aringer herbst winklbauer

AI ACT – STRATEGISCHE WEICHENSTELLUNG & NEXT STEPS

WIE BEREITE ICH MEIN UNTERNEHMEN RICHTIG VOR?

20. November 2024
LSZ CIO-Kongress West 2024

Mag. Constantin Maetz
Rechtsanwaltsanwärter

AGENDA

AI ACT – Anwendungsbereich & Begriffe

Risikobasierter Ansatz - Risikopyramide

Umsetzung & Priorisierung

Wrap up & Discussion

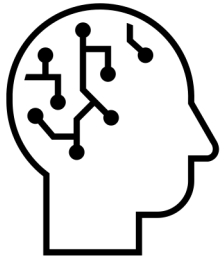
AI ACT –ZIELE DER VERORDNUNG, GELTUNGSBEREICH

- Teil der **EU-Digitalstrategie**
- unmittelbare Geltung (teilweise schon am 2.2.2025)
  - **KI-Systeme**
  - **KI-Modelle [mit allg. Verwendungszweck (GPAI)]**
- **Innovationsförderung** durch Rechtssicherheit und Reallabore (Regulatory Sandboxes)

WAS IST KI?

KI-System

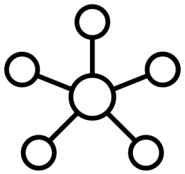
ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen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



1. **Computer-programm (Software)**
2. **Ausgaben durch Ableitung von Eingaben**
3. **relevante Information für Empfänger**
4. **gewisse Autonomie**

WAS IST KI?

KI-Modell mit allgemeinem Verwendungszweck (GPAI)



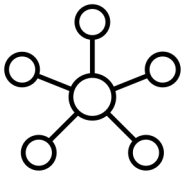
KI-Modell, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann

1. **allgemeine Verwendbarkeit**
2. **breites Aufgabenspektrum**
3. **nachgelagerte Systeme integrierbar**

ausgenommen Forschung, Entwicklung & OSS

WAS IST KI?

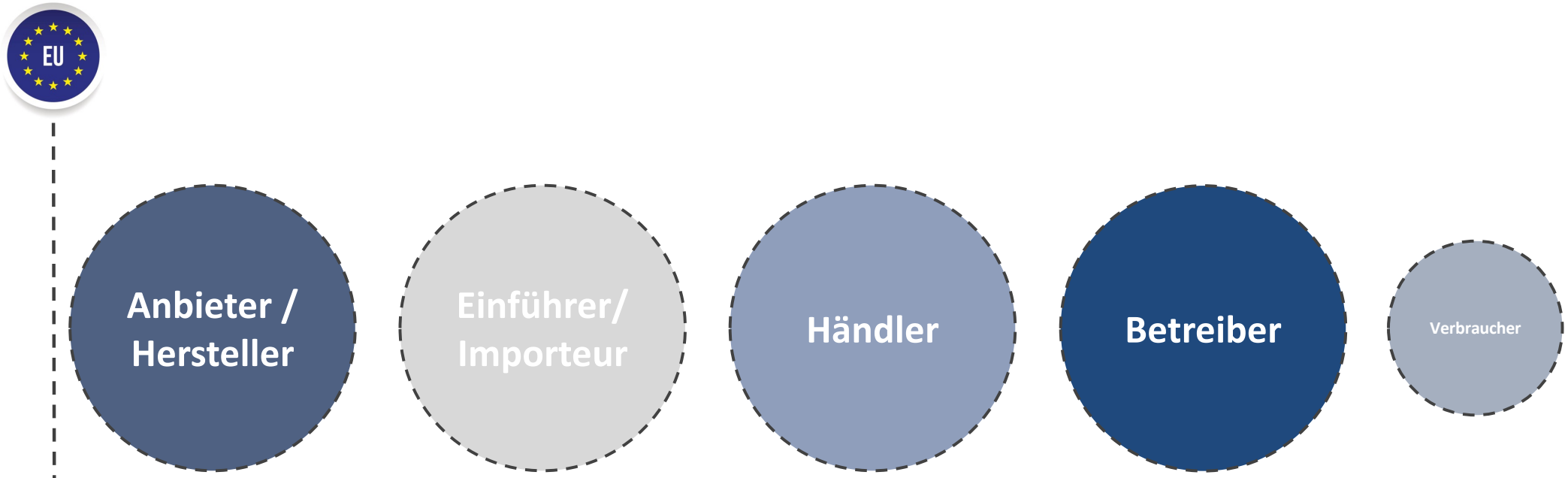
KI-Modell



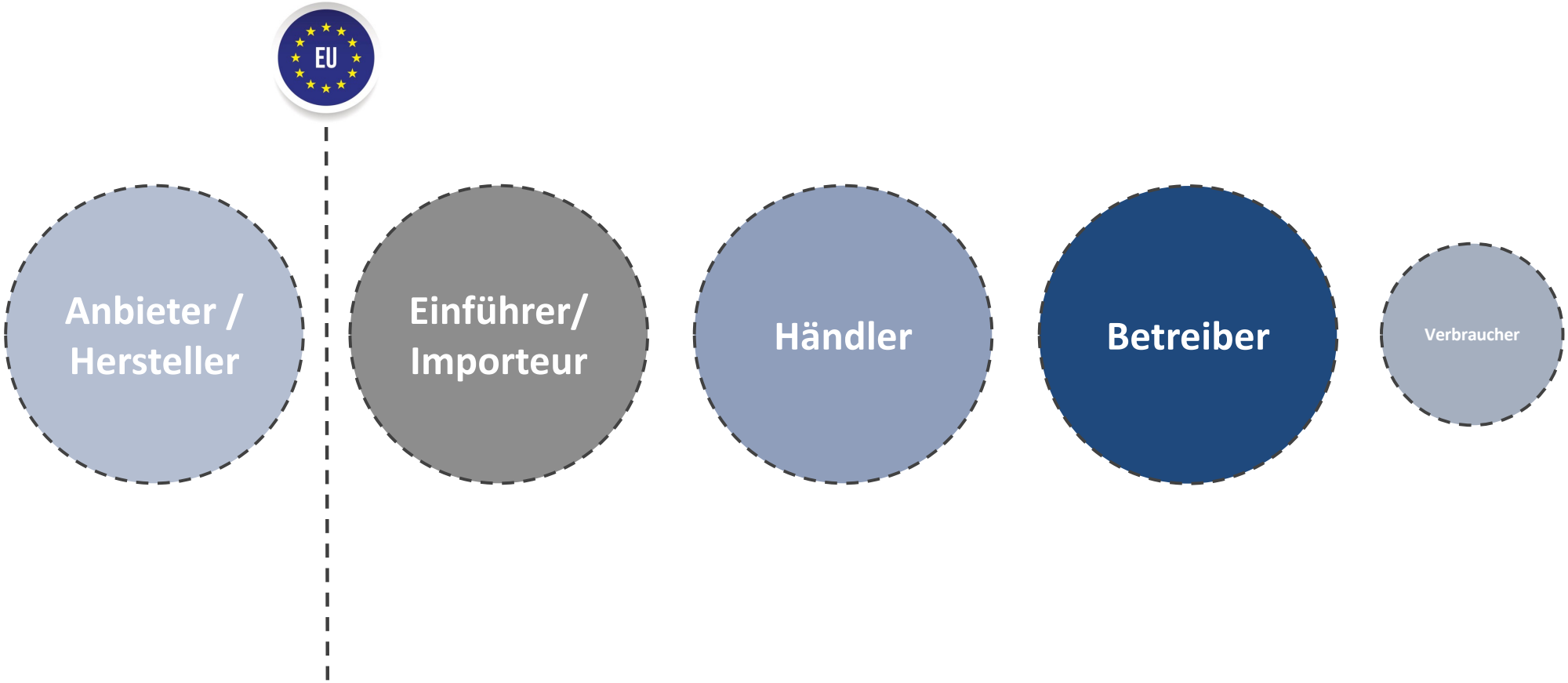
→ **ERROR 404**

1. **große Datenmenge**
2. **Ergebnis versch. Trainingsmethoden**
3. **keine Nutzerschnittstelle**

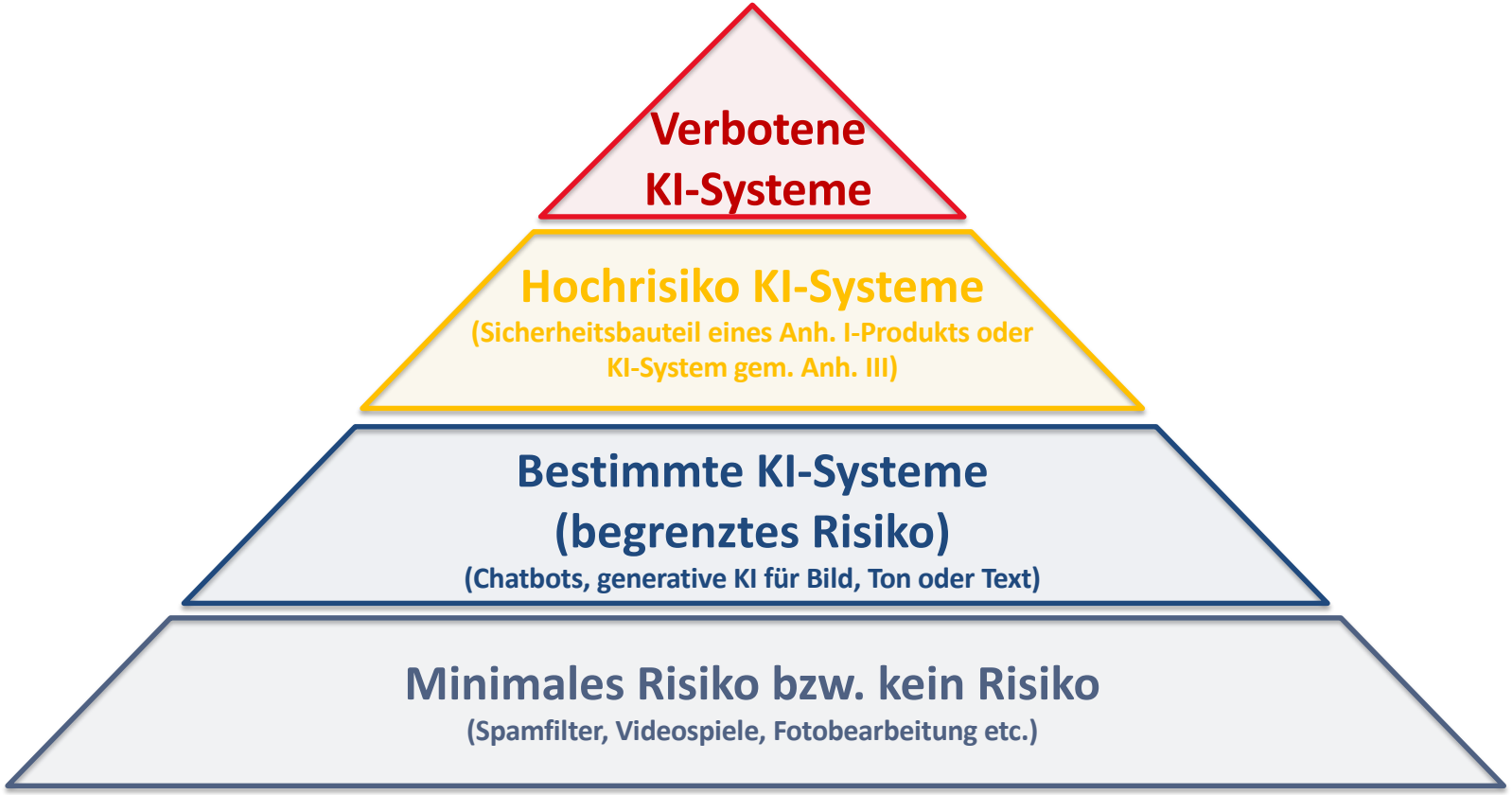
„AKTEURE“ (WHO IS WHO?)



„AKTEURE“ (WHO IS WHO?)



RISIKOBASIERTER ANSATZ – KI-SYSTEME

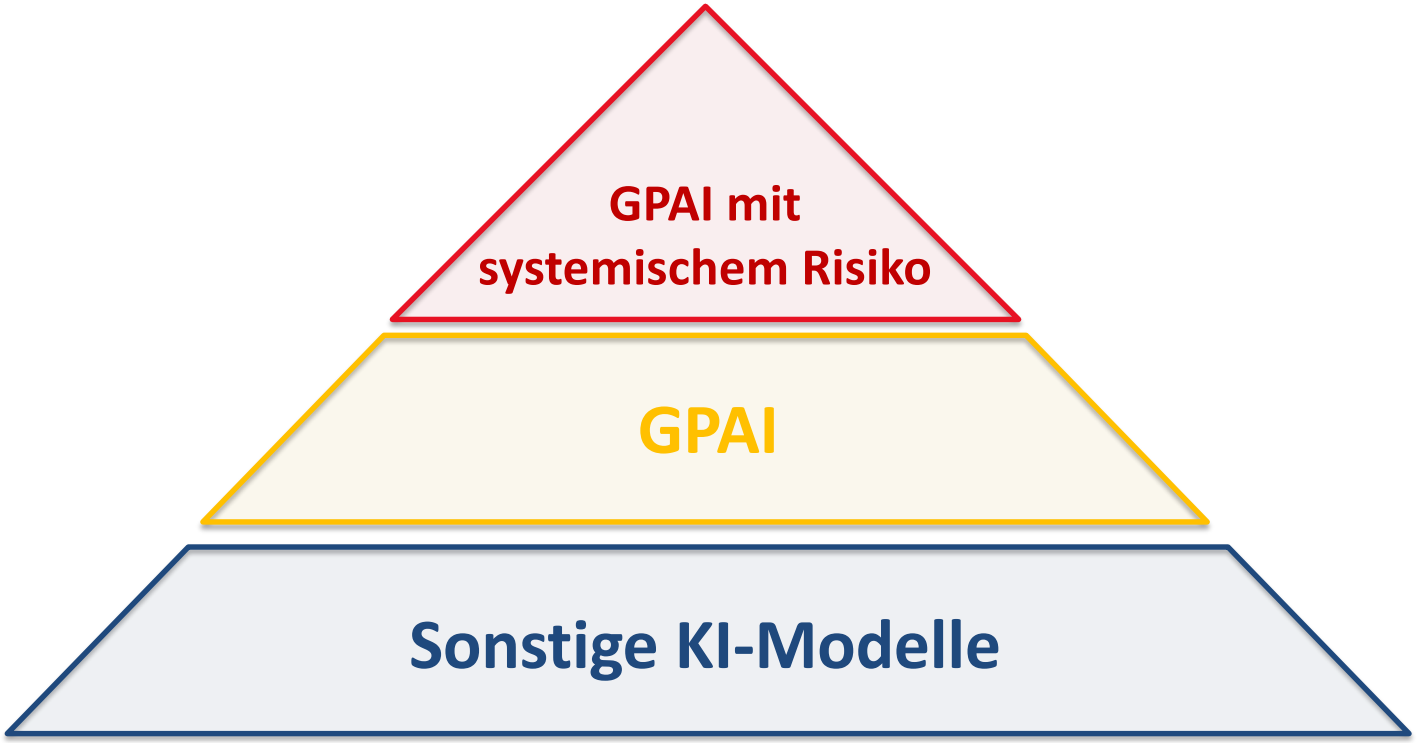


ANBIETER-VERPFLICHTUNGEN

Hochrisiko-KI

- **KI-Kompetenz** (auch außerhalb des Hochrisikobereichs!)
- **Risikomanagementsystem**
- **Technische Dokumentation**
- **Qualität** der Daten
  - Herkunft, Bias, Verzerrungen, Lücken und Mängel
- **Implementierung menschlicher Aufsicht**
- **Genauigkeit, Robustheit, Cybersicherheit**
- **Transparenz- und Informationspflichten** (Betriebsanleitung)
- **Konformitätsbewertung, CE-Kennzeichnung**
- **Registrierungspflicht** vor Inverkehrbringen
- **Qualitätsmanagement**, Korrekturmaßnahmen

RISIKOBASIERTER ANSATZ – KI-MODELLE



ANBIETER-VERPFLICHTUNGEN

GPAI mit systemischem Risiko

- **Modellbewertung**
  - Systemische **Risiken bewerten und mindern**
- **Schwerwiegende Vorfälle** melden und Dokumentieren
- Erhöhtes Maß an **Cybersicherheit**
- **Mitteilung an Kommission**

GPAI

- **Technische Dokumentation & Offenlegung**
- Allgemeine **Beschreibung** des Modells und der Entwicklung
- **Verhinderung** rechtsverletzender Inhalte (z.B. Urheberrecht)
- **Veröffentlichung** trainingsrelevanter Datensätze und urheberrechtlich geschützter Inhalte
- **Risikomanagementsystem**

BETREIBER-VERPFLICHTUNGEN

Hochrisiko-KI

- **KI-Kompetenz**
- Zweckentsprechende **Verwendung**
- **Menschliche Aufsicht**
- **Meldung** schwerwiegender Vorfälle
- **Aufbewahrung** von Protokollen
- evtl. **Datenschutz-Folgenabschätzung**
- **Nutzerrecht auf Erläuterung** der Entscheidungsfindung
- **Grundrechtefolgenabschätzung** (sofern im öffentl. Auftrag)

Bestimmte KI-Systeme & GPAI

- **KI-Kompetenz** (auch beim Einsatz von minimal risk KI!)
- **Kennzeichnungs-/Transparenzplicht** bei Interaktion mit Menschen
- **Täuschungsrisiko** minimieren bei generierten Inhalten

SANKTIONEN

Bis zu **35 Mio**. oder
7% des Jahresumsatzes

- Verstoß gegen Bestimmungen zu **verbotener KI**

Bis zu **15 Mio.** oder
3% des Jahresumsatzes

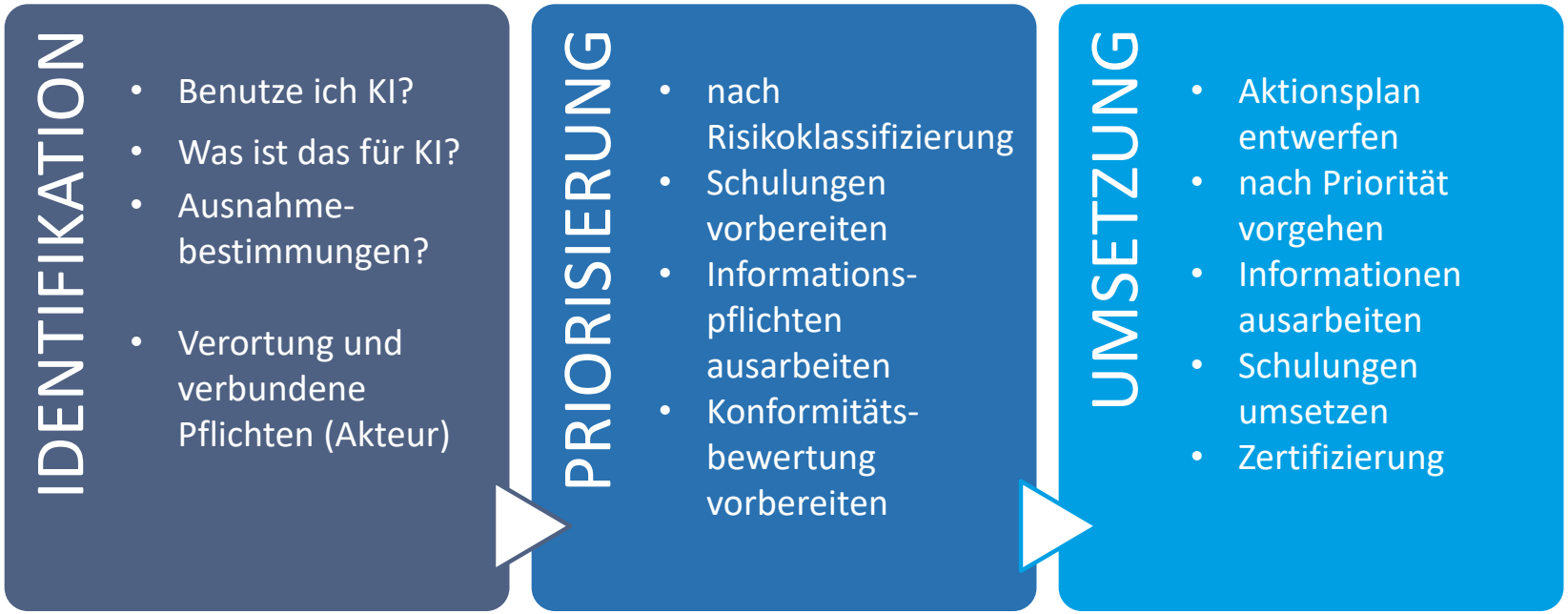
- Verstoß gegen Bestimmungen zu **Hochrisiko KI-Systemen**
- Verstoß gegen Bestimmungen zu **GPAI**
- Verstoß gegen Bestimmungen zu **Transparenzpflichten**

Bis zu **7,5 Mio.** oder
1% des Jahresumsatzes

- **Falsche, unvollständige oder irreführende Aussagen** gegenüber zuständiger Behörde im KI-Verfahren (Auskunfsersuchen)

AI ACT – GESTAFFELTE GELTUNG

VORBEREITUNG – STEP PLAN



KEY TAKE-AWAYS UND Q&A

- **Unterscheidung** KI-System und KI-Modell
- Unterschiedliche **Anforderungen** an unterschiedliche Akteure
- **Risikoverortung** (GPAI, Hochrisiko-KI, systemisches Risiko, kein Risiko)
- **Schulungen** beim Einsatz von KI im Unternehmen („**KI-Kompetenz**“)
- **Vorsicht** bei nicht-zweckentsprechender Verwendung v. Hochrisiko-KI

Diskussion und Fragen

VIELEN DANK!

Mag. Constantin Maetz
Rechtsanwaltsanwärter

aringer herbst winklbauer rechtsanwälte

Grillparzerstraße 5, 1010 Wien
+43 1 890 90 17
maetz@ahwlaw.at