

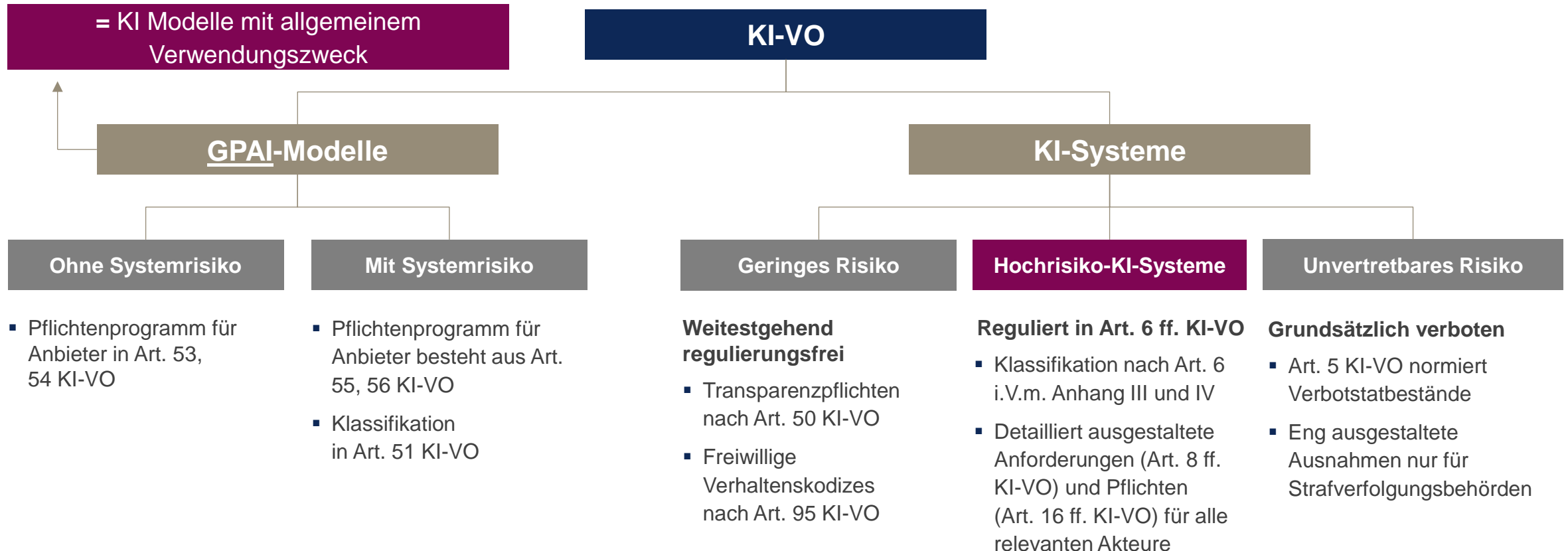
SYSTEMATISIERUNG VON KI-SYSTEMEN NACH DER KI-VERORDNUNG

Dr. Marc Ruttloff | Moritz Stilz, LL.M. (Duke)

10. September 2024

Regulierungsstruktur der KI-VO

Die Untergliederung verschiedener KI-Systeme



ChatGPT = GPAI

KI-MODELL VS. KI-SYSTEM

Definition KI-System

Art. 3 Nr. 1 KI-VO

”

[...] 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;

”



• “System, das für [...] autonomen Betrieb ausgelegt”

• “nach seiner Betriebsaufnahme anpassungsfähig”

• “aus den erhaltenen Eingaben für [...] Ziele ableitet“

Was ist ein KI-Modell?

KI VO definiert KI-Modell nicht

„wesentliche Komponente“

KI-Modell Teil eines KI-Systems

Jedes KI-System enthält ein KI-Modell

”

Obwohl **KI-Modelle** wesentliche Komponenten von KI-Systemen sind, **stellen sie für sich genommen keine KI-Systeme dar**. Damit KI-Modelle zu KI-Systemen werden, ist die Hinzufügung weiterer Komponenten, zum Beispiel einer Nutzerschnittstelle, erforderlich. KI-Modelle sind in der Regel in KI-Systeme integriert und Teil davon

ErwG. 97

“Hinzufügung weiterer Komponenten”

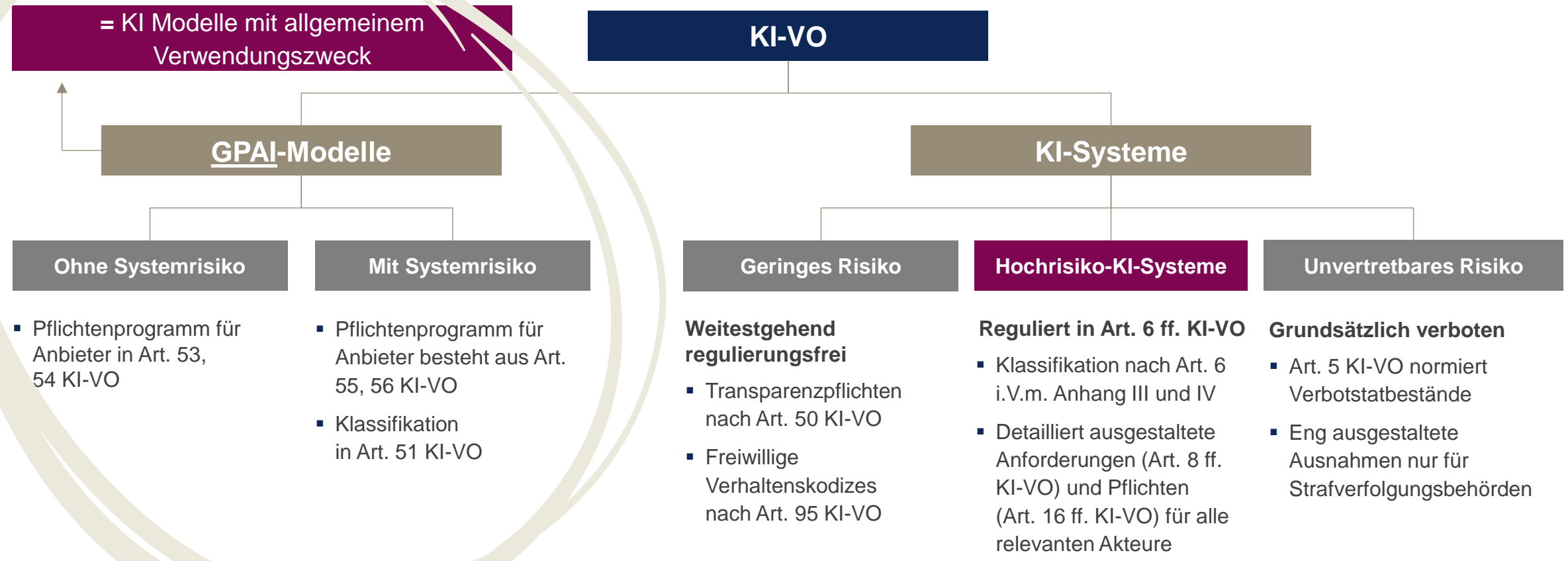
Per se kein KI-System

Durch hinzufügen bspw. einer “Nutzerschnittstelle” kann KI-Modell zu einem KI-System werden.

KI VO reguliert GPAI-Modelle

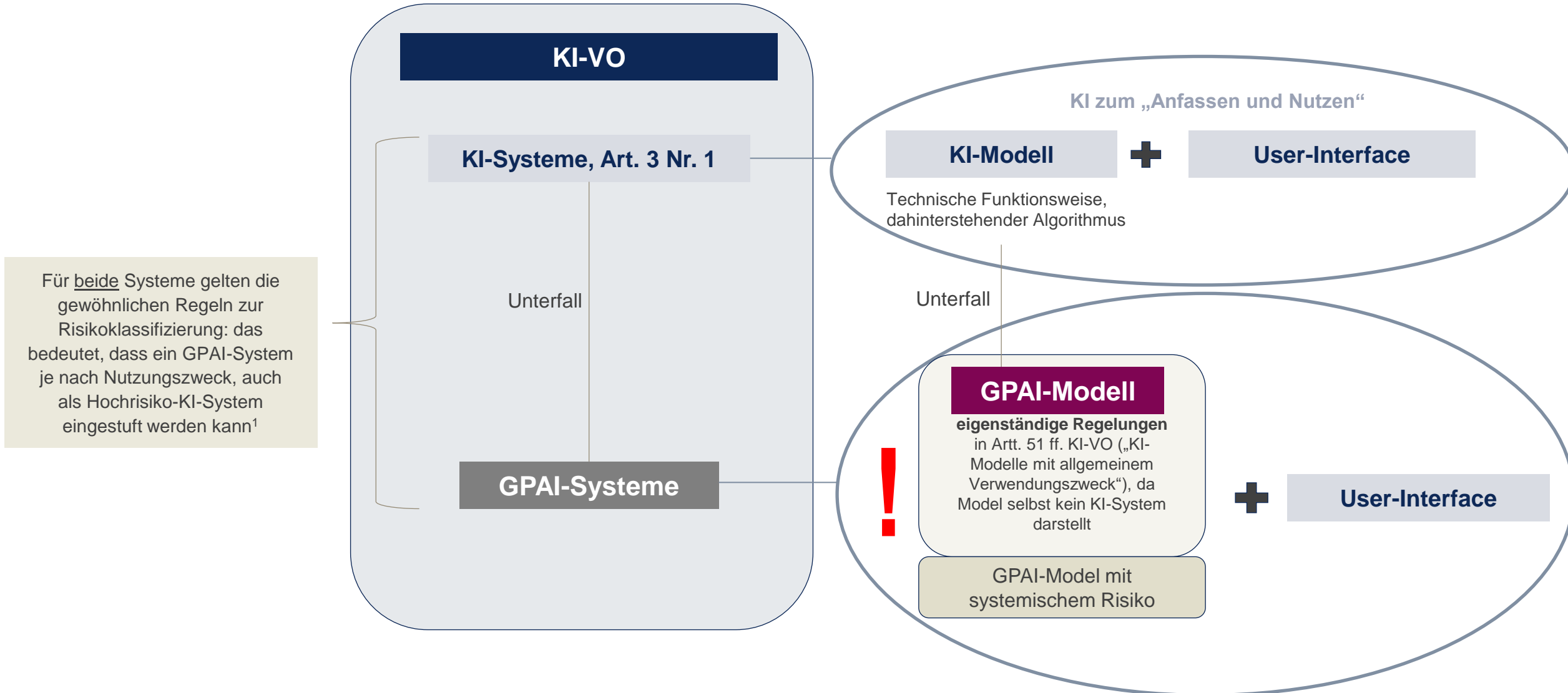
Regulierungsstruktur der KI-VO

Die Untergliederung verschiedener KI-Systeme



ChatGPT = GPAI

Unterscheidung: KI-Modell und KI-System

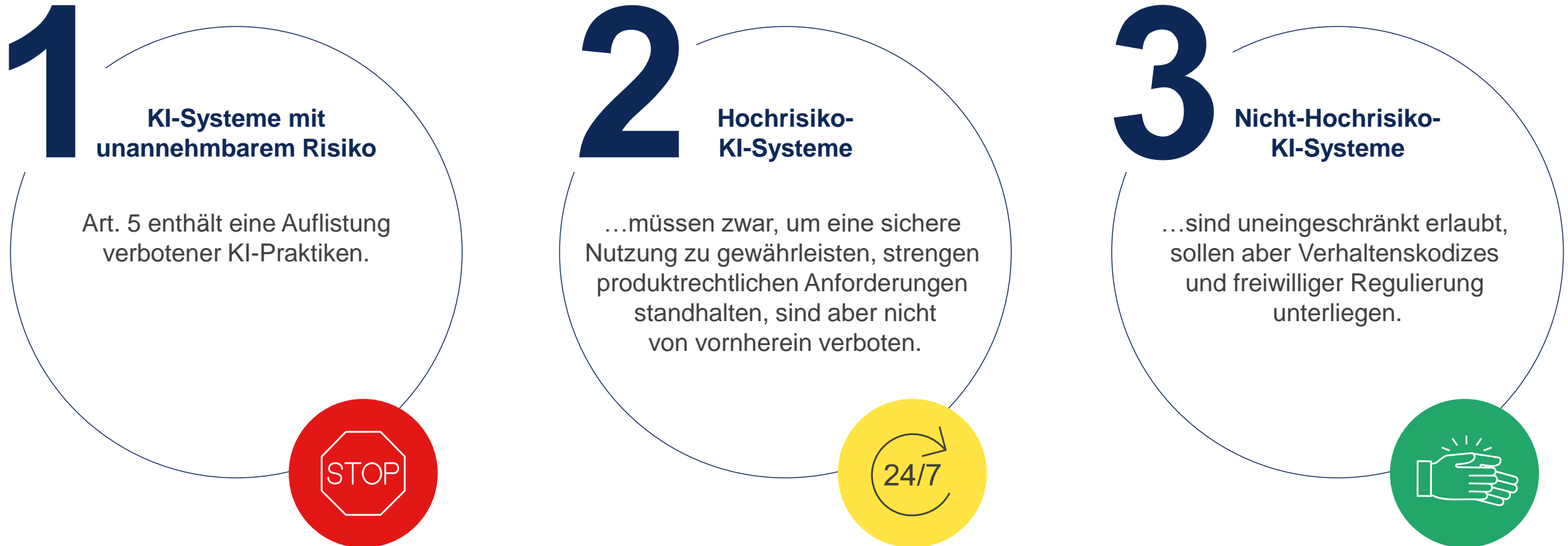


Für beide Systeme gelten die gewöhnlichen Regeln zur Risikoklassifizierung: das bedeutet, dass ein GPAI-System je nach Nutzungszweck, auch als Hochrisiko-KI-System eingestuft werden kann¹

¹Vgl. ErwG. 85: „KI-Systeme mit allgemeinem Verwendungszweck können als eigenständige Hochrisiko-KI-Systeme eingesetzt werden oder Komponenten anderer Hochrisiko-KI-Systemen sein“

RISIKOKLASSIFIZIERUNG VON KI-SYSTEMEN

Risikobasierter Ansatz



Risikobasierter Ansatz

Wesentliche Inhalte

Verbot bestimmter KI-Praktiken

- **Beeinflussung** des Verhaltens
- **Ausnutzung schutzbedürftiger** Gruppen
- „Social Scoring“
- Biometrische **Echtzeit-Fernidentifizierung**

Gering riskante KI-Systeme

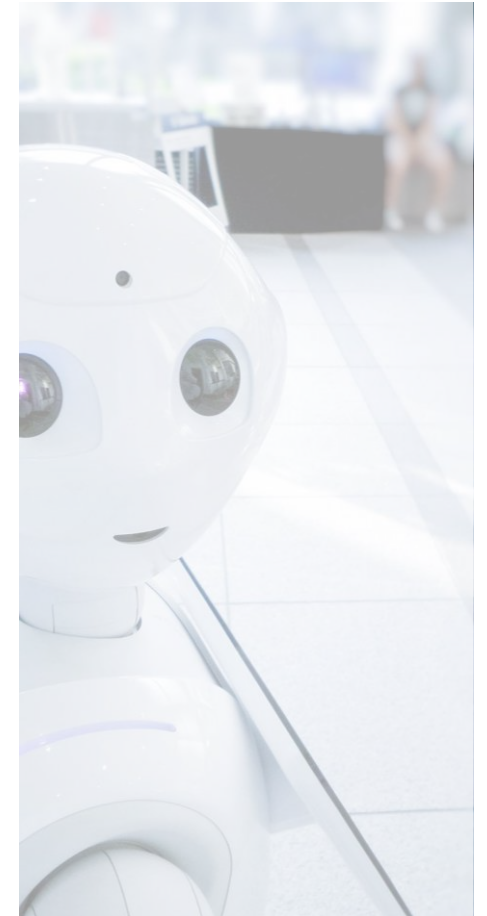
- **Weitestgehend uneingeschränkter Einsatz**
- Aber allgemeine Transparenzpflicht (Hinweis auf die Verwendung von KI)
- **Beispielsweise** kommunikative KI (Chatbot)

Hochrisiko-KI-Systeme

- **Besondere Bestimmungen**
 - Zulassungserfordernis
 - Transparenz- / Kennzeichnungspflichten
 - Risiko- und Qualitätsmanagementsysteme
- **Beispielsweise:** KI für Feststellung/Zuweisung zu Bildungseinrichtungen oder Bewertung von Lernergebnissen.

Adressaten

- **Anbieter** von KI-Systemen
 - Hat die **Gesamtverantwortung** für das KI-System
- Zudem: **Hersteller, Händler, Nutzer, Einführer** und **sonstige Dritte** mit unterschiedlichen Anforderungen und (geringeren) Pflichten
 - Nutzer haftet etwa nur, wenn er das System **nicht gemäß der Gebrauchsanweisung** bedient



Betreiber - Anbieter

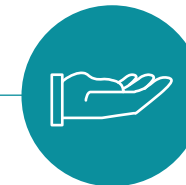
Maßgebliche Unterscheidung



„Betreiber“

(engl. „*deployer*“) ist, wer ein **KI-System in eigener Verantwortung verwendet** [...] (Art. 3 Nr. 4 KI-VO).

- ▶ Betreiber muss „nur“ Überwachungs- und Transparenzanforderungen erfüllen



"ANBIETER"

(engl. „*provider*“) ist, wer ein **KI-System entwickelt** oder entwickeln lässt, um es unter ihrem **eigenen Namen** oder ihrer eigenen Handelsmarke **in Verkehr bringt** oder in Betrieb nimmt (Art. 3 Nr. 3 KI-VO).

- ▶ ANBIETER trägt „Gesamtverantwortlichkeit“



Betreiber kann nach den Vorgaben des Art. 25 KI-VO zum Anbieter werden.



Modifizierung bestehender KI-Systeme

Wie Betreiber durch Art. 25 KI-VO plötzlich zu Anbietern werden.

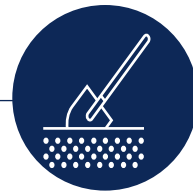
Ausgangspunkt: In Verkehr gebrachte oder in Betrieb genommene Hochrisiko-KI-Systeme



Anbringen des eigenen Namens/ der eigenen Marke

unbeschadet vertraglicher Vereinbarungen.

(gilt nur für Hochrisikosysteme)



Vornahme einer wesentlichen Änderung

so, dass das Hochrisiko-KI-System ein solches bleibt.

(gilt nur für Hochrisikosysteme)



Änderung des Verwendungszwecks

auch bei GPAI-Modellen wie ChatGPT, die durch Modifikation zu Hochrisikosystemen werden

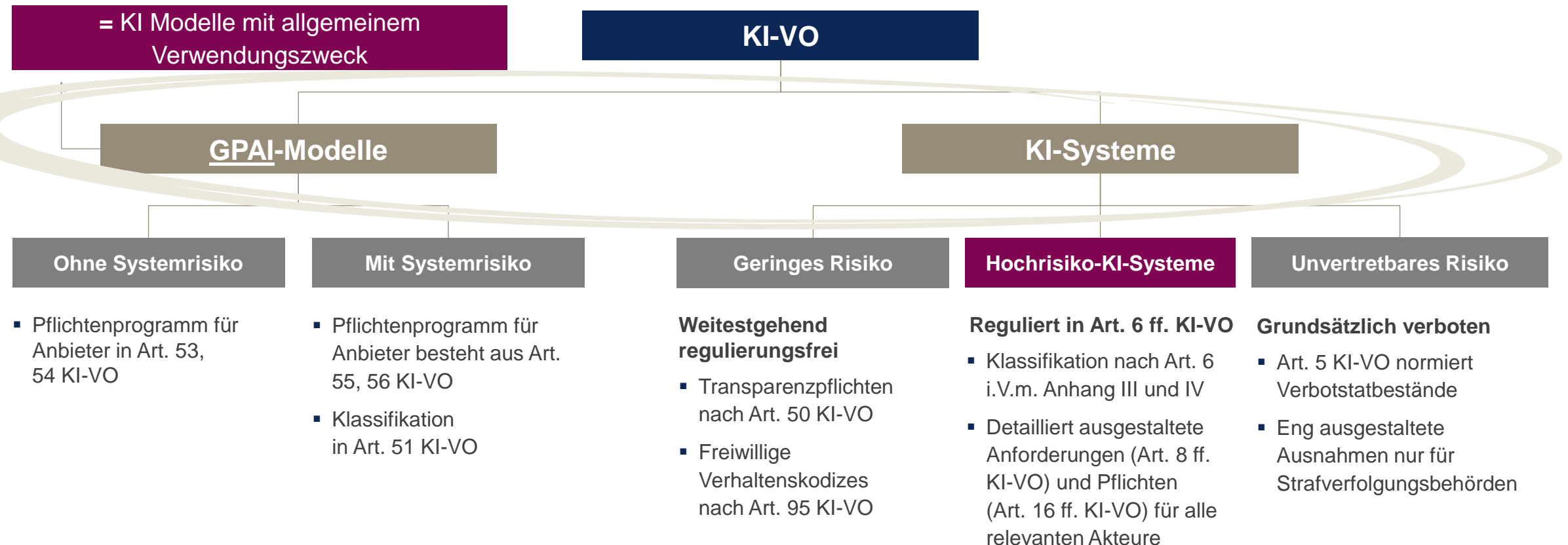


Sobald KI-Systeme dergestalt verändert werden, geht die Anbietereigenschaft und somit auch das entsprechende Pflichtenprogramm auf den modifizierenden „neuen Anbieter“ über.

GPAl UND HOCHRISIKO-KI-SYSTEME

Regulierungsstruktur der KI-VO

Die Untergliederung verschiedener KI-Systeme



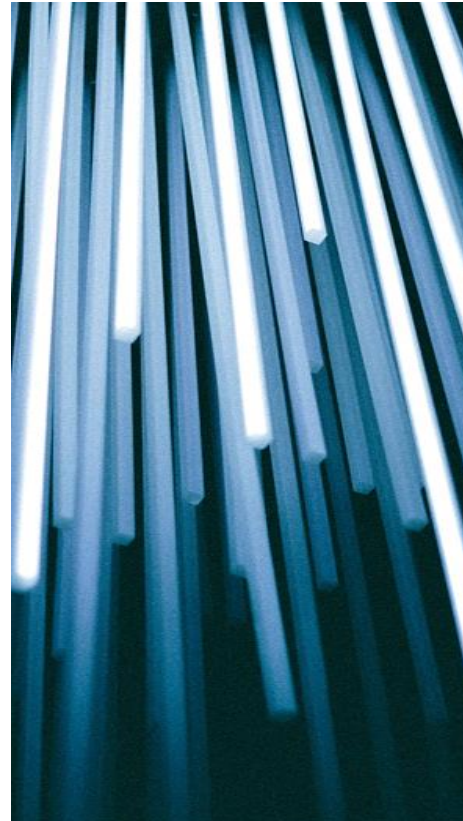
ChatGPT = GPAI

KI-Kategorien

GPAI

KI-Modelle, die erhebliche **Generalität** aufweisen und **breites Aufgabenspektrum** erfüllen können (Art. 51 ff. KI-VO).

- Klassifizierung nach technischen Parametern oder von Amts wegen durch Kommissionsentscheidung (Anhang XIII KI-VO)
- Differenzierung nach Systemrisiko, inklusive verschiedener Pflichtenprogramme



HOCHRISIKO-KI-SYSTEME

KI-Systeme, die aufgrund **Art, Zwecks** oder **Funktionsweise besonders** gefährlich für die öffentliche Gesundheit, Sicherheit und die Grundrechte sind.

- Klassifizierung erfolgt nach Art. 6 und Anhang III und IV.
- Art. 6 ff. KI-VO regeln die Klassifizierung und die Pflichtenprogramme für Hochrisiko-KI-Systeme

„allgemeinem Verwendungszweck“ vs. „bestimmungsgemäß“

Anwendungsrisiken am Beispiel CoPilot

Verbotene Praktiken und Hochrisiko-KI-Systeme

VERBOTENE PRAKTIKEN

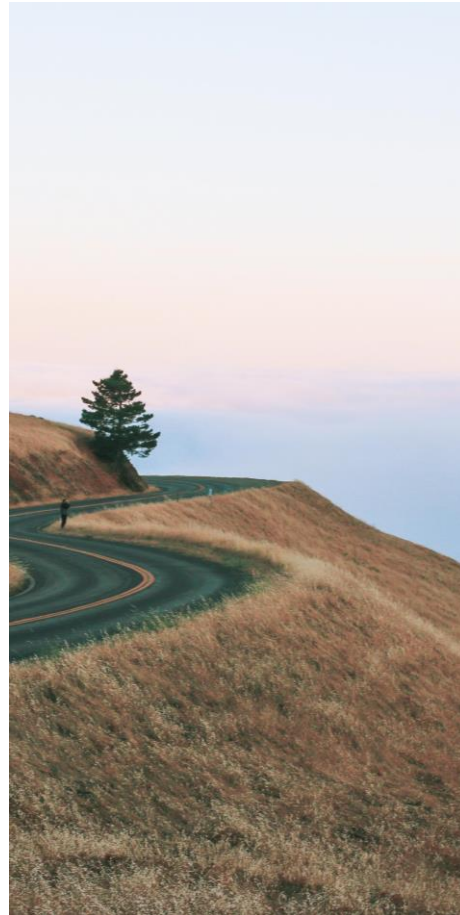
Art. 5 KI-VO normiert KI-Systeme mit unverhältnismäßigen Risiken, die grds. verboten sind.

- Manipulative Techniken zur Verhaltenssteuerung
- Ausnutzung von Schwachstellen verletzlicher Personen oder Personengruppen
- Biometrische Kategorisierung und Echtzeit - Fernidentifikation
- Soziale Bewertung

Bei Verstoß drohen Bußgelder bis zu 35 Mio. € oder 7% des gesamten weltweiten Jahresumsatzes.



CoPilot ist hierzu nicht ohne Weiteres in der Lage



HOCHRISIKO-KI-SYSTEME

CoPilot als Hochrisiko-System (Art. 6 Abs. 2 in Verbindung mit Anhang III Punkte 3 und 4)

- Berufliche Bildung
- **Beschäftigung und Arbeitnehmermanagement**
- Problem: Zweckbestimmung einer Allzweck-KI

Wenn (+), dann **Pflichtenkatalog des Art. 26 KI-VO.**

Bei Verstoß Bußgelder bis zu 15 Mio. € oder 3% des gesamten weltweiten Jahresumsatzes.



Achtung im HR-Bereich

ErwG. 85: „KI-Systeme mit allgemeinem Verwendungszweck können als eigenständige Hochrisiko-KI-Systeme eingesetzt werden [...]

Hochrisiko-Bereich Bildung

Regelungsbereiche des Anhang III Punkt 3 KI-VO

Allgemeine und berufliche Bildung

- (a) *KI-Systeme, die bestimmungsgemäß zur **Feststellung** des Zugangs oder der **Zulassung** oder zur **Zuweisung** natürlicher Personen zu **Einrichtungen** aller Ebenen der allgemeinen und beruflichen **Bildung** verwendet werden sollen*
- (b) *KI-Systeme, die bestimmungsgemäß für die **Bewertung** von **Lernergebnissen** verwendet werden sollen, **einschließlich** des Falles, dass diese **Ergebnisse dazu dienen**, den **Lernprozess** natürlicher Personen in Einrichtungen oder Programmen aller Ebenen der allgemeinen und beruflichen Bildung **zu steuern***
- (c) *KI-Systeme, die bestimmungsgemäß zum Zweck der Bewertung des angemessenen Bildungsniveaus, das eine Person im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung erhalten wird oder zu denen sie Zugang erhalten wird, verwendet werden sollen;*

”

Zudem: Art. 22 Abs. 1 DSGVO für KI-Letztentscheidungen - dürfen nur für positive KI-Letztentscheidungen verwenden.



Hochrisiko-Bereich

Human Resources

Regelungsbereiche des Anhang III Punkt 4 b KI-VO

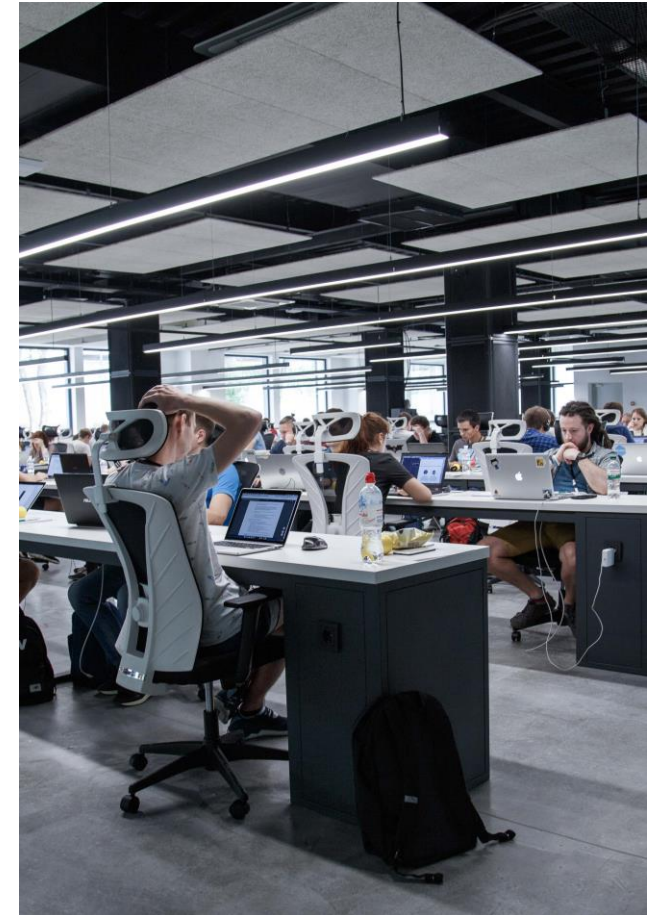
(b) KI-Systeme, die bestimmungsgemäß für Entscheidungen, die die **Bedingungen** von Arbeitsverhältnissen, **Beförderungen** und **Kündigungen** [...] beeinflussen, für die **Zuweisung von Aufgaben** aufgrund des individuellen Verhaltens oder persönlicher Merkmale oder Eigenschaften oder für die **Beobachtung** und Bewertung der **Leistung** und des Verhaltens von Personen in solchen **Beschäftigungsverhältnissen** verwendet werden soll.

”

- ➔ disziplinarisches Weisungsrecht
- ↳ fachliches Weisungsrecht: nur Aufgabenzuweisung

Art. 26 Abs. 7 KI-VO: Information „Arbeitnehmervertreter und betroffene Arbeitnehmer [...], dass sie Verwendung des Hoch-Risiko-KI-Systems unterliegen werden“

Zudem: Art. 22 Abs. 1 DSGVO für KI-Letztentscheidungen - AG dürfen nur für AN positive KI-Letztentscheidungen verwenden.



GPAI und Hochrisiko-KI-Systeme

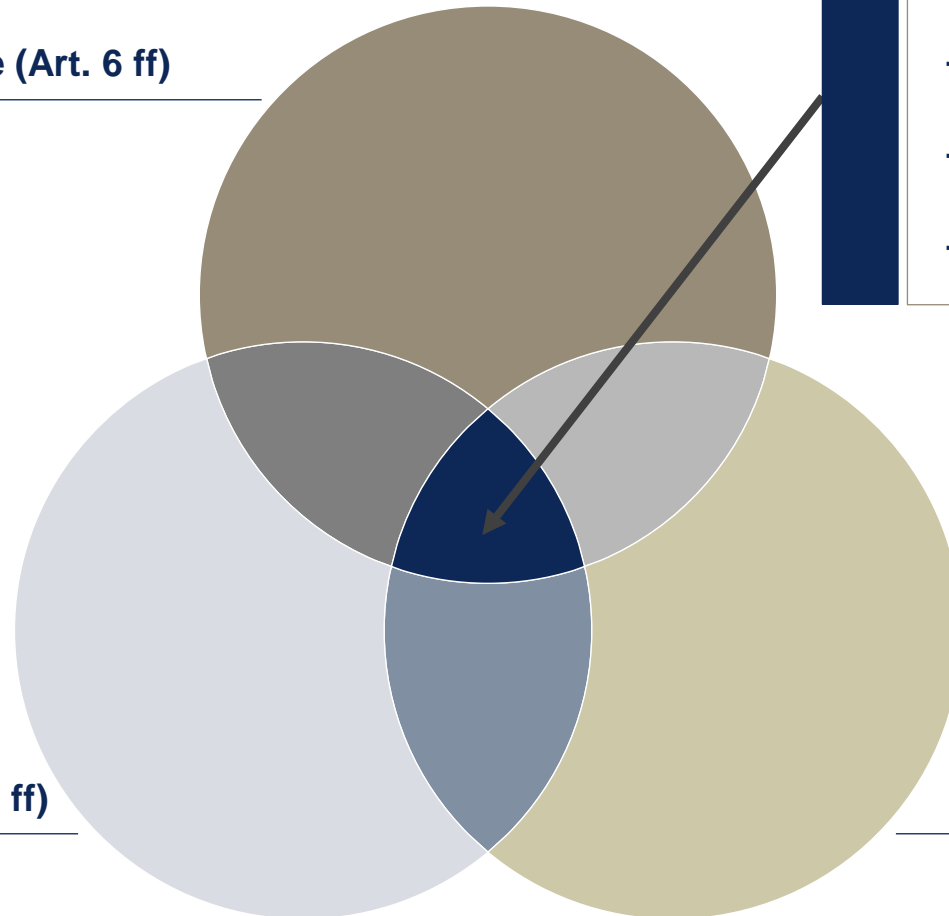
Zusammenfassung



Regeln für Hoch-Risiko-Systeme (Art. 6 ff)



Regeln für GPAI Modelle (Art. 51 ff)



GPAI-Modell

+ Benutzeroberfläche

+ Hochrisikozweck

+ Interaktion mit Menschen

Transparenzpflichten (Art. 50)



BEISPIEL

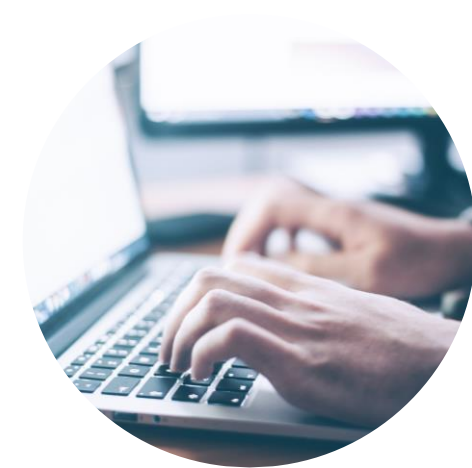
Wann wird GPAI Modell zu KI-System?



ChatGPT 3.5



**LLM eingebunden in
Python Script**



**Prompting in natürlicher
Sprache**

Ihre heutigen Referenten



Dr. Marc Ruttloff

Partner
Gleiss Lutz | Stuttgart



Moritz Julian Stilz

Assoziierter Partner
Gleiss Lutz | Stuttgart

Systematisierung von KI-
Systemen nach der KI-
Verordnung

10. September 2024

Standorte

Berlin

Washingtonplatz 3
10557 Berlin
Deutschland

T +49 30 800979-0
F +49 30 800979-979

Frankfurt

Taunusanlage 11
60329 Frankfurt
Deutschland

T +49 69 95514-0
F +49 69 95514-198

München

Karl-Scharnagl-Ring 6
80539 München
Deutschland

T +49 89 21667-0
F +49 89 21667-111

Brüssel

Rue de Lozum 25
1000 Brüssel
Belgien

T +32 2 551-1020
F +32 2 551-1039

Metaverse

Gleiss Lutz
42,-55 Decentraland

Düsseldorf

Dreischeibenhaus 1
40211 Düsseldorf
Deutschland

T +49 211 54061-0
F +49 211 54061-111

Hamburg

Görtz-Palais
Neuer Wall 86
20354 Hamburg
Deutschland

T +49 40 460017-0
F +49 40 460017-28

Stuttgart

Lautenschlagerstraße 21
70173 Stuttgart
Deutschland

T +49 711 8997-0
F +49 711 855096

London

125 Old Broad Street
London EC2N 1AR
Vereinigtes Königreich

F +44 20 7374 0811

www.gleisslutz.com

VIELEN DANK!