TECHNISCHE UNIVERSITÄT DARMSTADT

How to (AI) Act

KI kompetent nutzen –
Wie Algorithmen und Agenten Wirtschaft und Arbeitswelt verändern

Janine Wendt

Bürgerliches Recht u. Unternehmensrecht

TU Darmstadt

AI ACT

TECHNISCHE UNIVERSITÄT DARMSTADT

Ausgangslage

- Am **1. August 2024** trat die Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (= AI Act) in Kraft.
- Die Übergangsfristen zur Anwendbarkeit liegen zwischen **sechs Monaten und drei Jahren**.
- Beim AI Act handelt es sich um den **ersten umfassenden Rechtsrahmen für die Entwicklung, Herstellung und Nutzung von KI weltweit**.

AI ACT

TECHNISCHE UNIVERSITÄT DARMSTADT

KI-Kompetenz

- Art. 4 AI Act: „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.“

AI ACT

TECHNISCHE UNIVERSITÄT DARMSTADT

KI-Kompetenz

- Art. 3 Ziff. 56 AI Act definiert KI-Kompetenz als „die **Fähigkeiten**, die **Kenntnisse** und das **Verständnis**, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, **KI-Systeme sachkundig einzusetzen** sowie sich **der Chancen und Risiken** von KI und möglicher Schäden, die sie verursachen kann, **bewusst zu werden**.“
- Gesetzgeber wählt damit ein flexibles System der Kompetenzanforderungen, das eine Differenzierung nach „**allgemeinen KI-Kompetenzen**“ und „**spezifischen KI-Kompetenzen**“ zulässt.

AI ACT

TECHNISCHE UNIVERSITÄT DARMSTADT

KI-Kompetenz

- Nach ErwG 20 AI Act soll die KI-Kompetenz allen einschlägigen Akteuren der KI-Wertschöpfungskette die Kenntnisse vermitteln, „**die erforderlich sind, um die angemessene Einhaltung und die ordnungsgemäße Durchsetzung“ des AI Acts sicherzustellen**.
- Das legt nahe, dass auch rechtliche Kenntnisse Inhalt der KI-Kompetenz sind.

HESSIAN.AI.LITERACY

FREE WORKSHOP ON AI LITERACY

September 25, 2025
10 AM - 2 PM
Frankfurt UAS, Building Section B,
2. Floor, Room 205/206

Keynote by Kai Zenner
(Head of Office & Digital Policy Adviser,
Axel Voss, MEP European Parliament)

hessian.AI
FRANKFURT UNIVERSITY OF APPLIED SCIENCES
ReLaTe Research Lab for Law and applied Technologies
dit lab Research Lab for Digital Innovation & Transformation
COMPLIANCE & REGULATION Bürgerliches Recht und Unternehmensrecht
TECHNISCHE UNIVERSITÄT DARMSTADT

AI ACT

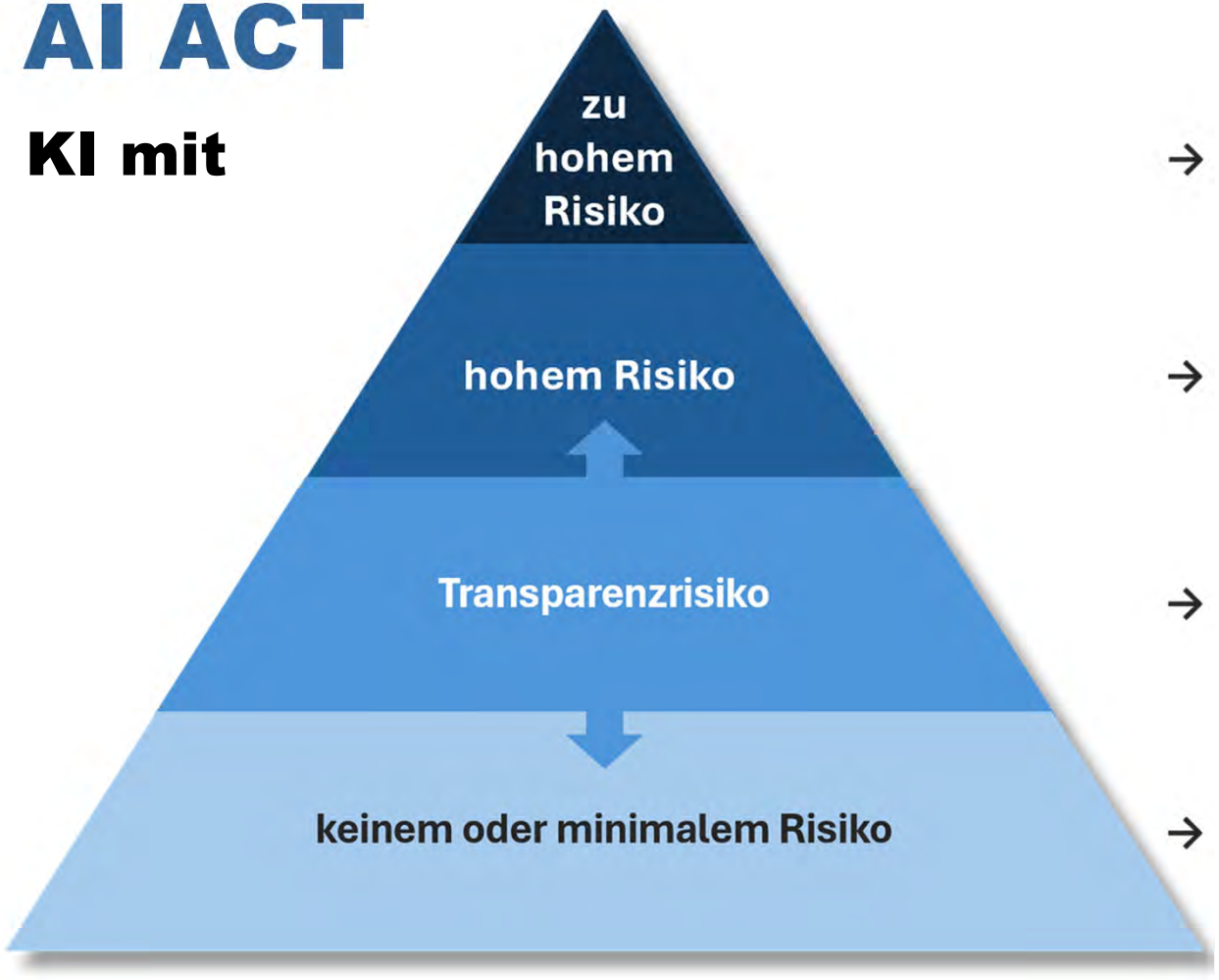
TECHNISCHE UNIVERSITÄT DARMSTADT

Regulierungsansatz

- **Horizontal**: Keine sektorale, sondern branchenübergreifende Regulierung
- **Technologieneutral**: Regulierung des spezifischen Einsatzes, nicht des KI-Systems als solches
- **Risikoorientiert**: Verknüpfung von Vorgabenintensität und Risikohöhe

AI ACT

KI mit



→ **verbotene Praktiken**

→ **Compliance-Anforderungen**

→ **Transparenz-Anforderungen**

→ **Verhaltens-kodizes**

AI ACT

TECHNISCHE UNIVERSITÄT DARMSTADT

Pflichten für Anbieter und Betreiber

- **Anbieter:** natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell für allgemeine Zwecke entwickelt oder entwickeln lässt und es unter eigenem Namen oder Handelsmarke entgeltlich oder unentgeltlich in den Verkehr bringt oder in Betrieb nimmt;
- **Betreiber:** natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht-beruflichen Tätigkeit verwendet.

TECHNISCHE UNIVERSITÄT DARMSTADT

PFLICHTEN FÜR ANBIETER

Qualitätsmanagementsystem

Aufbewahrung der Dokumentation

Aufbewahrung der automatisch erzeugten Protokolle

Konformitätsbewertungsverfahren vor Inverkehrbringen

EU Declaration of Conformity und CE-Kennzeichnung

Registrierung in der EU-Datenbank

Maßnahmen gegen nicht-konforme KI-Systeme

TECHNISCHE UNIVERSITÄT DARMSTADT

PFLICHTEN FÜR BETREIBER

Anwendung entsprechend der Betriebsanleitung

Menschliche Aufsicht mit entsprechender Kompetenz und Entscheidungsbefugnis

Überwachung des Systems und evtl. Information an den Anbieter

Meldung an Anbieter und Behörde bei ernstem Zwischenfall

Aufbewahrung der automatisch erzeugten Protokolle

AI ACT

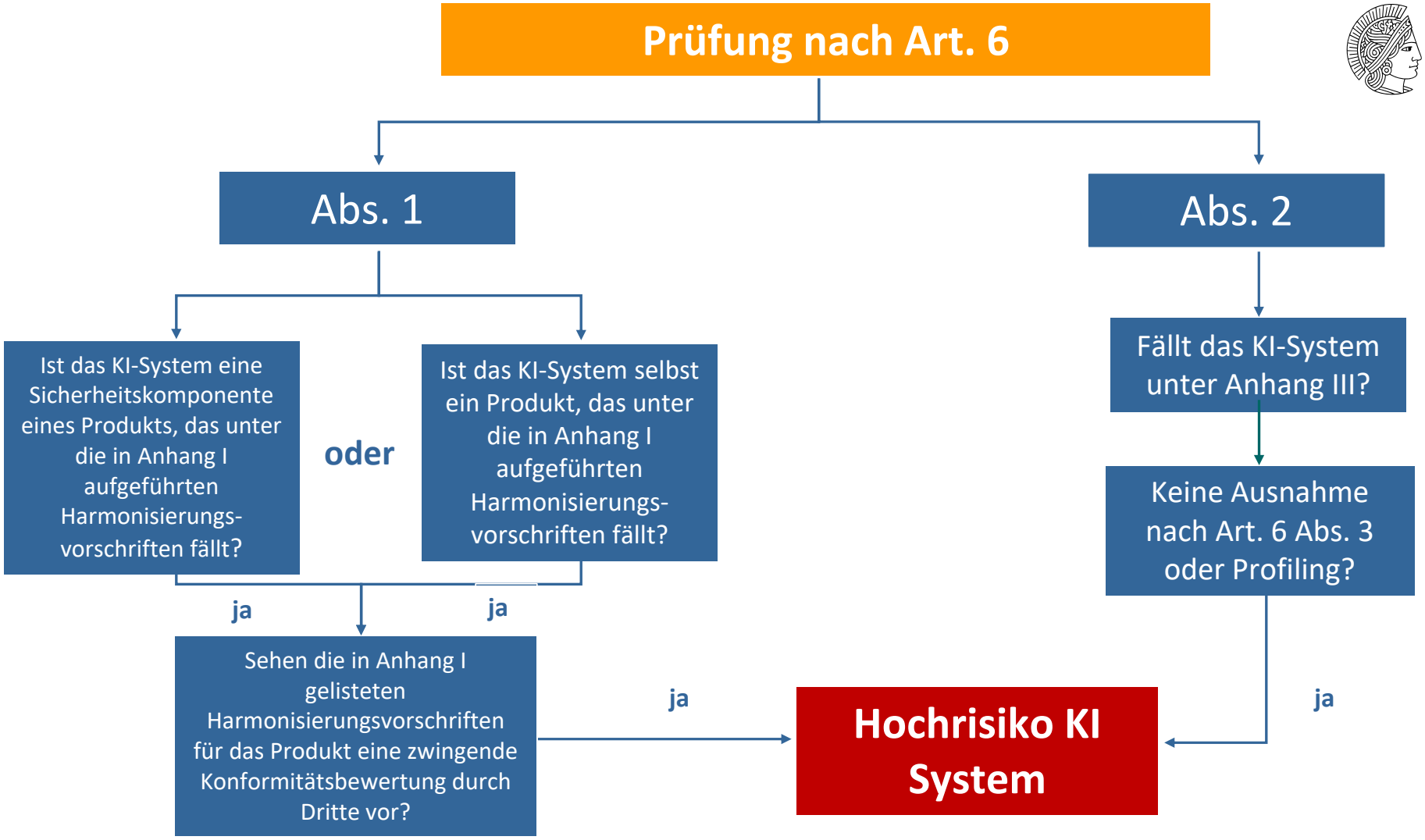
TECHNISCHE UNIVERSITÄT DARMSTADT

Wann ist ein KI System mit hohem Risiko behaftet?

- Der AI Act gibt eine **Methodik** vor, um KI Systeme mit hohem Risiko zu ermitteln.
- Ein Hochrisiko KI System wird in Art. 6 Abs. 1, 2 unter Verweis auf **Anhang I** und **Anhang III** definiert.

TECHNISCHE UNIVERSITÄT DARMSTADT

Prüfung nach Art. 6



AI ACT GPAI

AI ACT GPAI

- Welche Vorgaben für **KI-Modelle mit allgemeinem Verwendungszweck (= General Purpose AI = GPAI)** gelten sollen, zu denen regelmäßig auch die generative KI gehört, war ein umstrittener Diskussionspunkt im Trilog.
- Zunächst legt der AI Act selbst nicht dezidiert fest, wann ein KI-Modell als GPAI gilt. Er stellt lediglich darauf ab, dass das KI-Modell „**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** […]“.

AI ACT GPAI

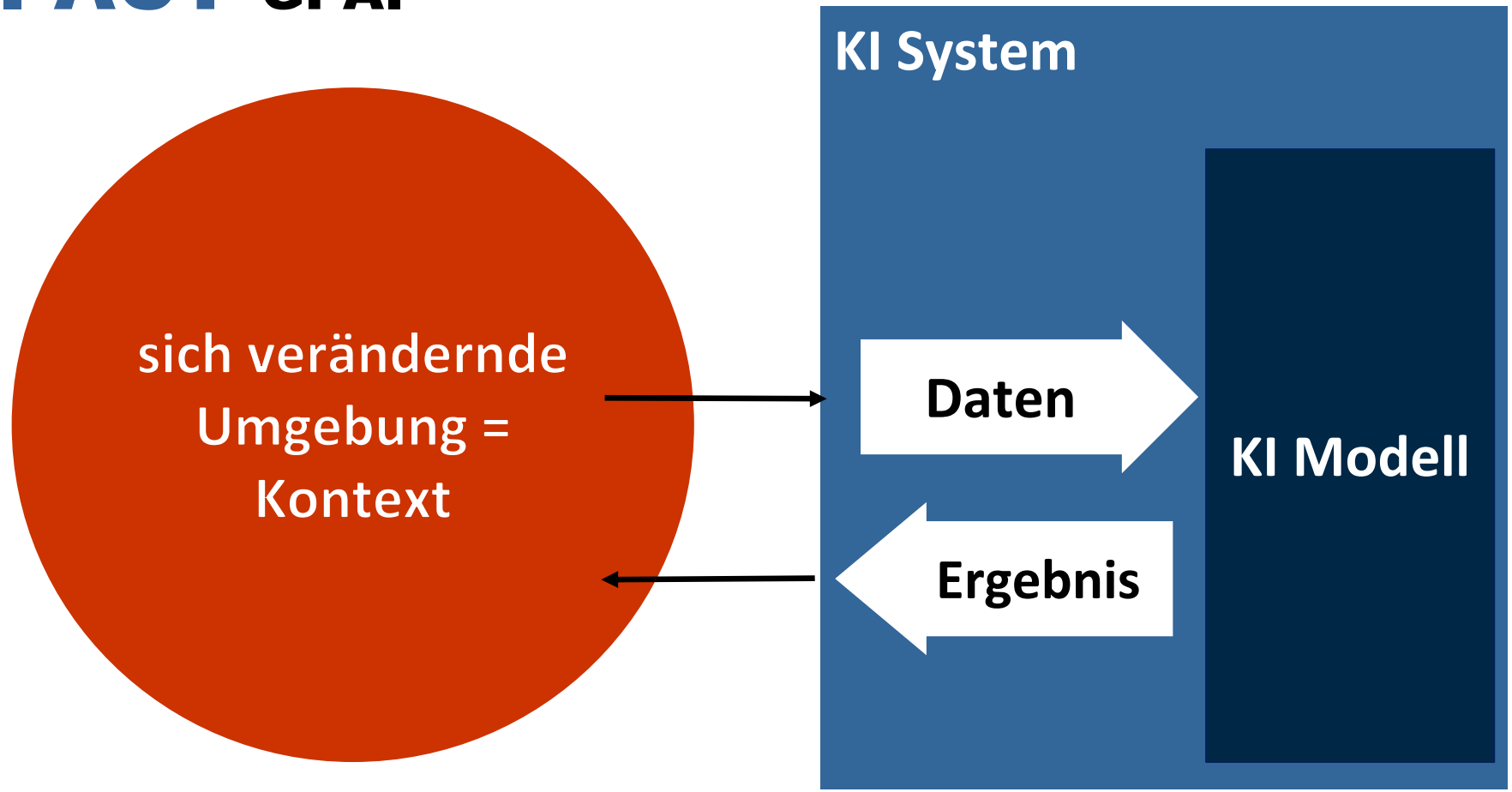
- Eine rechtsklare Abgrenzung erfolgte erst jüngst über die **GPAI-Leitlinien der EU-Kommission** vom 18.7.2025.
- Die Leitlinien legen einen **quantitativen Schwellenwert** fest: Ob es sich um eine KI mit allgemeinem Verwendungszweck handelt, wird anhand der **Rechenleistung entschieden, die für das Training des Modells verwendet** wurde. Als Grenzwert gilt eine kumulierte Menge von mehr als 10^{23} Gleitkomma-Operationen, gemessen in Floating Point Operations (FLOPs).
- Das multidisziplinäre Forschungsinstitut EpochAI veröffentlichte im April 2024 eine Einschätzung, welche Rechenleistung in das **Training der großen Modelle** fließt: Viele Modelle überschritten hiernach bereits die Schwelle von 10^{23} FLOPs.

AI ACT GPAI

- Der Begriff der **generativen KI** fällt im AI Act demgegenüber lediglich in den **Erwägungsgründen** 99 und 105:
- **Generative KI-Modelle** sollen als ein **typisches Beispiel für GPAI-Modelle** gelten, da sie in der Regel eine flexible Erzeugung von Inhalten ermöglichen – etwa in Form von Text-, Audio-, Bild- oder Videoinhalten, die ein weites Spektrum unterschiedlicher Aufgaben umfassen können.

TECHNISCHE UNIVERSITÄT DARMSTADT

AI ACT GPAI



AI ACT GPAI

- Dabei werden allgemeine GPAI-Modelle häufig **modifiziert** bzw. zu neuen KI-Modellen **optimiert**. Auf das Pre-Training, das mit einem großen allgemeinen Datensatz stattfindet, folgt in diesem Fall eine **Feinabstimmung** für konkrete Aufgaben. Vor allem die hinteren Schichten des GPAI-Modells werden hierbei verändert, um die Fähigkeiten mit Blick auf eine konkrete Zielsetzung zu verbessern.
- **Wird der Betreiber durch das Finetuning zum neuen Anbieter**? Der AI Act gibt hierauf keine Antwort. Er kennt zwar die wesentliche Änderung in Art. 25 AI Act, aber nur für die regulären KI-Systeme, nicht für GPAI-Modelle.

AI ACT GPAI

- Auch diese Regelungslücke haben die GPAI-Leitlinien vom 18.7.2025 geschlossen: Sie ziehen erneut die Rechenleistung heran, um die **Änderungsintensität eines Finetunings** zu bemessen:
- Trainiert ein Unternehmen ein Modell mit mehr als einem Drittel der ursprünglichen Menge an FLOPs nach, wertet das AI Office **das neue Modell als eigenständig**.
- Ein Drittel der ursprünglichen Trainingsrechenleistung ist eine enorm große Menge für ein Finetuning. Die Messlatte liegt hoch, damit gerade kleinere Unternehmen und Start-ups, die nur geringe Anpassungen vornehmen, **nicht automatisch als Anbieter gewertet** werden.

AI ACT GPAI

- Bei der **inhaltlichen Ausfüllung der Anbieterpflichten** konzentriert sich der AI Act vorrangig auf GPAI-Systeme und Modelle mit **systemischem Risiko**.
- Ein systemisches Risiko liegt vor, wenn ein KI-Modell etwa aufgrund seiner Reichweite tatsächliche oder vorhersehbare **negative Folgen für die öffentliche Gesundheit, die Sicherheit, die Grundrechte oder die Gesellschaft insgesamt** entfaltet, die sich auch über die Wertschöpfungskette hinweg verbreiten können.

AI ACT GPAI

- Ein GPAI-Modell weist ein systemisches Risiko auf, wenn es über Fähigkeiten **mit hohem Wirkungsgrad** verfügt. Aktuell geht der AI Act davon aus, dass ein hoher Wirkungsgrad vorliegt, wenn die **kumulierte Menge der für das Training verwendeten Berechnungen**, gemessen in Gleitkommaoperationen **(FLOPs)**, mehr als 10^{25} beträgt.
- Das **AI Office** wird diesen Wert dem technischen Fortschritt anpassen und **weitere Kriterien** (z.B. Anzahl der Nutzer oder Grad der Autonomie des Modells) **benennen**.

AI ACT GPAI

- Anbieter von Modellen mit systemischen Risiken sind verpflichtet, ihre Risiken zu bewerten, **schwerwiegende Vorfälle zu melden**, **Tests und Modellbewertungen** nach dem neuesten Stand der Technik **durchzuführen**, **Cybersicherheit** zu gewährleisten und **Angaben zum Energieverbrauch ihrer Modelle** zu machen.

AI ACT GPAI

- Eine Konkretisierung der Pflichten erfolgt über den **Praxisleitfaden (Code of Practice)** für GPAI.
- Die Erarbeitung des Leitfadens erfolgte ab Herbst 2024 in einem **Multi-Stakeholder-Verfahren**. Einbringen konnten sich Anbieter, Branchenverbände, die Wissenschaft und Zivilgesellschaft.
- Die endgültige Fassung sollte nach Art. 56 Abs. 9 AI Act bis zum **2.5.2025** vorliegen und konkrete Ziele, Maßnahmen und Leistungsindikatoren enthalten. Sie wurde schließlich am **10.7.2025** veröffentlicht.
- Besonders umkämpft war, in welchem Maß Anbieter **Informationen über ihre Trainingsdaten und -prozesse offenlegen müssen**.

AI ACT GPAI

- Der **Praxisleitfaden ist rechtlich nicht bindend.** Die Befolgung begründet aber – ähnlich den harmonisierten Normen – den **Anschein der Konformität**.
- Das AI Office ersucht die Anbieter, den Leitfaden zu befolgen. Als zusätzlicher **Anreiz** greift eine **Schonfrist**: Anbieter, die den Leitfaden unterzeichnen, erfahren im ersten Jahr keine Sanktionierung bei Verstößen gegen den AI Act.
- Besonders umkämpft war, in welchem Maß Anbieter **Informationen über ihre Trainingsdaten und -prozesse offenlegen müssen**.

AI ACT GPAI

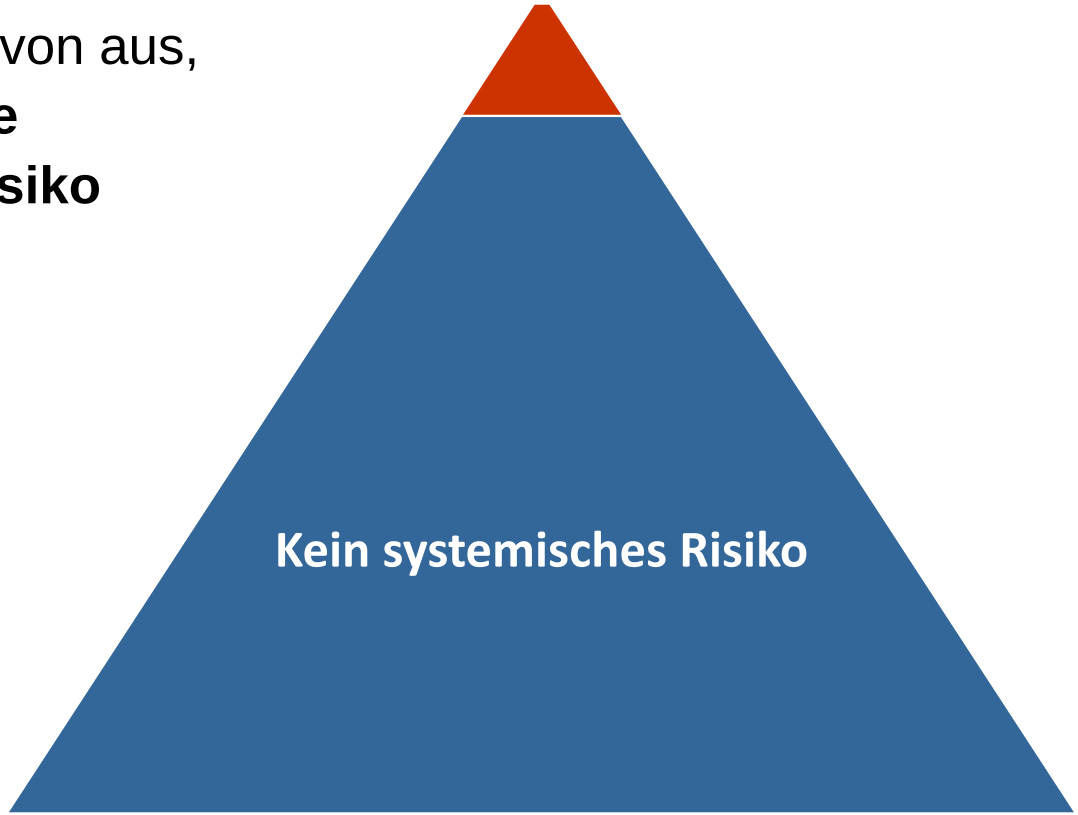
- Inhaltlich **soll** der Praxisleitfaden den **Anbietern von GPAI-Modellen** – mit und ohne systemisches Risiko – eine konkrete Orientierung bei der Auslegung ihrer Pflichten geben.
- Der Leitfaden gliedert sich hierzu in drei Kapitel:
  - **Transparenz**
  - **Urheberrecht**
  - **Sicherheit** (= Gefahrenabwehr)

AI ACT GPAI

- Im Kapitel **Transparenz** nimmt der Leitfaden zu einem großen Streitthema Stellung, der Pflicht der Anbieter, ihre Trainingsdaten und -prozesse offenzulegen.
- Der **Leitfaden differenziert**: Einige **Informationen** sind auch **für Betreiber** bestimmt, die GPAI-Modelle in ihre KI-Systeme integrieren. Andere, sensiblere Informationen wiederum müssen Anbieter nur gegenüber dem AI Office und nationalen Behörden offenlegen.
  - Betreiber haben das Recht auf Information, wie **Trainingsdaten gesammelt** wurden (Crawling, Lizensierung, Synthetisierung) und validiert wurden.
  - Den Behörden gegenüber sind auch die **Kernelemente des Modells** offenzulegen (inkl. Biases).

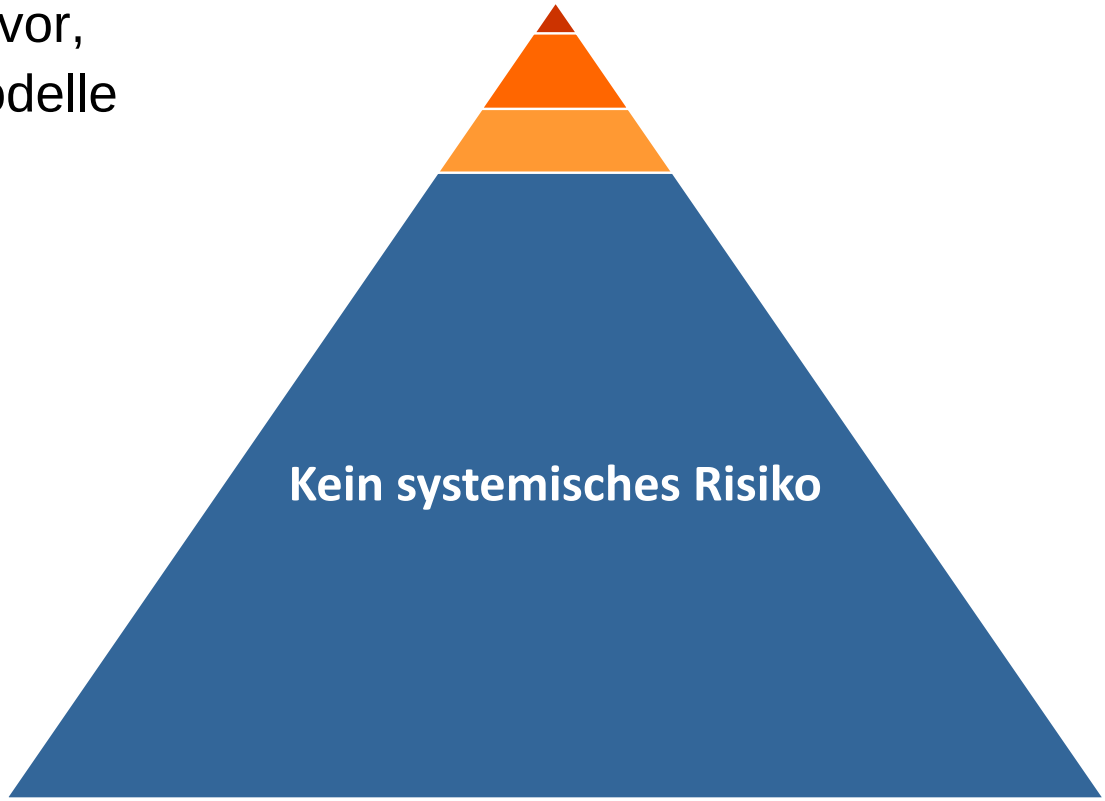
AI ACT GPAI

- Der Praxisleitfaden geht dabei davon aus, dass **derzeit nur wenige Modelle überhaupt ein systemisches Risiko aufweisen**.



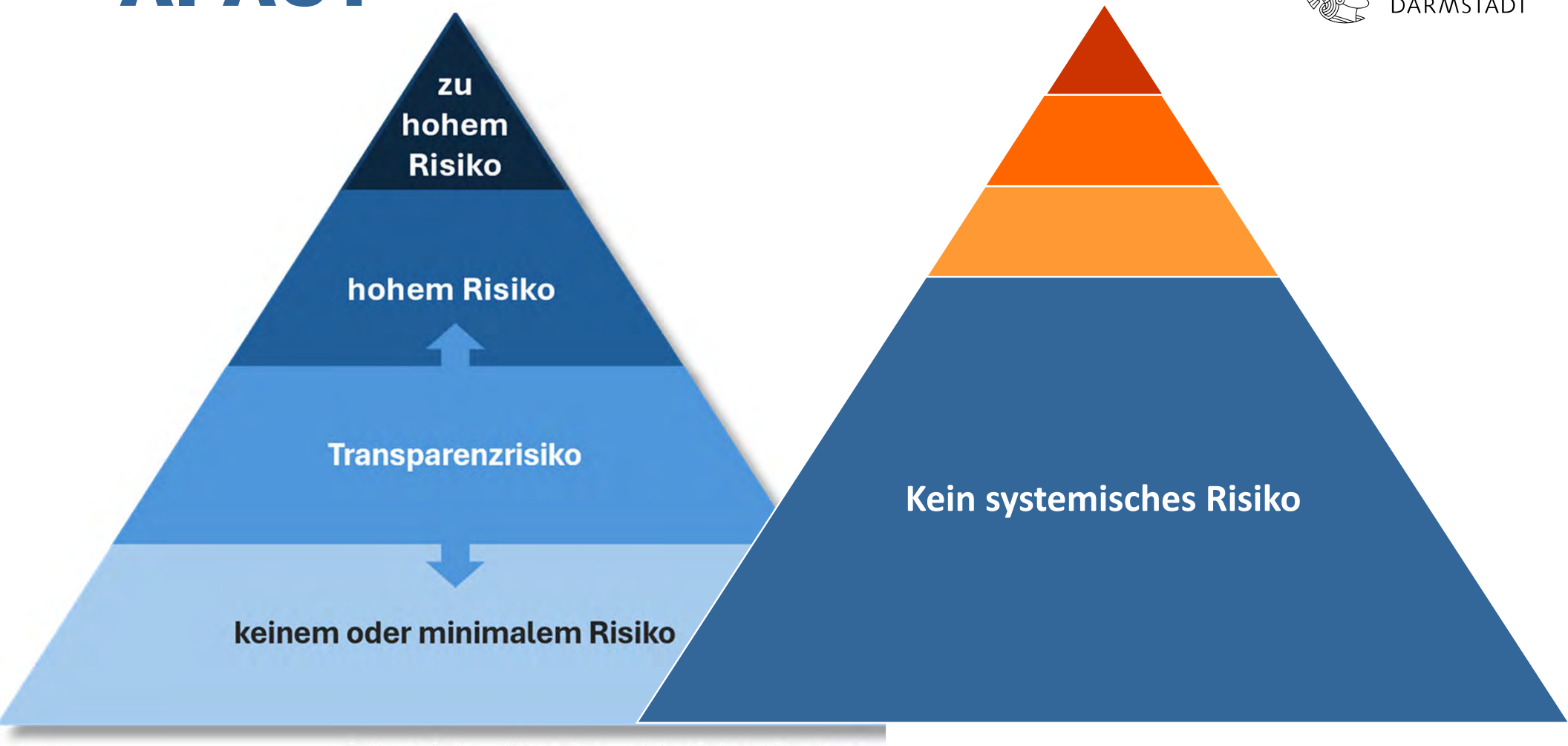
AI ACT GPAI

- Er sieht ein **abgestuftes System** vor, dass manche Maßnahmen auf Modelle beschränkt, die ein spezifisches systemisches Risiko aufweisen.



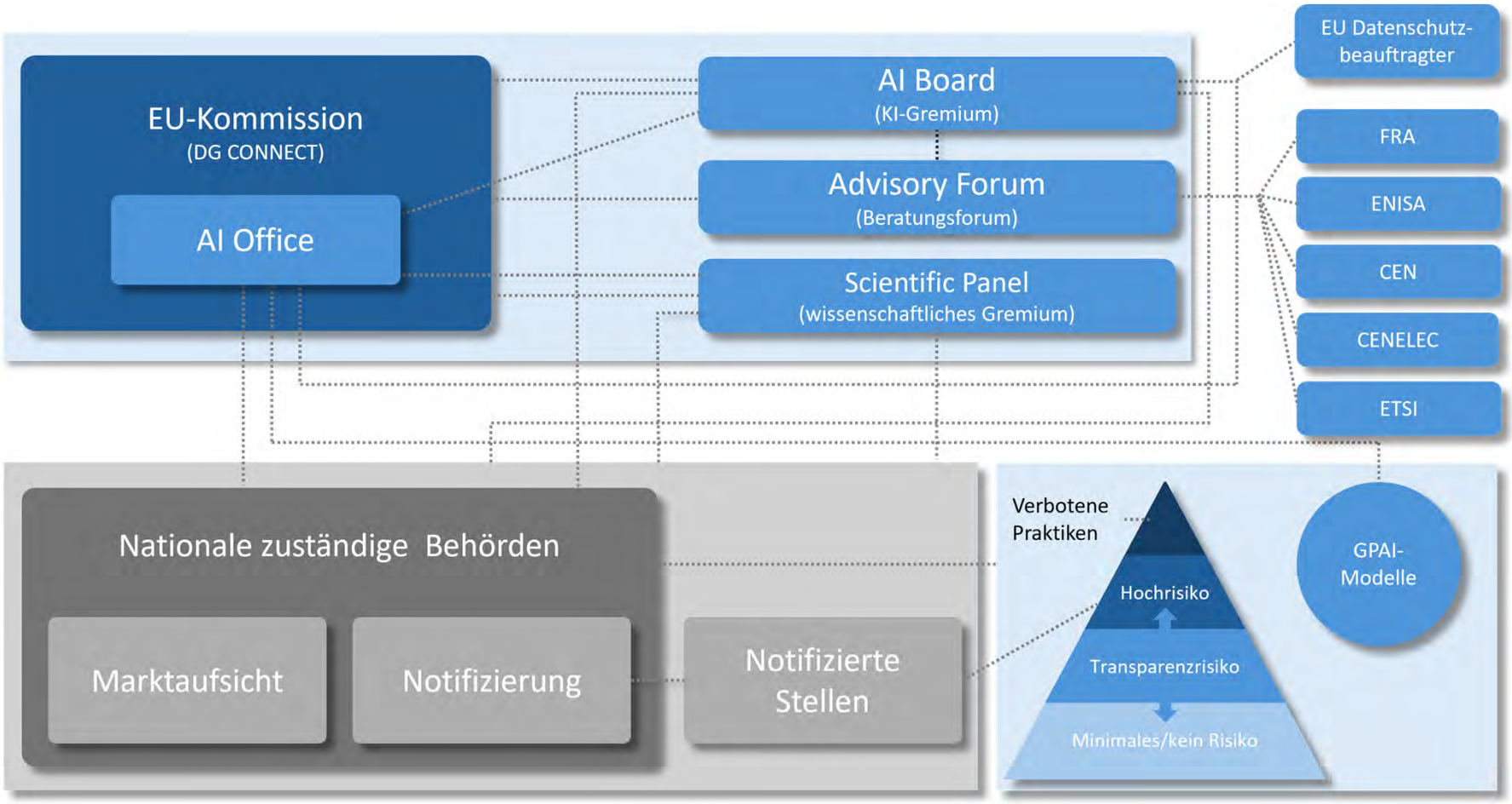
AI ACT

TECHNISCHE UNIVERSITÄT DARMSTADT



AI ACT Aufsichtssystem

TECHNISCHE UNIVERSITÄT DARMSTADT



TECHNISCHE UNIVERSITÄT DARMSTADT

1. Aug. 2024
Inkrafttreten

2. Febr. 2025
Geltungsbeginn der verbotenen Praktiken und der KI-Kompetenz

Febr. 2025
Veröffentlichung der ersten Leitlinien, zu verbotenen Praktiken und der Definition KI-System

Juli 2025
Veröffentlichung des Praxisleitfadens für GPAI

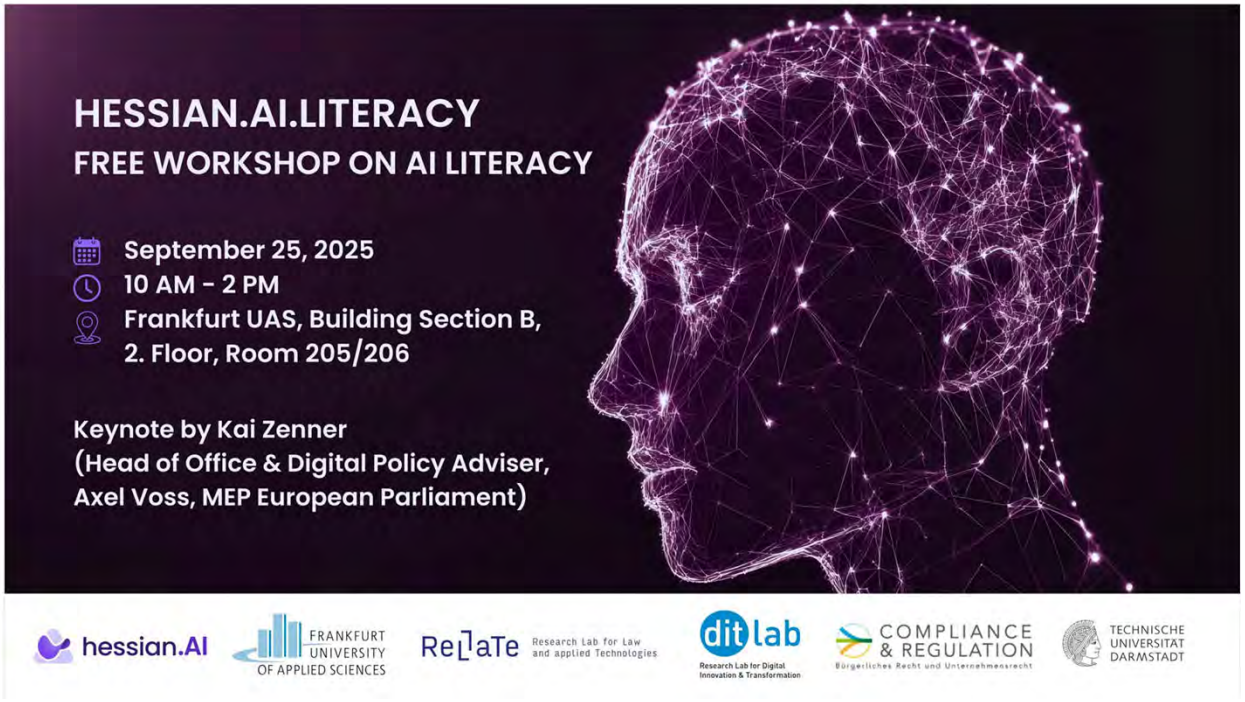
2. Aug. 2025
Geltungsbeginn der Regelungen für GPAI

Aug. 2025
Bekanntgabe der nationalen Aufsichtsstruktur inkl. Personalplanung;
KIMÜG-Entwurf

2. Febr. 2026
Geltungsbeginn des Hauptteils des AI Acts, insb. Hochrisiko gem. Anhang III

2. Febr. 2027
Geltungsbeginn der Regeln des AI Acts, Hochrisiko gem. Anhang I

TECHNISCHE UNIVERSITÄT DARMSTADT



VIELEN DANK!

TECHNISCHE UNIVERSITÄT DARMSTADT

Weiterführende Literatur