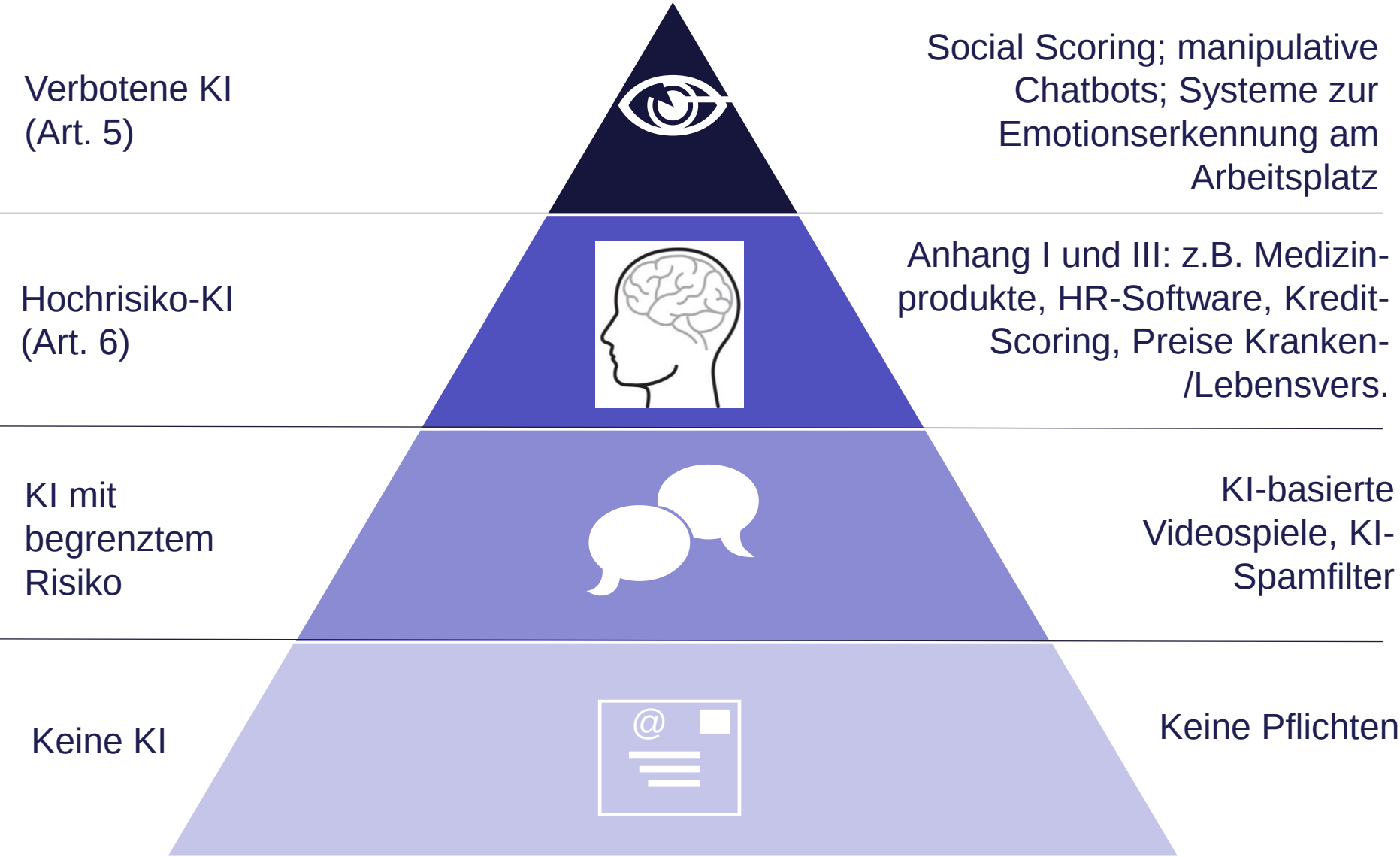


Oppenhoff

GI-Themenabend Künstliche Intelligenz

Köln, 9. September 2024
Dr. Marc Hilber

Risikobasierter Ansatz



AI-Models
(Art. 51 ff.)

GPAI-System,
(Art. 3 Nr. 66)

Generative KI (Art. 50 Abs. 2, 4)

Inter-agierende KI (Art. 50 Abs. 1, 3)

KI Schulung
(Art. 4)

Hochrisiko-KI-Systeme, Art. 6 Abs. 1 i.V.m. Anhang I

- KI-System, das **Sicherheitsbauteil** eines Produktes ist, dass unter die in Anhang I aufgelisteten EU-Regulierungsvorschriften fällt oder selbst ein solches Produkt ist, vgl. Art. 6 Abs. 1
- Sicherheitsbauteil (Art. 3 Nr. 14, vgl. auch EG 55) = keine „Funktionsteile“?

Abschnitt A (New Legislative Framework)	Abschnitt B (Detailharmonisierungsvorschriften)
Bsp.: Spielzeuge, Medizinprodukte, Druckgeräte, Aufzüge • Regelungen zu Hochrisiko-KI-Systemen und insbesondere zu den Anforderungen an das KI-System selbst (Art. 8 ff.) unmittelbar anwendbar	Bsp.: Zivilluftfahrt, Marktüberwachung von forstwirtschaftlichen Fahrzeugen • KI-Gesetz auf diese Produkttypen nicht unmittelbar anwendbar (Art. 2 Abs. 2) • Vorhandene Regulierung (sog. Harmonisierungsvorschriften) sollen um Regelungen entsprechend dem KI-Gesetz ergänzt werden (Art. 102 ff., EG 49 ff.)

Hochrisiko-KI-Systeme, Art. 6 Abs. 2 i.V.m. Anhang III

- Eigenständiges KI-System ist aufgrund sensiblen Einsatzbereichs in Anhang III genannt, z.B.
 - Biometrik: biometrische Fernidentifizierungssysteme, Kategorisierung, Emotionserkennung, Verhaltensanalyse
 - Kritische Infrastruktur: Sicherheitsbauteil iRd. Verwaltung und Betrieb kritischer digitaler Infrastruktur (Bsp. Wasser-, Gas-, Wärme- und Stromversorgung)
 - Bildung: Feststellung des Zugangs zu Einrichtungen, Bewertung von Lernergebnissen, Erkennen von unzulässigem Prüfungsverhalten
 - Arbeit: Schaltung gezielter Stellenanzeigen, Einstellung und Prüfung der Eignung von Bewerbern, **für die Beobachtung und Bewertung der Leistung und des Verhaltens von Personen**
 - Private und öffentliche Dienste: Kreditwürdigkeitsprüfung, Bewertung/Klassifizierung von Notrufen, Bewertung bei dem Abschluss von Kranken- und Lebensversicherungen
- Ausnahmeregelung nach Art. 6 Abs. 3 anwendbar

Ausnahmen gem. Art. 6 Abs. 3

- Abweichend von Art. 6 Abs. 2 gilt ein KI-System nicht als hochriskant, wenn
 - **eng verfasste Verfahrensaufgabe** durchgeführt werden soll;
 - das Ergebnis einer **zuvor menschlich abgeschlossenen Tätigkeit verbessert** werden soll;
 - **Entscheidungsmuster oder Abweichungen** von diesen **erkannt werden sollen** und menschliche Bewertung nicht ohne Überprüfung ersetzt oder beeinflusst werden soll;
 - **eine vorbereitende Aufgabe** für eine Bewertung durchgeführt werden soll, die für Anwendungsfälle des Anhang III relevant ist.
- **Aber:** KI-System immer hochriskant, wenn es **Profiling** von natürlichen Personen vornimmt,
 - d.h. personenbezogene Daten verarbeitet, um Arbeitsleistung, wirtschaftliche Lage, Interessen oder Zuverlässigkeit der natürlichen Person vorherzusagen.

Überblick: Die wichtigsten Pflichten bei Hochrisiko-KI

Art. 8-16

Pflichten des **Anbieters** für
das KI-System selbst

- Risikomanagementsystem, Art. 9
- Daten und Daten-Governance, Art. 10
- Technische Dokumentation, Art. 11
- Aufzeichnungspflichten, Art. 12
- Transparenzpflicht, Art. 13
- Menschliche Aufsicht, Art. 14
- Genauigkeit, Robustheit und Cybersicherheit, Art. 15

Art. 16-22

Organisatorische Anforderungen
an **Anbieter**

- Name und Kontaktanschrift, Art. 16 lit. b
- Qualitätsmanagementsystem, Art. 17
- Aufbewahrungspflicht, Art. 18
- Aufbewahrungspflicht, Art. 19
- Korrekturmaßnahmen und Informationspflicht, Art. 20
- Zusammenarbeit mit zuständigen Behörden, Art. 21
- Bevollmächtigte der Anbieter, Art. 22

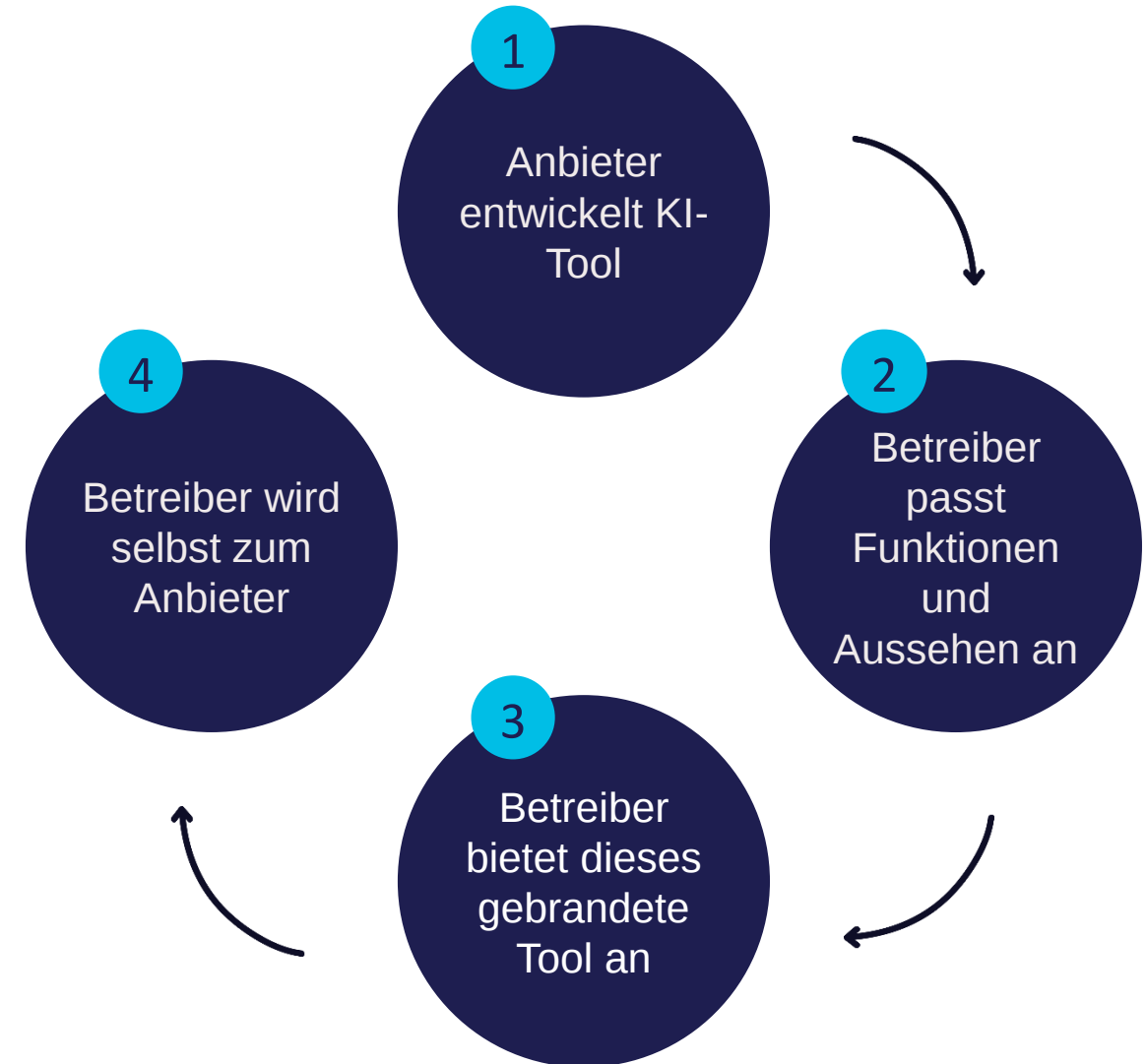
Art. 26 und 27

Organisatorische Anforderungen
an **Betreiber**

- TOMs, Eingabedaten, Überwachung, Protokolle (Art. 26)
- Grundrechte-Folgenabschätzung (Art. 27)

Art. 25: Vom Betreiber zum Anbieter

- Gilt nur für Hochrisiko-KI-Systeme
- **Betreiber wird insbesondere zu Anbieter, wenn er ...**
 - seinen Namen/Warenzeichen auf das System anbringt
 - (GPAI-)KI-System so verändert, dass es zu einem Hochrisiko-KI-System wird
- **Rechtsfolge:**
 - Anbieterwechsel
 - Unterstützungspflicht des ursprünglichen Anbieters
 - Ausnahme: die Veränderung des KI-Systems wurde ausdrücklich ausgeschlossen



KI Modelle

- Abgrenzung zu KI-Systemen
 - KI-Modell: Technische Basis für ein KI-System; **nicht für Endnutzer geeignet** (Art. 3 Nr. 63)
 - KI-System: Funktionsfähige, mit Benutzeroberfläche ausgestattete KI-Anwendung

EG 97: „Damit KI-Modelle zu KI-Systemen werden, ist die Hinzufügung weiterer Komponenten, zum Beispiel einer Nutzerschnittstelle, erforderlich.“
 - Typisches Beispiel für GPAI Models sind große generative KI-Modelle wie LLMs, vgl. EG 99
- Pflichten der Anbieter von KI-Modellen (Art. 53)
 - Müssen nachgelagerten Anbietern **Informationen zum Modell bereitstellen** (Ausn: Open Source)
 - Entwicklung einer Strategie, dass beim Training der Modelle **Urheberrecht eingehalten** wird
- KI-Modelle mit systemischem Risiko (Art. 51, 55)
 - Gesamtrechenleistung von mehr als 10^{25} FLOPs
 - strenge Anforderungen (Cybersicherheit, Risikomanagement, Meldepflichten, Energieverbrauch)

KI Systeme mit allgemeinem Verwendungszweck (General Purpose AI)

- GPAI-Systeme sind gem. Art. 3 Nr. 66 KI-Systeme, die...
 - auf einem GPAI-Model beruhen und
 - in der Lage sind, einer **Vielzahl von Zwecken** zu dienen,
 - sowohl in direkter Verwendung als auch über eine Integration in andere KI-Systeme.
- GPAI-Systeme sind selbst keine Hochrisiko-KI-Systeme, können aber als solche verwendet werden oder in solche integriert werden, EG 85
- Allgemeine Transparenzpflichten gelten auch GPAI-Systeme
 - **Kennzeichnungs- und Offenlegungspflichten** für KI-generierte Inhalte gelten nach Art. 50 Abs. 2 KI-Gesetz ausdrücklich auch für GPAI-Systeme

Interagierende KI

- KI-System, das direkt mit Menschen interagiert (oft in Echtzeit)
 - Bsp.: Chatbots und virtuelle Assistenten
- Spezifische **Transparenzpflichten**, Art. 50 Abs. 1 und 3
 - Inhalt: Offenlegung, dass Interaktion mit KI stattfindet, Grenzen des KI-Systems und Rechte der Betroffenen
 - Zeitpunkt: Spätestens erste Interaktion
 - Ausnahme: Interaktion mit KI-System ist offensichtlich
 - Schutzbedürfnis vulnerabler Personen muss berücksichtigt werden
- Interagierende KI kann abhängig von Einsatzbereich auch Hochrisiko-KI-System sein

Generative KI

- KI-System, das neue Inhalte generieren kann
 - insb. Texte, Bilder, Musik oder Videos
 - Bsp.: Sora, Midjourney
 - Inhalte basieren auf Mustern, die KI-System aus Trainingsdaten gelernt hat
- Spezifische **Offenlegungs- und Kennzeichnungspflichten**, Art. 50 Abs. 2 und 4
 - Pflichten gelten unabhängig von Risikostufe des Systems
 - Kennzeichnung der Inhalte als künstlich erzeugt/manipuliert in maschinenlesbarer Form
 - Offenlegung von Deepfakes
- Generative KI kann abhängig von Einsatzbereich auch Hochrisiko-KI-System sein

Ihre Ansprechpartner

Bei weiteren Fragen stehen wir Ihnen gerne zur Verfügung.



Dr. Marc Hilber

Partner • Rechtsanwalt

Konrad-Adenauer-Ufer 23

50668 Köln

Tel.: +49 (0) 221 2091-612

marc.hilber@oppenhoff.eu