



TaylorWessing AI



MERANTIX
MOMENTUM

AI Act – Entschlüsselt

20. Februar 2025 | Mareike C. Gehrman, Dr. Gregor Schmid & Fabio Vigliar



Agenda



01 Intro TW x MXM
Wer spricht heute? Was bringt uns heute zusammen?
Was ist unser Ziel für heute?

02 AI Act – Wo stehen wir heute?
Umsetzungsfristen der KI-VO
Update: Guidelines und Codes of Practice

03 Scoping – Bin ich betroffen?
Akteure der KI-VO
Anbieter vs. Betreiber
Hochrisiko-KI: Ja oder Nein?
Hochrisiko-KI: Anbieterpflichten
Hochrisiko-KI: Betreiberpflichten
Risikobasierter Ansatz der KI-VO
Dimension High-Risk / Low-Risk

04 Use Cases
Aufbau einer KI-Governance
Einsatz im Bereich HR
Einsatz im Bereich Public

05 AI Literacy
KI-Kompetenz – Was muss getan werden?
Praktische Empfehlungen für Corporates und KMUs

06 Next Steps & Diskussion
Einblicke aus der technischen Implementierung
Erfahrungen in der Rechtspraxis



01

Intro

TW x MXM

Wer spricht heute? Was bringt uns heute zusammen?



**Dr. Gregor Schmid, LL.M.
(Cambridge)**

Partner, Taylor Wessing



Fabio Vigliar

Lead AI Strategy

Merantix Momentum



Mareike Christine Gehrman

Partnerin, Taylor Wessing



Was ist unser Ziel für heute?

- Einblicke in Beispiele aus der Praxis für angewandte KI-Governance geben
- Strategien zur Integration der Einhaltung der KI-VO in technische und rechtliche Prozesse aufzeigen
- Klarheit darüber verschaffen, was die KI-Verordnung heute von Ihnen verlangt und wie Sie sich auf die Zukunft vorbereiten können



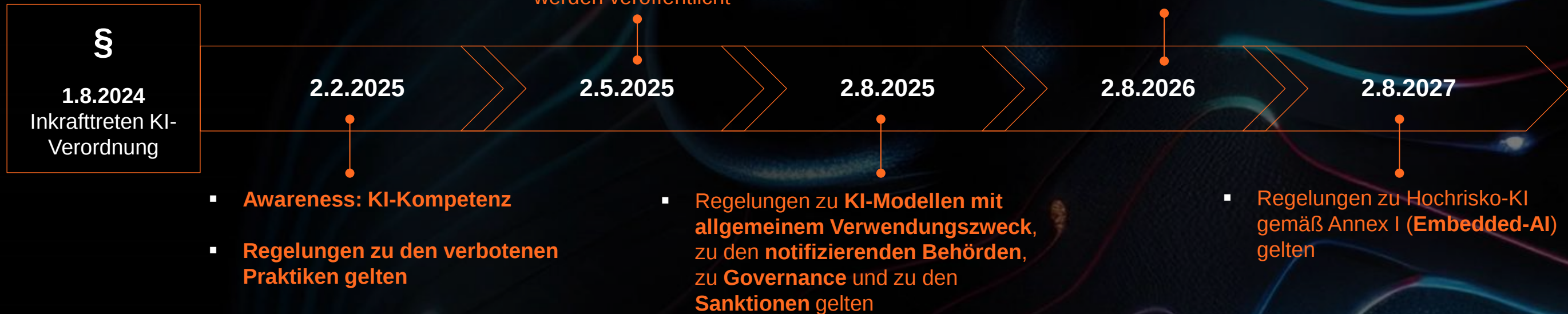
02

EU AI Act –

Wo stehen wir heute?

Umsetzungsfristen der KI-VO

Die KI-Verordnung wurde am **12. Juli 2024** offiziell im Amtsblatt der EU veröffentlicht und trat 20 Tage später, am **1. August 2024**, in Kraft. Bis zur vollumfänglichen Geltung sind Übergangsfristen vorgesehen:



Update: Guidelines und Codes of Practices

- In Bearbeitung: Das Amt für Künstliche Intelligenz erarbeitet mit den Stakeholdern aktuell die “**General-Purpose AI Code of Practice**”, welche die Umsetzung der Pflichten für **Anbieter von KI-Modellen mit allgemeinem Verwendungszweck und systemischen Risiken** erleichtern sollen.
 - Transparenz und Copyright policy (Art. 53 AI Act)
 - Pflichten für Anbieter von GPAI mit systemischem Risiko
- In Bearbeitung: Entwurf des KI-Büros des „**Template for summary of training data**“ für **Anbieter von KI-Modellen mit allgemeinem Verwendungszweck**
- In Bearbeitung: **Commission Guidelines on Application of the Definition of an AI System and the Prohibited AI Practices** Established in AI Act.

Update: Guidelines und Codes of Practices

- **Einige Datenschutzbehörden haben bereits zum Verhältnis von KI zum Datenschutz Stellung bezogen:**
 - Bayrisches Landesamt für Datenschutzaufsicht: KI & Datenschutz ([Link](#))
 - Europäischer Datenschutzbeauftragter: Generative AI and the EUDPR ([Link](#))
 - Landesbeauftragte für Datenschutz und Informationssicherheit Baden-Württemberg: Rechtsgrundlagen im Datenschutz beim Einsatz von KI ([Link](#))
 - CNIL (Frankreich): Fragen bei der Gestaltung eines KI-Systems ([Link](#))
 - Datenschutzkonferenz: Orientierungshilfe, Version 1.0 ([Link](#))
 - Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: Diskussionspapier: Large Language Models und personenbezogene Daten ([Link](#))

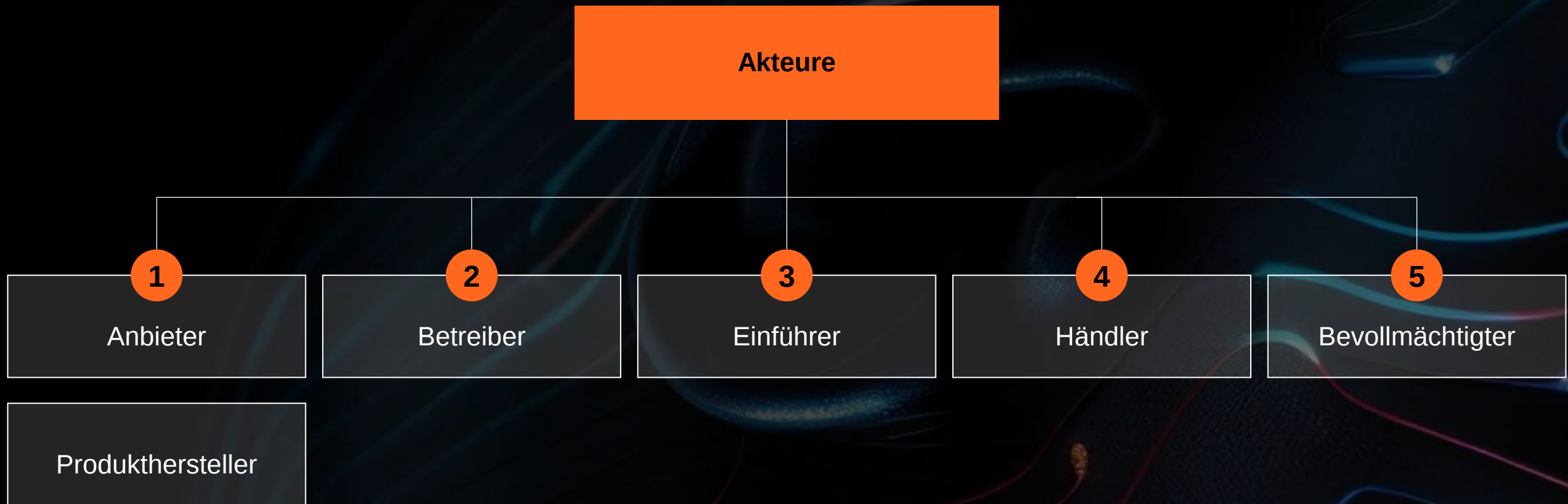


03

Scoping –

Bin ich betroffen? Und wenn, ja, wie?

Akteure der KI-VO



Anbieter vs. Betreiber

1

Sie sind Anbieter...

- wenn Sie das KI-System selbst entwickeln oder
- entwickeln lassen **und** es unter ihrem eigenen Namen **oder** ihrer Handelsmarke auf dem Markt bereitstellen oder in Betrieb nehmen.

2

Sie sind Betreiber...

- wenn Sie das KI-System in eigener Verantwortung verwenden,
- außer das KI-System wird persönlich und nicht-beruflich verwendet.

Anbieter vs. Betreiber



KI-Entwickler A
(Auftragnehmer)

KI-Käufer X
(Auftraggeber)

Szenario 1:
Beide Parteien
sind Anbieter

Anbieter

Anbieter

“KI made by X”

Der Käufer lässt ein KI-System entwickeln und bringt es unter eigenem Namen in den Betrieb.

Szenario 2:
KI-Entwickler ist
einziger Anbieter

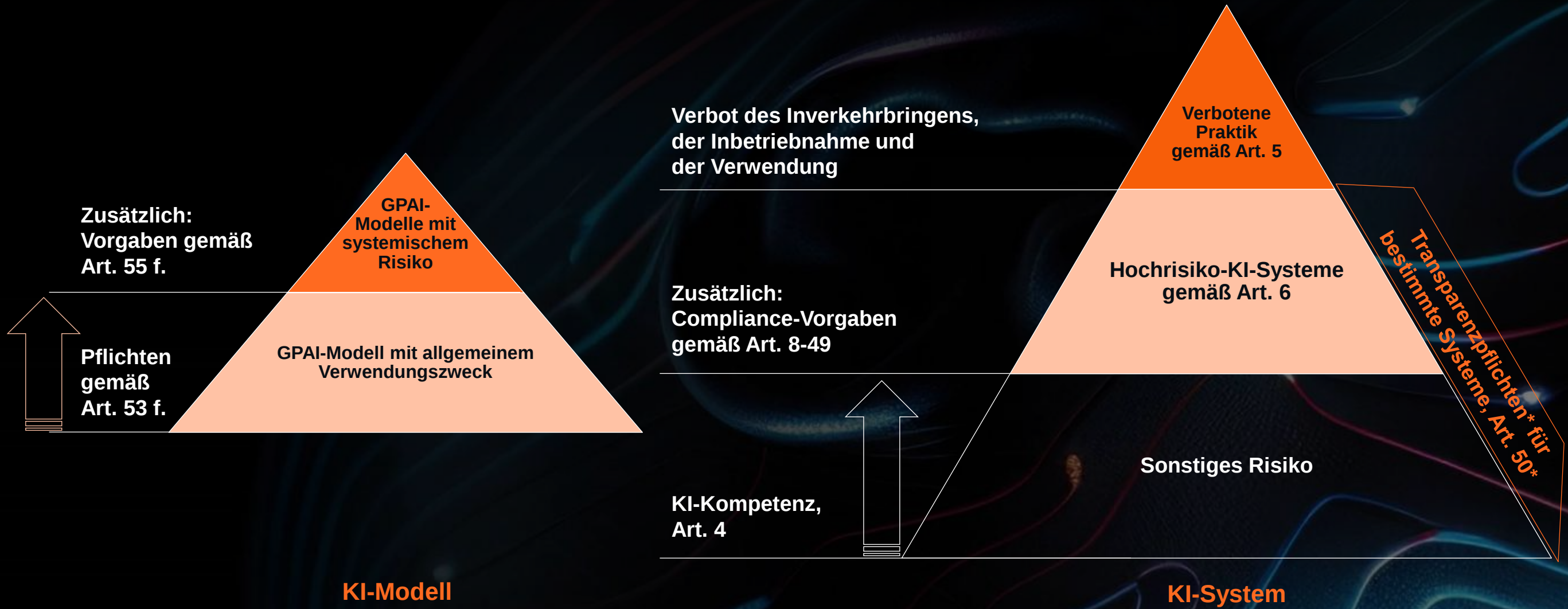
Anbieter

Kein Anbieter

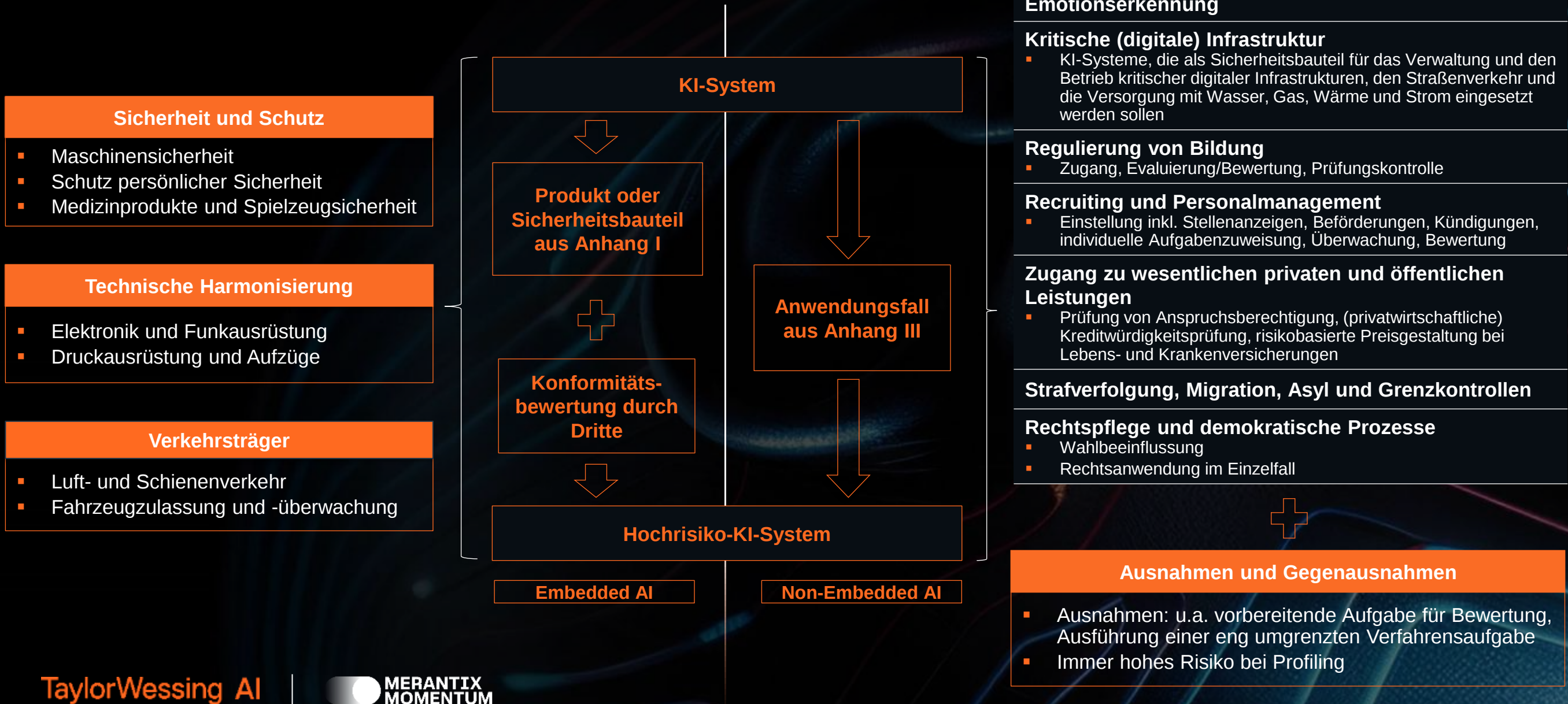
“KI powered by A”

Der Entwickler entwickelt ein KI-System und bringt dieses unter eigenem Namen in den Betrieb, der Käufer lizenziert es.

Risikobasierter Ansatz der KI-VO



Hochrisiko-Anbieter: Ja oder Nein?





04 KI Governance in der Praxis

Framework und Anwendungsfälle



Aufbau einer KI-Governance

Aufbau einer KI-Governance

☐ Bündelung von Kompetenzen durch Aufbau eines interdisziplinären KI-Teams

☐ Implementierung einer KI Strategie

☐ Definition klarer Verantwortlichkeiten und Rollen

☐ Definition der akzeptablen Risiken

☐ Prüfung, wo und welche KI bereits genutzt wird (KI-Inventur)

☐ Prüfung der Risikokategorie eingesetzter KI und Katalogisierung

☐ Aufbau einer Risikomanagementstruktur zur Einhaltung der gesetzlichen Vorgaben

☐ Schulung der Mitarbeiter bezüglich Nutzung von KI

☐ Entwicklung von Leitlinien, Awareness Strategien und Best-Practices

☐ Aufsetzen von internen Auditstrukturen

Wie setzen wir ein typisches KI-Projekt um?



Wir denken KI-Projektmanagement & -Governance zusammen





Beispiele aus realen KI-Anwendungen

Sprachmodelle für Ihr Unternehmen

Kannst du mir erklären, wie ich in unserem Unternehmen Adidas ein neues KI-Projekt aufsetze?

1. **Use Case definieren:** Klären Sie den konkreten Mehrwert des KI-Projekts für Adidas (z. B. Prognosen im Supply Chain, Demand-Forecasting, Personalisierung im E-Commerce). Definieren Sie klar messbare Ziele (KPIs).
2. **Stakeholder und Ressourcen festlegen:** Identifizieren Sie relevante Fachbereiche (z. B. IT, Data Analytics, Marketing) sowie Entscheidungsträger. Stellen Sie sicher, dass benötigte Budgets, Daten und Kompetenzen vorhanden sind.
3. **Daten- und Technologie-Check:**
 - **Datenqualität prüfen:** Welche Datenquellen sind verfügbar (z. B. ERP-, CRM-, POS-Daten)? Sind sie bereinigt und strukturiert?
 - **Technologie-Stack auswählen:** Cloud-Provider (AWS, GCP, Azure), KI-Frameworks (TensorFlow, PyTorch) und passende MLOps-Lösungen (z. B. Kubeflow). Berücksichtigen Sie Adidas-spezifische Vorgaben und Sicherheitsrichtlinien.
4. **Prototyp / Proof of Concept entwickeln:** Erstellen Sie einen ersten KI-Prototypen mit überschaubarem Funktionsumfang, um Machbarkeit und Nutzen zu validieren. So erkennen Sie frühzeitig technische Hürden.
5. **Rechtliche und Compliance-Aspekte:** Prüfen Sie Datensicherheit, Datenschutz (insbesondere DSGVO) und interne Compliance-Regeln, bevor Sie Daten verarbeiten oder Modelle ausrollen.
6. **Implementierung & Integration:** Passen Sie das KI-System an bestehende Systeme an (z. B. ERP-Integration). Sorgen Sie für robuste APIs oder Microservices, damit das Modell in Adidas-Prozesse eingebunden werden kann.

KI-STECKBRIEF

Tausende

Nutzer in Ihrer Organisation

30%

Beschleunigung in Textverarbeitung

FUNKTIONEN

- Datenschutzkonformer, sicherer und intern nutzbarer KI-Assistent
- 4 Funktionen: Zusammenfassung, Textgenerierung, Recherche & Chat
- Verbesserung der Effizienz & Qualität in allen Prozessen

Zentrale Fragen

1. Wie können wir verhindern, dass die Nutzer falsche Informationen eingeben, z. B. persönliche, sensible oder sicherheitskritische Daten, um eine Einstufung in ein Hoch-Risiko-System zu vermeiden?
2. Wenn wir GPT-Modelle wie von OpenAI verwenden, um eine Schnittstelle unter der Marke unseres Kunden zu erstellen, wer haftet dann für die Antworten, die das LLM liefert?

1. Hilfestellungen und Einschränkungen für Benutzer





2. LLM-Anbieter müssen konforme Modelle veröffentlichen

- Anbieter wie OpenAI veröffentlichen Systemkarten, die ihre Modelle und deren Verwendung erklären.
- Dies sollte Sie davor schützen, für das Modell selbst haften zu müssen (da Sie es ohnehin nicht erklären können).
- Aber wie würde das in der Praxis funktionieren? Kann ich die Haftung wirklich vergessen, wenn ich ein LLM in meinem System verwende?

GPT-4o System Card

OpenAI

August 8, 2024

1 Introduction

GPT-4o[1] is an autoregressive omni model, which accepts as input any combination of text, audio, image, and video and generates any combination of text, audio, and image outputs. It's trained end-to-end across text, vision, and audio, meaning that all inputs and outputs are processed by the same neural network.

GPT-4o can respond to audio inputs in as little as 232 milliseconds, with an average of 320 milliseconds, which is similar to human response time[2] in a conversation. It matches GPT-4 Turbo performance on text in English and code, with significant improvement on text in non-English languages, while also being much faster and 50% cheaper in the API. GPT-4o is especially better at vision and audio understanding compared to existing models.

In line with our commitment to building AI safely and consistent with our voluntary commitments to the White House[3], we are sharing the GPT-4o System Card, which includes our Preparedness Framework[4] evaluations. In this System Card, we provide a detailed look at GPT-4o's capabilities, limitations, and safety evaluations across multiple categories, with a focus on speech-to-speech (voice)¹ while also evaluating text and image capabilities, and the measures we've implemented to ensure the model is safe and aligned. We also include third party assessments on dangerous capabilities, as well as discussion of potential societal impacts of GPT-4o text and vision capabilities.

2 Model data and training

GPT-4o's text and voice capabilities were pre-trained using data up to October 2023, sourced from a wide variety of materials including:

- **Select publicly available data**, mostly collected from industry-standard machine learning datasets and web crawls.
- **Proprietary data from data partnerships**. We form partnerships to access non-publicly available data, such as pay-walled content, archives, and metadata. For example, we partnered with Shutterstock[5] on building and delivering AI-generated images.

¹Some evaluations, in particular, the majority of the Preparedness Evaluations, third party assessments and some of the societal impacts focus on the text and vision capabilities of GPT-4o, depending on the risk assessed. This is indicated accordingly throughout the System Card.

Hoch Risiko oder nicht? Oft eine Frage des Designs

Recommendation Engine

Das KI-System schätzt Fälle eigenständig ein und stellt Empfehlungen aus, ob Sozialleistungen ausgezahlt werden sollen.

- Der Zugang zu staatlichen Leistungen wird algorithmisch bestimmt.
- Die Kontrolle über den Algorithmus wird womöglich vernachlässigt.

RAG-System

Das KI-System beantwortet spezifische Fallfragen nach Recherche in vorher festgelegten und ratifizierten Quelldokumenten, z.B. Gesetzen.

- Die SachbearbeiterInnen erhalten eine Hilfestellung mit Quellenangabe
- Die Ausgabe des KI-Systems muss menschlich verarbeitet werden.



Einsatz im HR-Bereich

Anwendungsfälle im HR-Bereich

■ Recruiting

- Stellenanzeige
- Auswahl
- Sourcing (Ermittlung geeigneter Kandidaten im Internet)
- Matching
- People Analytics

■ Personalplanung

- Identifizierung von Verbesserungspotenzialen
- Hochrisiko-KI?
- Verbotene Praktiken (z.B. Social Scoring)?

■ Kündigung

- Sozialauswahl
- Berechnung von Abfindungen
- Formulieren von Abmahnungen und Kündigungsschreiben



Einsatz im Bereich Public

Einsatz eines Tools zur Unterstützung in Verwaltungsaufgaben

Anwendungsfall im Bereich Public

- **Scoping / Rolle**

- Anbieter vs. Betreiber

- **Hochrisiko-KI? Z.B.**

- Beschäftigung und Personalmanagement
- allgemeine und berufliche Bildung
- Inanspruchnahme öffentlicher Dienstleistungen
- Strafverfolgung

- **Transparenzpflichten: Art. 50 AI Act**

- **KI-Kompetenz**

- **ToDo's**

- Maßnahmen zur Vermeidung der Anbietereigenschaft
- KI-Kompetenz, Onboarding-Training
- Periodische Überprüfung / Risk Assessment



05 AI Literacy – KI-Kompetenz



KI-Kompetenz – Was muss getan werden?

Art. 4 KI-VO: „Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre **technischen Kenntnisse**, ihre **Erfahrung**, ihre **Ausbildung** und **Schulung** und der **Kontext**, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind.“

Was ist gemeint?

- Verständnis der Funktionsweise von KI generell **und** im konkreten Anwendungsfall
- Instruktions- **und** Schulungspflicht
- Zum Zwecke des Bewusstseins für die Potenziale **und** (!) die Risiken

Do's

- Regelmäßige, personalisierte Aus- und Fortbildung, z.B. über technische, rechtliche und ethische Themen wie
 - „Wie funktioniert ein KI-System?“
 - „How to prompt?“
 - „Herausforderungen durch KI“
- Berücksichtigung der konkreten Verwendung im Unternehmen und durch die zu schulenden Mitarbeiter. Anwendungsfallbezogene Aus- und Fortbildung
- Dabei darf der technologische Fortschritt nicht außer Acht gelassen werden – KI steht nicht still!

Dont's

- Unternehmensweite Freigabe von KI-Verwendung
- Einmalige Schulungen
- Unreflektierte Nutzung von KI-Ausgaben
- Vernachlässigung der Erklärbarkeit von KI macht die notwendige AI literacy unmöglich



06 Next Steps & Diskussion

Einblicke aus der technischen Implementierung

1

Katalogisieren

Erfassen Sie die KI-Systeme, die Sie nutzen, an denen Sie arbeiten oder in die Sie investieren möchten.

2

Integrieren

Sensibilisieren Sie und bauen Sie Expertise zur KI-Verordnung in Ihrer Führungsebene auf.

3

Abstimmen

Passen Sie Ihre KI- und Unternehmens-Strategie an die KI-Verordnung an, um Risiken zu mindern.

Durchführung von
Risikobewertungen für alle KI-Systeme

Technische Entscheidungen
dokumentieren

Vorbereitung auf die Kosten für die Einhaltung der Vorschriften

Erfahrungen aus der Rechtspraxis

Einbettung von LLMs

- Wer ist Anbieter des GPAI-Modells?
- Gibt es einen Einführer? (KI-System vs. KI-Modell)
 - Achtung: Wer ist mein Vertragspartner?
- Wer ist Anbieter des KI-Systems? Welche Pflichten gelten?
- Anbieter gemäß Art. 25 KI-VO?



Fragen? Anmerkungen?



Merantix: Providing Excellence in AI since 2019



We are Germany's leading consultancy with a clear focus on AI.

5 years experience

150+ projects

60 employees

Contact

Fabio Vigliar
Lead AI Strategy

fabio.vigliar@merantix-momentum.com

Merantix Momentum GmbH

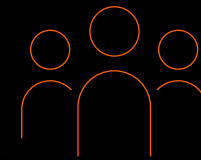
Max-Urich-Straße 3
13355 Berlin
Deutschland

www.merantix-momentum.com

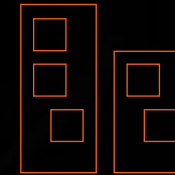
Taylor Wessing Standorte weltweit



Wir verbinden praxisnahe Beratung und fundiertes Branchen-Know-how mit internationaler Erfahrung und Kenntnis der lokalen Märkte.



1.200+
Anwält:innen



28
Büros



17
Länder

Belgien	▪Brüssel
China	▪Hongkong ▪Peking* ▪Shanghai*
Deutschland	▪Berlin ▪Düsseldorf ▪Frankfurt ▪Hamburg ▪München
Frankreich	▪Paris
Großbritannien	▪Cambridge ▪Liverpool ▪London ▪London Tech City
Niederlande	▪Amsterdam ▪Eindhoven
Österreich	▪Wien ▪Klagenfurt*
	▪Warschau
	▪Dublin
Slowakei	▪Bratislava
Südkorea	▪Seoul**
Tschechische Republik	▪Prag ▪Brünn*
Ukraine	▪Kiew
Ungarn	▪Budapest
USA	▪Silicon Valley* ▪New York*
VAE	▪Dubai

* Repräsentanzen

** Assoziierte Büros

... melden Sie sich bei Taylor Wessing



Mareike Christine Gehrman

Partnerin, Taylor Wessing



**Dr. Gregor Schmid, LL.M.
(Cambridge)**

Partner, Taylor Wessing



... melden Sie sich bei Taylor Wessing



**KI-Kompetenz –
Basiswissen für Ihre
Mitarbeiter:innen
und Externe**

Online-Schulung

TaylorWessing

 Anmeldung und Kosten:
Unsere Basisschulung ist kostenpflichtig, Staffelpreise für Unternehmen möglich.
Alle Informationen zu Preisen, Schulungs-Terminen und Anmeldung.

taylorwessing.com



Ihre Ansprechpartnerinnen:



Mareike Christine Gehrman, Fachanwältin für IT-Recht
Telefon: + 49 211 / 83 87 162
E-Mail: m.gehrmann@taylorwessing.com



Dr. Anne Förster, Fachanwältin für Arbeitsrecht
Telefon: + 49 211 / 83 87 118
E-Mail: a.foerster@taylorwessing.com

Demnächst auch als eLearning-Tool.

