mit erhöhtem Transparenzbedarf



universität wien

2 Der AI Act als Verbraucherschutzrecht

Die drei Säulen des Verbraucherschutzes …

… und ihr Niederschlag in Artikel 6

Artikel 6
Einstufungsvorschriften für Hochrisiko-KI-Systeme

(1) Ungeachtet dessen, ob ein KI-System unabhängig von den unter den Buchstaben a und b genannten Produkten in Verkehr gebracht oder in Betrieb genommen wird, gilt es als Hochrisiko-KI-System, wenn die beiden folgenden Bedingungen erfüllt sind:

a) das KI-System soll als Sicherheitsbauteil eines unter die in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union fallenden Produkts verwendet werden oder das KI-System ist selbst ein solches Produkt;

b) das Produkt, dessen Sicherheitsbauteil gemäß Buchstabe a das KI-System ist, oder das KI-System selbst als Produkt muss einer Konformitätsbewertung durch Dritte im Hinblick auf das Inverkehrbringen oder die Inbetriebnahme dieses Produkts gemäß den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union unterzogen werden.

(2) Zusätzlich zu den in Absatz 1 genannten Hochrisiko-KI-Systemen gelten die in Anhang III genannten KI-Systeme als hochriskant.

Sicherheits-risiken

Grundrechts-risiken

Die acht „Bereiche“ in Anhang III

ANHANG III

Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2

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

1. Biometrie, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:
2. Kritische Infrastruktur: KI-Systeme, die bestimmungsgemäß als Sicherheitsbauteile im Rahmen der Verwaltung und des Betriebs kritischer digitaler Infrastruktur, des Straßenverkehrs oder der Wasser-, Gas-, Wärme- oder Stromversorgung verwendet werden sollen
3. Allgemeine und berufliche Bildung
4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit
5. Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen:
6. Strafverfolgung, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:
7. Migration, Asyl und Grenzkontrolle, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:
8. Rechtspflege und demokratische Prozesse

Sicherheitsrisiken

Wirtschaftl Risiken

Grundrechts-risiken

universität wien

Ausnahmen im Einzelfall

(3) Abweichend von Absatz 2 gilt ein in Anhang III genanntes KI-System 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.

Unterabsatz 1 gilt, wenn eine der folgenden Bedingungen erfüllt ist:

a) das KI-System ist dazu bestimmt, eine eng gefasste Verfahrensaufgabe durchzuführen;

b) das KI-System ist dazu bestimmt, das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit zu verbessern;

c) das KI-System ist dazu bestimmt, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, und ist nicht dazu gedacht, die zuvor abgeschlossene menschliche Bewertung ohne eine angemessene menschliche Überprüfung zu ersetzen oder zu beeinflussen; oder

d) das KI-System ist dazu bestimmt, eine vorbereitende Aufgabe für eine Bewertung durchzuführen, die für die Zwecke der in Anhang III aufgeführten Anwendungsfälle relevant ist.

Ungeachtet des Unterabsatzes 1 gilt ein in Anhang III aufgeführtes KI-System immer dann als hochriskant, wenn es ein Profiling natürlicher Personen vornimmt.

Grundrechts-risiken

universität wien

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

a) KI-Systeme, die bestimmungsgemäß von Behörden oder im Namen von Behörden verwendet werden sollen, um zu beurteilen, ob natürliche Personen Anspruch auf grundlegende öffentliche Unterstützungsleistungen und -dienste, einschließlich Gesundheitsdiensten, haben und ob solche Leistungen und Dienste zu gewähren, einzuschränken, zu widerrufen oder zurückzufordern sind;

Wirtschaftl Risiken

b) KI-Systeme, die bestimmungsgemäß für die Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen verwendet werden sollen, mit Ausnahme von KI-Systemen, die zur Aufdeckung von Finanzbetrug verwendet werden;

c) KI-Systeme, die bestimmungsgemäß für die Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Lebens- und Krankenversicherungen verwendet werden sollen;

universität wien

AI Act als Verbraucherschutzrecht

- Der AI Act verwendet nicht den Begriff des Verbrauchers und schützt natürliche Personen nicht in einer bestimmten Rolle (wohl aber sind natürliche Personen, die für persönliche und nicht berufliche Zwecke handeln, von den Betreiberpflichten ausgenommen)
- Der AI Act betont den grundrechtlichen Verbraucherschutz und daneben den gesundheitlich-technischen Verbraucherschutz, während der wirtschaftliche Verbraucherschutz (zB KI in Vertragsverhältnissen) stark „unterbelichtet“ bleibt.
- Klassischer, wirtschaftlicher Verbraucherschutz, wie wir ihn aus dem Verbrauchervertragsrecht oder Lauterkeitsrecht kennen, betrifft zB KI-Systeme zur Kreditwürdigkeitsprüfung und zur Risikobewertung bei Lebens- und Krankenversicherungen – sofern die in der Praxis verwendeten Systeme überhaupt dem AI Act unterfallen!

universität wien

3

Verbleibende Probleme – das Beispiel der KI-Definition

universität wien

Definition eines KI-Systems in Art. 3 Nr. 1 AI Act

Artikel 3

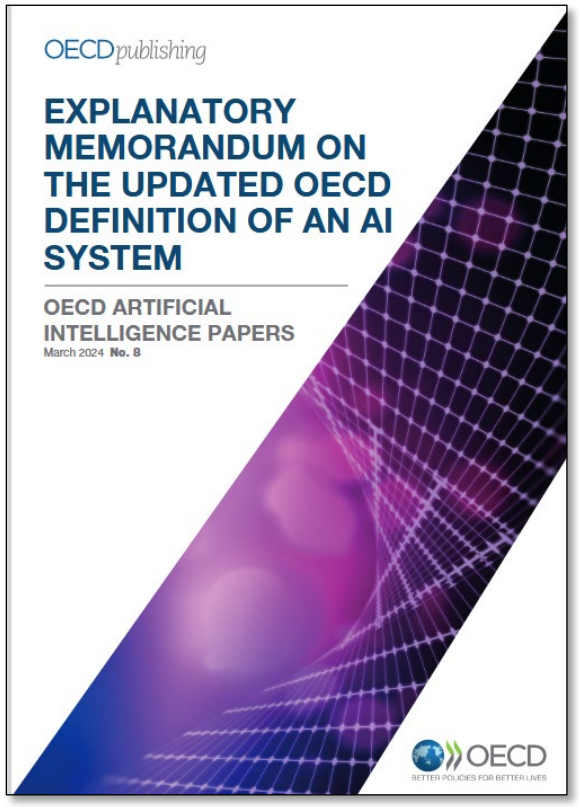
Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

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

universität wien

OECD 2019/2023



The OECD definition of an AI system contained in the OECD AI Principles (OECD, 2019[1]); (OECD, 2019[2]) built on the conceptual view of AI detailed in Artificial Intelligence: A Modern Approach (Russell and Norvig, 2009[3]). It read: "*An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy*".

The text above is replaced with the following updated definition:

> *An AI system is a machine-based system that ~~can~~, for ~~a given set of human-defined~~ explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as ~~makes~~ predictions, content, recommendations, or decisions that can influenc~~ing~~e physical ~~real~~ or virtual environments. Different AI systems ~~are designed to operate with~~ varying in their levels of autonomy and adaptiveness after deployment.*

The updated definition reads as follows:

> ***An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.***

1. Ein maschinengestütztes System …
2. … das auf einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist …
3. … und das nach seiner Betriebsaufnahme anpassungsfähig sein kann …
4. … und das aus den erhaltenen Eingaben … ableitet, WIE Ausgaben … erstellt werden …
5. … für explizite oder implizite Ziele …
6. … Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen …
7. … die physische oder virtuelle Umgebungen beeinflussen können.

Bis auf Nr 6 sind die Tatbestandsmerkmale für eine Abgrenzung nicht hilfreich bzw nahezu unverständlich.

Die Definition könnte fast alle oder fast keine der heute gebräuchlichen IT-Systeme erfassen.

universität wien

Artikel 96

Leitlinien der Kommission zur Durchführung dieser Verordnung

(1) Die Kommission erarbeitet Leitlinien für die praktische Umsetzung dieser Verordnung, die sich insbesondere auf Folgendes beziehen:

[...]

f) die Anwendung der Definition eines KI-Systems gemäß Artikel 3 Nummer 1.

Fazit: Kommission hat fast völlige Freiheit bei der Konkretisierung!

universität wien

„Drei-Faktor-Ansatz“

Faktor I:

Rolle von Daten oder (domänenspezifischem) Erfahrungswissen bei der Entwicklung

Faktor II:

Rolle zielorientierter Optimierung bei der Anwendung (schließt ggf Adaptivität ein)

Faktor III:

Ausmaß formaler Unbestimmtheit bei den Ausgaben

Wendehorst, Nessler et al in MMR 2024

Anwendung	Faktor I Entste-hung	Faktor II Funk-tion	Faktor III Ergebnisse/ Einsatzfel-der	Emp-fehlung
OCR (maschinengeschrie-bener Text)	++	0	0	nicht erfasst
OCR (Handschrift)	++	0/++	+	erfasst
Chatbot auf Basis eines festen Open Source LLMs	++	0	++	erfasst
Chatbot mit API-Zu-gang zu einem LLM	++	++	++	erfasst
Suchmaschine Google, Duck-Duck-Go, Bing	++	0	++	erfasst
Empfehlungssystem in Amazon	++	++	++	erfasst
Timeline und Filte-rung bei X (früher Twitter)	++	++	++	erfasst
Empfehlungssystem Spotify	++	0	++	erfasst
Bonitäts-Checks (zB KSV und SCHUFA)	+/++	0	++	erfasst
Medizinische Bild-diagnostik (zB Haut-krebs, CT-/MRT-Bilder)	++	0	++	erfasst
Stundenplan-Generator	0	+	+/0	nicht erfasst
Routenplaner, Navigationssystem	0	+	0	nicht erfasst
Predictive Mainte-nance	++	0	++	erfasst
Adaptiver Heizungs-regler	0	++	0	nicht erfasst
Adaptive Regler in der Robotik (zB „Spot“)	0	++	+	erfasst
Excel Sheet	++/+/0	++/+/0	++/+/0	(nicht) erfasst
Rechtschreib- und Grammatikprüfung	++	0	0	nicht erfasst

Wenn noch Fragen offen sind … ;-)

Neu Toptitel Erschienen: 20.09.2024

Martini / Wendehorst

KI-VO: Verordnung über Künstliche Intelligenz

Kommentar
Buch. Hardcover (Leinen)
2024
XXII, 1178 S.
C.H.BECK. ISBN 978-3-406-81136-4
Format (B x L): 16,0 x 24,0 cm
Gewicht: 1610 g

Zusammenfassung

- Die EU folgt mit dem AI Act einem risikobasierten und produktsicherheitsrechtlichen Ansatz, welcher der Struktur des „neuen Rechtsrahmens“ folgt und sich weitgehend harmonisch in das bestehende Produktsicherheits- und Marktüberwachungsrecht einpasst.
- Der AI Act dient primär dem grundrechtlichen und dem gesundheitlich-technischen Verbraucherschutz, während der wirtschaftliche Verbraucherschutz nur marginal adressiert worden ist. Diesbezüglich bedarf es weiterer Maßnahmen, insb im Bereich des Verbrauchervertragsrechts.
- Die Schnittstelle zwischen AI Act und existierendem Verbraucherschutzrecht (und Anti-Diskriminierungsrecht usw) würde besser funktionieren, wenn eine Zurechnungsnorm existierte, die das „Verhalten“ von KI ihrem Betreiber strikt zurechnet.
- Was der AI Act für den Verbraucherschutz wirklich leistet, hängt noch von der Konkretisierung zentraler Normen ab, wie etwa der Definition dessen, was überhaupt ein KI-System ist.