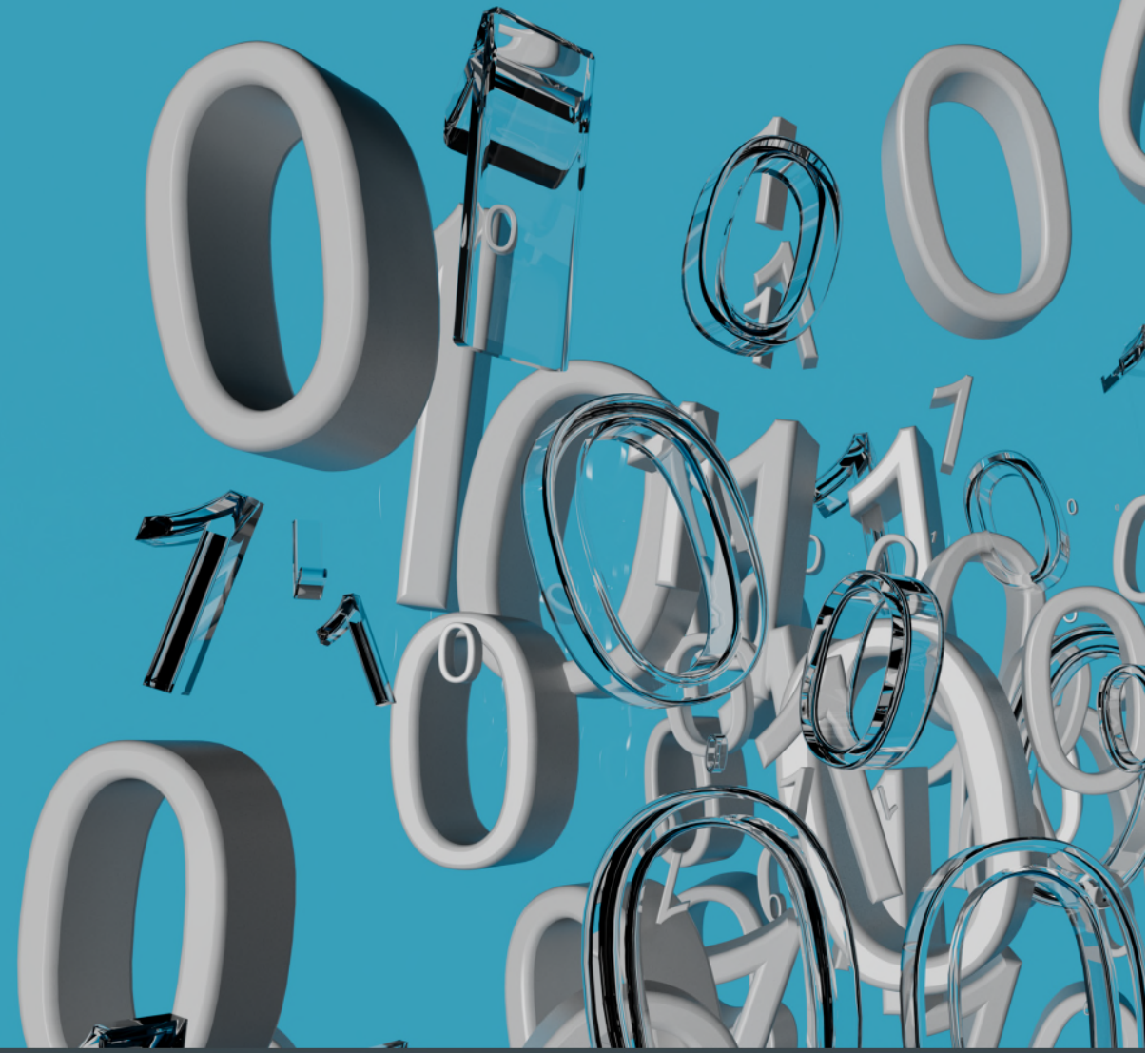


„AI Act“ und „AI Liability Directive“ – ein Überblick

Digital Day, München, 11. Mai 2023

Christopher Götz, LL.M.
Dr. Tina Gausling, LL.M.

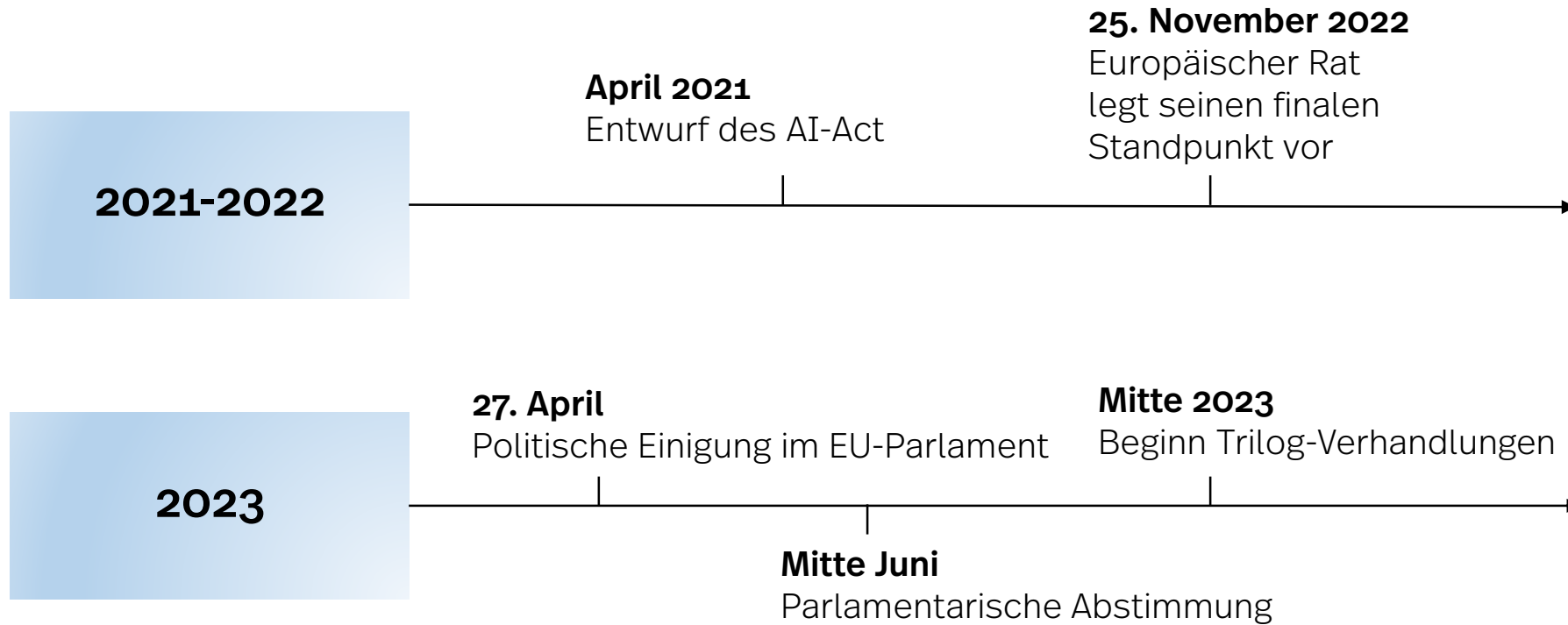


Überblick	Status Quo
• April 2021: Erster Entwurf des Artificial Intelligence Acts (AI-Act) der EU Kommission • EU-Verordnung, die in allen ihren Teilen verbindlich und unmittelbar in jedem EU-Mitgliedsstaat gelten wird • Relevanz für öffentlichen und privaten Sektor • Entwurf durchläuft gerade das EU-Gesetzgebungsverfahren	• Letzter öffentlicher Entwurf: • Council of the EU: 25. November 2022 • „General Approach“ • Nicht-öffentliche Debatten?

AI Act - Timeline



Timeline



Was gilt als „KI – System“?



„KI-System“ – Definition (Stand April 2023):

*„ist ein ~~maschinengestütztes~~ System, das so konzipiert ist, dass es mit unterschiedlichen **Autonomie**-Graden arbeitet **und** das zu expliziten oder impliziten Zwecken **Ergebnisse wie Vorhersagen, Empfehlungen oder Entscheidungen erzeugen kann**, die physische oder virtuelle Umgebungen beeinflussen“*

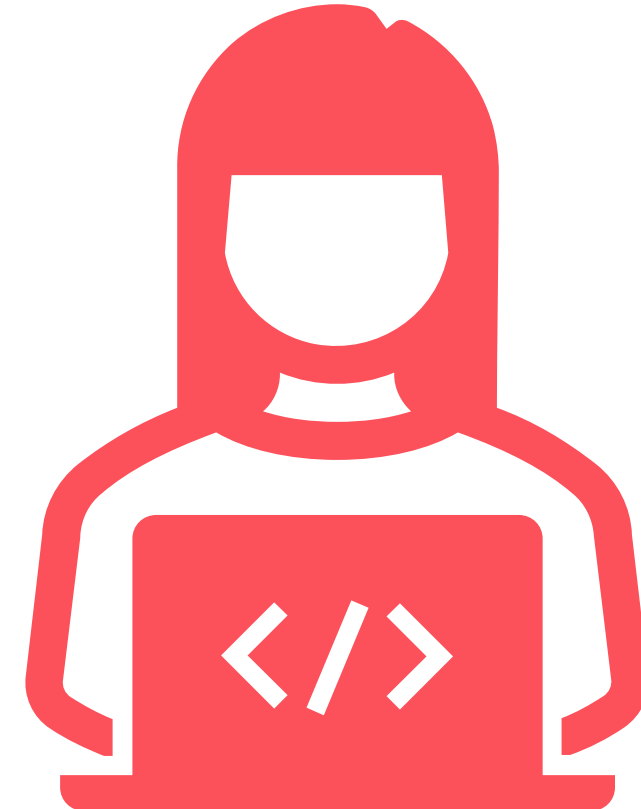
- Engere Definition von KI-Systemen als im Ursprungs-Entwurf, um von klassischen Softwaresystemen/Algorithmen abzugrenzen!
- OECD - KI-Definition: fast deckungsgleich

Wer ist vom AI Act betroffen?

Scope

EU (Niederlassung / Präsenz)

- ❑ „Anbieter“, die KI Systeme in EU in Verkehr bringen / in Betrieb nehmen
 - Entwickler bzw. Firmen/Behörden, die im Auftrag entwickeln lassen
 - unter eigenen Marke auf den Markt bringt/in Betrieb nimmt



Qualifikation als „Anbieter“?

Scope

Achtung!

- ❑ Nat. / jur, Personen, die z.B. (Hochrisiko) KI-System, das bereits auf Markt,
 - mit ihrem Namen/Marke versehen oder
 - eine wesentliche Änderung an dem KI-System vornehmen

- ❑ Drittprodukt-Hersteller, wenn
 - KI-System als Sicherheitskomponente in einem Produkt verwendet wird und
 - zusammen mit diesem Produkt unter eigener Marke auf Markt bringt



Wer ist noch vom AI Act betroffen?

Scope

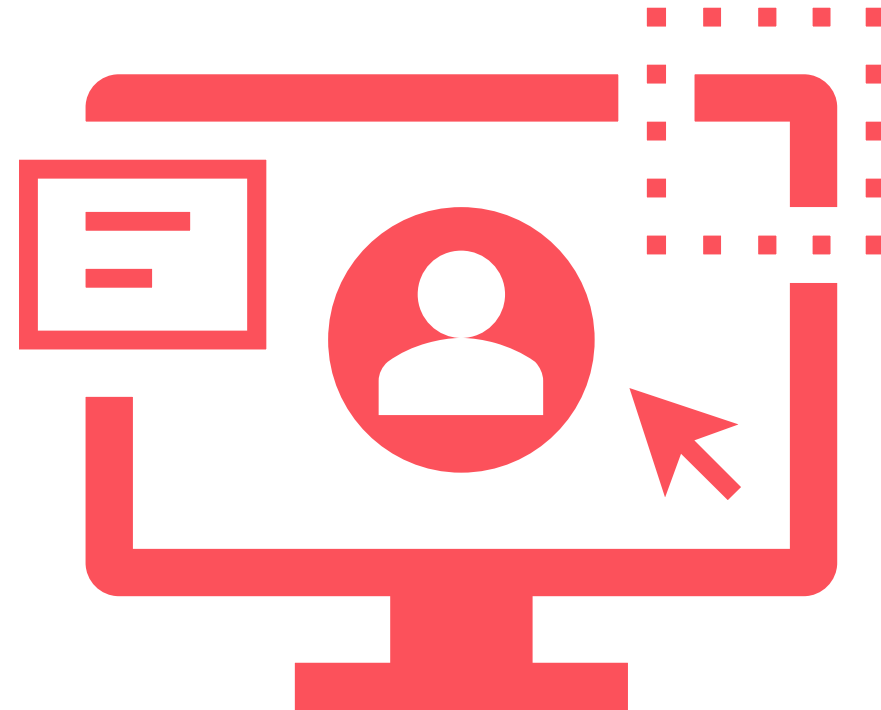
EU (Niederlassung / Präsenz)

❑ Nutzer von KI Systemen

- Jede Person/Firma/Behörde, die KI-Systeme nutzt

❑ Importeure von KI-Systemen

- Nat./ jur. Person in der EU, die ein KI-System auf den Markt bringt, das mit einer Marke/ Namen eines Dritten aus einem Drittland versehen ist



Anwendung des AI Acts im Drittland?

Scope

Drittland (Niederlassung / Präsenz)

- ❑ Anbieter, die
 - *KI Systeme* in EU in Verkehr bringen / in Betrieb nehmen oder
 - wenn das vom KI System hervorgebrachte *Ergebnis in EU verwendet* wird (!)
- ❑ Nutzer von KI Systemen, wenn
 - das vom KI System hervorgebrachte *Ergebnis in EU verwendet* wird
- ❑ Distributor (stellt KI-System in der EU zur Verfügung und ist weder Anbieter noch Importeur)



Anforderungen an „Stakeholder“ varrieren stark“

KI-System – in welche Kategorie fällt es?



Kategorien

Unterschiedliche Konsequenzen / Anforderungen

**Verbotene KI
Systeme
(Art. 5 AI Act)**

**Hochrisiko
KI-Systeme
(Art. 6 AI Act)**

**KI Systeme mit
geringem Risiko
(Art. 52 AI Act)**

**KI Systeme mit
minimalem Risiko
(Art. 69 AI Act)**

AI Act: Kategorien von KI-Systemen

- **Verbotene KI-Systeme:**
 - Unterschw Techniken, die Verhalten neg. beeinflussen können
 - „Social-Scoring“ Systeme von/für Behörden
 - **Software zur biometrischen Identifizierung** (öffentliche Räume und Strafverfolgung, Ausnahme: schwere Straftat & vorh. gerichtl. genehmigt)
 - „absichtliche Manipulationen“
 - **Software zur Emotionserkennung** (Strafverfolgung, Grenzmanagement, Arbeitsplatz u. Bildung)
 - „Predictive Policing“ (Straftaten u. Owis)
- **Hochrisiko KI-Systeme:**
 - Systeme, die *erheblich* schädliche Auswirkungen auf die Gesundheit, Sicherheit und Grundrechte von Personen in der EU haben (Erw. 27)
- **KI-Systeme mit geringem Risiko:**
 - Chatbots
 - Gefühlerkennung
 - Deep Fakes (Ausnahme: absichtliche Manipulation, s.o.)

Verbotene KI-Systeme
(Art.5)

Hochrisiko KI-Systeme
(Art.6 ff)

KI-Systeme mit geringem
Risiko (Art.52)

KI-Systeme mit minimalem
Risiko (Art.69)

Verbotene KI Systeme: Sanktionen, Art. 71 Abs.3



Sanktionen

- Inverkehrbringen, Inbetriebnahme oder Nutzung von verbotenen KI-Systemen



bis zu

- EUR 30 Mio oder, im Falle einer Gesellschaft,
- 6 % des weltweiten Jahresumsatzes des vorherigen Wirtschaftsjahres

Ausnahme: Im Falle von **SMEs**, “including **start-ups**”: Deckel bei **3 %** des weltweiten Jahresumsatzes

Definition “SME” (vgl. Empfehlung der Kommission vom 6. Mai 2003 (2003/361/EG)):

“Unternehmen, die weniger als 250 Personen beschäftigen und einen Jahresumsatz von höchstens EUR 50 Mio. erzielen oder deren Jahresbilanzsumme sich auf höchstens EUR 43 Mio. beläuft.” (vgl. Art. 2 Abs. 1 der Empfehlung)

Kategorien von KI-Systemen



Hochrisiko

A large, solid yellow circle is centered on the slide, containing the text 'Hochrisiko-KI-Systeme (Art. 6 AI Act)'.

Hochrisiko-KI-Systeme
(Art. 6 AI Act)

Hochrisiko KI-Systeme -- Annex II

KI-System, das *selbst* als

- ❑ „Produkt“ in Anwendungsbereich einer der in Annex II aufgezählten RL/VO fällt

und

- ❑ im Rahmen dieser RL/VO einer Konformitätsbewertung durch Dritte unterzogen werden, bevor es auf den Markt gebracht werden kann

KI-System, das als

- ❑ Sicherheitskomponente eines Produkts, welches einer der in Annex II RL/VO unterfällt, verwendet wird

und

- ❑ einer Konformitätsbewertung durch Dritte unterliegt, bevor es auf den Markt gebracht werden kann

Life Science:

- Medical Device Regulation (2017/745)
- Regulation on in vitro diagnostic medical devices (2017/746)

Automotive:

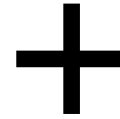
- Regulation on approval and market surveillance of motor vehicles and their trailers, and of systems, components and sep technical units intended for such vehicles

Aviation:

- Regulation on common rules in the field of civil aviation security

Hochrisiko KI-Systeme -- Annex III

KI-Systeme, die in Anhang III aufgelistet sind,
d.h. z.B. genutzt werden sollen für/als:



erhebliches Risiko für die Gesundheit,
die Sicherheit oder die Grundrechte

- Biometrische Identifikation
- Mitarbeiter Recruitment/Management (HR)
 - „Zielgerichtete job advertisements“
 - Analyse / Filterung von Bewerbungen
 - Evaluierung von Kandidaten
 - Entscheidungen in Bezug auf die Beförderung bzw. Beendigung von Arbeitsverträgen
 - Performance-Evaluierung
- Sicherheitskomponenten iRv Management / Betrieb v.
 - „kritischer digitaler Infrastruktur“
 - Versorgung mit Wasser, Gas, Wärme und Elektrizität

Anbieter - Pflichten bzgl. Hochrisiko KI-Systeme



Anbieterpflichten

Risikomanagement

Implementing process for entire lifecycle of HRAIS to identify, analyse and mitigate risks

Article 9

Datenqualität / Data Governance

Training and testing of HRAIS using data shall be undertaken in accordance with

Article 10

Technische Dokumentation

Drafting comprehensive “manual” for HRAIS which contains, at a minimum the Annex IV information

Article 11

“Record-keeping”

HRAIS must be designed to ensure automatic logging of events eg period of use and input data reviewed (Article 12) and providers must keep these logs

Article 20

Transparenz / Informationen

HRAIS must be accompanied by instructions for use which include detailed information including their characteristics, capabilities and limitations

Article 13

“Human oversight”

HRAIS must be designed so they can be overseen by humans, who should meet various requirements eg being able to understand the HRAIS and to stop its use

Article 14

Genauigkeit, Resilienz und Cybersicherheit

HEAIS must be accurate (with accuracy metrics included in instructions for use), resilient to errors or inconsistencies (eg through fail-safe plans) and resilient to cyber-attacks

Article 15

Qualitäts - Management Systeme

HRAIS providers must put in place a comprehensive quality management system which includes at least the extensive information requirements

Article 17

“Post-marketing monitoring”

HRAIS providers must document a system to collect and analyse data provided by users on the performance of the HRAIS throughout its lifetime

Article 61

Konformitätsbewertung

HRAIS provider shall follow conformity assessment procedure

Article 43

Verstoß gegen Anbieter-Pflichten: Sanktionen, Art. 71 Abs.4



- Verstoß gegen Anbieterpflichten gem. Art. 16



bis zu

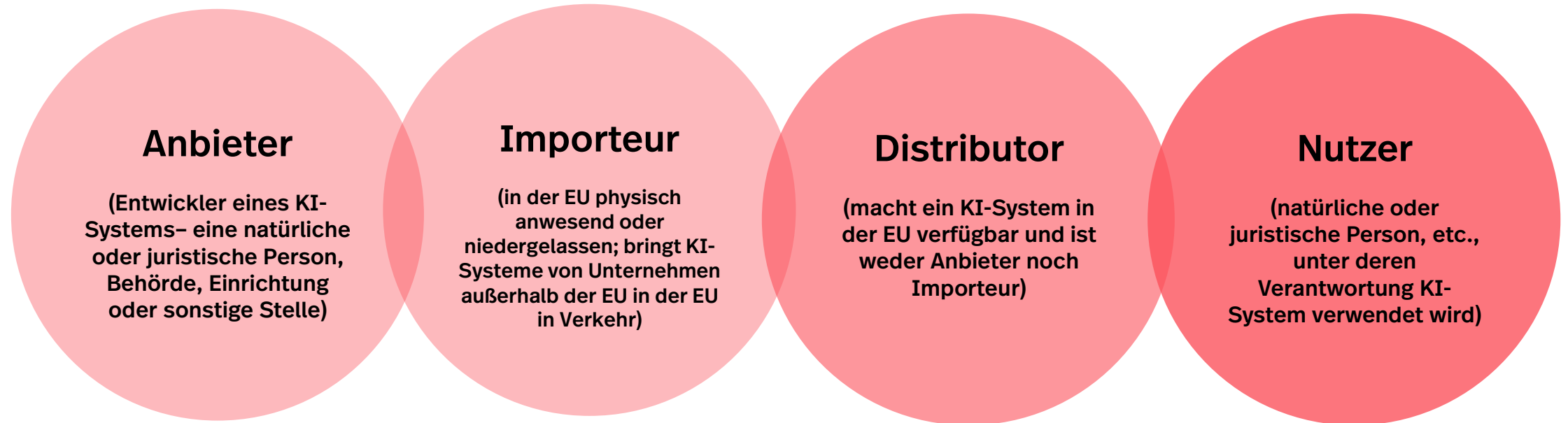
- **EUR 20 Mio** oder, im Falle einer Gesellschaft,
- 4 % des weltweiten Jahresumsatzes des vorherigen Wirtschaftsjahres

Ausnahme: Im Falle von **SMEs**, “including **start-ups**”: Deckel bei **2 %** des weltweiten Jahresumsatzes

Pflichten in Bezug auf Hochrisiko-KI-Systeme



Verschiedene Akteure



Verpflichtungen für Nutzer von Hochrisiko-KI-Systemen (Art.29)



- Übertragung der menschlichen Aufsicht auf natürliche Personen, die über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen
- Sicherstellen, dass Eingabedaten der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen
- Überwachung des Betriebs des Systems und Information des Anbieters / Händlers im Falle von Risiken sowie Aussetzung der Verwendung im Falle eines schwerwiegenden Vorfalls
- Protokollierung und Ereignisaufzeichnung (Pflicht zur Aufbewahrung von 6 Monaten, sofern nicht Widerspruch zur DS-GVO)
- Finanzinstitute & Logs: Aufzeichnung im Rahmen der relevanten „Financial Services Legislation“

Verpflichtungen von Importeuren (Art.26) und Distributoren (Art.27) bzgl. Hochrisiko KI-Systemen

§

Importeurs et alt.

Sicherstellen dass,

- die Konformitätsbewertung von dem Anbieter durchgeführt wurde
- der Anbieter technische Informationen bereitgestellt hat (beides nur relevant für Importeure)
- das KI-System die nötigen CE - Konformitätsmarker hat und die EU Konformitätserklärung beigefügt ist (vom Importeur 10 J. aufzubewahren)
- das KI-System auch eine Gebrauchsanweisungen enthält
- Lagerung oder Transport keine Verpflichtungen für Hochrisikosysteme des Anbieters gefährden
- Den Hersteller und die Marktüberwachungsbehörde informieren, falls Risiken entstehen

Verstoß gegen Pflichten: Sanktionen, Art. 71 Abs.4



- Nutzer/Importeure/Distributoren: Verstoß gegen Pflichten



bis zu

- EUR 20 Mio. oder, im Falle einer Gesellschaft,
- 4 % des weltweiten Jahresumsatzes des vorherigen Wirtschaftsjahres

Ausnahme: Im Falle von **SMEs**, “including **start-ups**”: Deckel bei **2 %** des weltweiten Jahresumsatzes

ChatGPT & sonstige „Large Language Models“



GPAI

General Purpose AI bzw. Foundation Modelle

Strenge Anforderungen für Foundation-Modelle geplant, u.a.

- ☐ angemessene Service-Levels
- ☐ Korrigierbarkeit
- ☐ Cybersicherheit
- ☐ umfassende Tests
- ☐ jegliches urheberrechtlich geschützte Material, das zur Entwicklung ihrer Systeme verwendet wurde, offenzulegen.
- ☐ Registrierung in EU Datenbank
- ☐ **Lieferkette**: Anbieter des GPAI-Systems sowie Unternehmen, die es nachgelagert anpassen → alle „Anbieter“ → Kollaboration!



Nachhaltigkeit von hochriskanter KI

KI-Systeme mit hohem Risiko werden Aufzeichnungen über ihren ökologischen Fußabdruck führen und die Gründungsmodelle werden den europäischen Umweltstandards entsprechen müssen.

Erweiterung der „AI Regulatory Sandboxes“/„KI-Reallabore“ (Art.53)

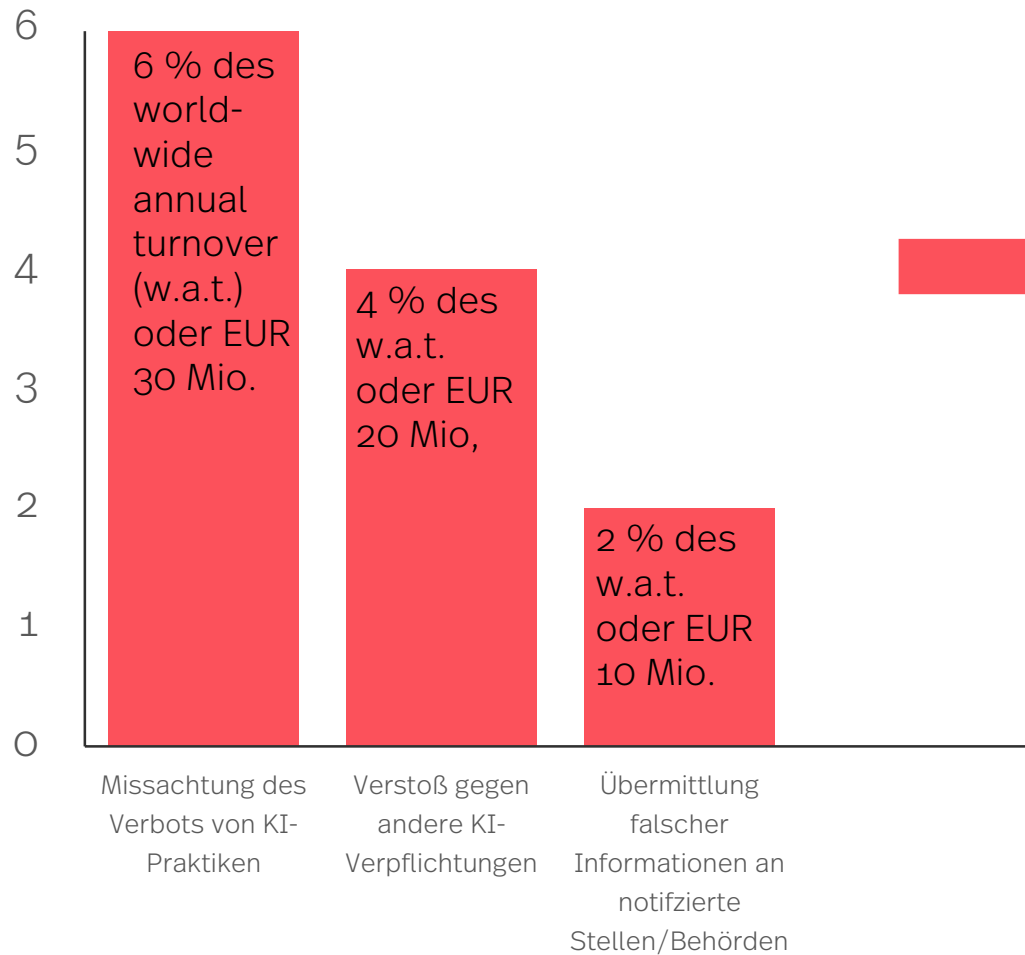
- Mitgliedstaaten nun zuständig für die Schaffung solcher „Sandboxes“
- Möglich für neue KI-Systeme vor Inbetriebnahme
- Soll die Förderung von Innovation und Wettbewerb, den Marktzugang für KI-Systeme und die Rechtssicherheit fördern

Ermöglichung von „Tests von Hochrisiko-KI-Systemen unter realen Bedingungen außerhalb von KI-Reallaboren“ (Art.54a)

- In-scope: Anbieter der in Anhang 3 gelisteten Hochrisikosysteme
- Voraussetzungen der Inanspruchnahme: Art. 54a (4))

- Nationale Behörde von den Mitgliedsländern zu bestimmen
- Stärkere Rolle des „European Artificial Intelligence Boards“ in Bezug auf Implementierung und Durchsetzung des AI-Act (Art.56,58)
 - Zusammensetzung: ein Repräsentant pro Mitgliedsland, European Data Protection Supervisor („observer“), EU Kommission (ohne Stimmrecht)
 - Aufgaben in Art. 58 abschließend aufgezählt
- Kommission kann einen zentralen Pool unabhängiger Experten zur Unterstützung bei der Durchsetzung der KI-VO schaffen (Art. 68b)

- Sanktionen, Art. 71 AI-Act.



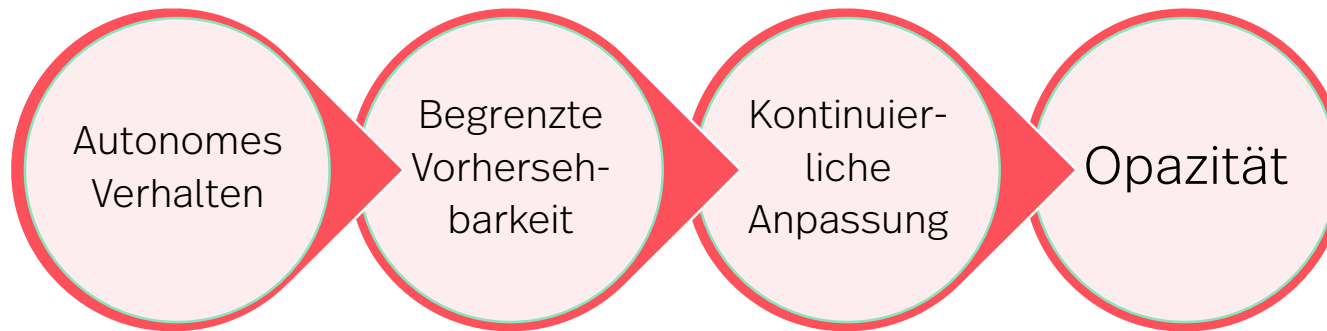
- Zivilrechtliche Haftung?

Aber...

Anpassung der Haftungsregelungen an digitale Zeitalter



EU Kommission: Eigenschaften von KI erschweren Schadensersatz-A'



Außerdem: „Kostspielig Schaden und Kausalität nachzuweisen (auch in Bezug auf fehlendes technisches Fachwissen)“

28. September 2022:

➤Vorschlag der EU Kommission für eine Richtlinie zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung)

AI Liability Directive (Entwurf)



Erleichterung der Durchsetzung von
Schadensersatzansprüchen bzgl
Hochrisiko – KI - Systemen

Pflicht, Beweismittel
offenzulegen bzgl HRAI, das
im Verdacht steht
(Plausibilität), Schaden
versucht zu haben

sofern keine Offenlegung:
widerlegbare Vermutung
eines Verschuldens

Widerlegbare Vermutung
eines ursächlichen
Zusammenhangs

im Falle eines Verschuldens

„Verschulden“ Anbieter u.a.:

- Datenqualität (-)
- Transparenzanforderung (-)
- Cybersicherheit (-)

„Verschulden“ Nutzer u.a.:

- Nutzung gem.
Gebrauchsanweisung (-)
- Eingabedaten widersprechen
Zweckbestimmung

An abstract 3D graphic on the right side of the page. It features various numbers (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) and rings in white and metallic blue, some of which are transparent and overlapping, creating a sense of depth and complexity.

simmons-simmons.com

STRICTLY PRIVATE AND CONFIDENTIAL

© Simmons & Simmons LLP and its licensors. All rights asserted and reserved. This document is for general guidance only. It does not contain definitive advice. Simmons & Simmons LLP is a limited liability partnership registered in England & Wales with number OC352743 and with its registered office at CityPoint, One Ropemaker Street, London EC2Y 9SS, United Kingdom. It is authorised and regulated by the Solicitors Regulation Authority and its SRA ID number is 533587. The word "partner" refers to a member of Simmons & Simmons LLP or one of its affiliates, or an employee or consultant with equivalent standing and qualifications. A list of members and other partners together with their professional qualifications is available for inspection at the above address.