DEEP DIVE

DIGITAL LEGAL ACADEMY 2025

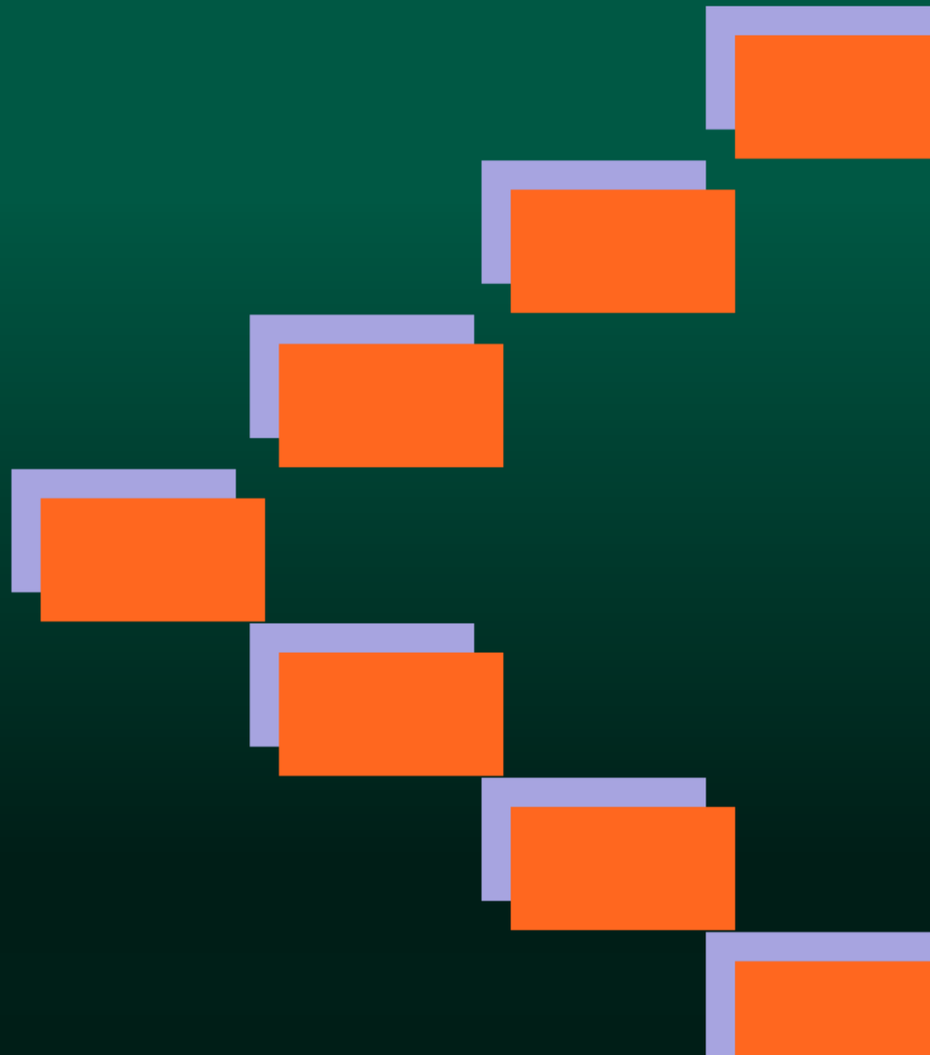
by TaylorWessing

GPAI-Start 2. August 2025: Leitlinien und Praxisleitfäden

8. Juli 2025 | Dr. Christian Frank

Agenda

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing



Wie sind wir hier gelandet?

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

AI-Act (VO (EU) 2024/1689 vom 13. Juni 2024, Amtsblatt 12. Juli 2024

Inkrafttreten und Geltungsbeginn – Art. 113

AI-Act tritt in Kraft

Bestimmungen für KI-Modelle mit allgemeinem Verwendungszweck („GPAI-Modell“) sind anwendbar

1.8.2024 | **2.2.2025** | **2.8.2025**

Regeln zu verbotenen Praktiken treten in Kraft

Zuvor sollten Praxisleitfäden bis zum 2.5.2025 vorliegen (Art. 56 (9))

Genereller Geltungsbeginn

2.8.2026 | **2.8.2027**

Klassifikationsregeln Hochrisiko-Systeme (Art. 6 (1)) + entsprechende Pflichten treten in Kraft

Wie sind wir hier gelandet?

DEEP DIVE
DIGITALLEGAL ACADEMY 2025
by TaylorWessing

AI-Act (VO (EU) 2024/1689 vom 13. Juni 2024, Amtsblatt 12. Juli 2024

Kapitel V	**GPAI-Modelle**
Art. 51	Einstufung mit/ohne „systemisches Risiko“
Art. 52	Verfahren
Art. 53	Pflichten für Anbieter von GPAI-Modellen
Art. 54	Bevollmächtige der Anbieter von GPAI-Modellen
Art. 55	Pflichten für Anbieter von GPAI-Modellen mit systemischem Risiko
Art. 56	**Praxisleitfäden**
Art. 96	**Leitlinien Kommission**

Art. 56 – Praxisleitfäden – Was soll drin sein?

DEEP DIVE
DIGITALLEGAL ACADEMY 2025
by TaylorWessing

(2) AI-Office und AI-Board *streben an sicherzustellen, dass Praxisleitfäden mind. die in den Art. 53 und 55 vorgesehenen Pflichten abdecken, einschließlich der folgenden Aspekte:*

a) Mittel zur Sicherstellung, dass Informationen gem. Art. 53 (1) a) und b) hins. Entwicklungen Markt und Technik auf neuesten Stand gehalten werden;

b) angemessene Detailgenauigkeit bei der Zusammenfassung der für das Training verwendeten Inhalte;

c) Ermittlung von Art und Wesen der systemischen Risiken auf Unionsebene, ggf. inkl. Ursachen;

d) Maßnahmen, Verfahren + Modalitäten für Bewertung + Management systemischer Risiken (inkl. Dokumentation)
- in angemessenem Verhältnis zu Risiken,
- berücksichtigt Schwere, Wahrscheinlichkeit +
- spezifische Herausforderungen bei Bewältigung entlang der KI-Wertschöpfungskette.

Art. 96 – Leitlinien – Was soll drin sein?

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

(1) Kommission erarbeitet Leitlinien für die praktische Umsetzung dieser Verordnung, die sich insb. auf Folgendes beziehen:

a) die Anwendung der in den Art. 8 bis 15 und in Art. 25 genannten Anforderungen und Pflichten;

b) die in Art. 5 genannten verbotenen Praktiken;

c) die praktische Durchführung der Bestimmungen über wesentliche Veränderungen;

d) die praktische Umsetzung der Transparenzpflichten gemäß Art. 50;

e) detaillierte Informationen über das Verhältnis dieser Verordnung zu den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union sowie zu anderen einschlägigen Rechtsvorschriften der Union, auch in Bezug auf deren kohärente Durchsetzung;

f) die Anwendung der Definition eines KI-Systems gemäß Art. 3 Nr 1.

Art. 96 – Leitlinien – Was soll drin sein?

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

(1) Kommission erarbeitet Leitlinien für die praktische Umsetzung dieser Verordnung, die sich insb. auf Folgendes beziehen:

a) die Anwendung der in den Art. 8 bis 15 und in Art. 25 genannten Anforderungen und Pflichten;

b) die in Art. 5 genannte verbotenen Praktiken;

4.2.2025

c) die praktische Durchführung der Bestimmungen über wesentliche Veränderungen;

d) die praktische Umsetzung der Transparenzpflichten gemäß Art. 50;

e) detaillierte Informationen über das Verhältnis dieser Verordnung zu den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union sowie zu anderen einschlägigen Rechtsvorschriften der Union, auch in Bezug auf deren kohärente Durchsetzung;

f) die Anwendung der Definition eines KI-Systems gemäß Art. 3 Nr 1.

6.2.2025

Art. 96 – Leitlinien – Was soll drin sein?

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

(1) Kommission erarbeitet Leitlinien für die praktische Umsetzung dieser Verordnung, die sich insb. auf Folgendes beziehen:

4.2.2025

a) die Anwendung der in den Art. 8 bis 15 und in Art. 25 genannten Anforderungen und Pflichten;

b) die in Art. 5 genannte verbotenen Praktiken;

c) die praktische Durchführung der Bestimmungen über wesentliche Veränderungen;

d) die praktische Umsetzung der Transparenzpflichten gemäß Art. 50;

e) detaillierte Informationen über das Verhältnis dieser Verordnung zu den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union sowie zu anderen einschlägigen Rechtsvorschriften der Union, auch in Bezug auf deren kohärente Durchsetzung;

f) die Anwendung der Definition eines KI-Systems gemäß Art. 3 Nr 1.

6.2.2025

– aber ohne Abgrenzung AI-System vs GPAI-Modell – Ziffer III Rdn 64

Art. 56 – Timeline

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

30.9.2024
Praxisleitfäden Kick-off Event mit 1.000 Teilnehmern
Vier Arbeitsgruppen
- Transparenz & Urheberrecht
- Risikoidentifikation & Bewertung inkl. Evaluierung
- Technische Risikominderung
- Internes Risikomanagement & Governance von GPAI-Anbietern

14.11./ 19.12.2024
Veröffentlichung 1. / 2. Entwurf

11.3.2025
Veröffentlichung 3. Entwurf

22.4.2025
AI-Office startet Konsultation / Beteiligungsverfahren Art. 56 (3) -> Beiträge zur Präzisierung von Vorschriften

30.6.2025
Treffen AI-Board (Art. 65)

2.7.2025
Workshop GPAI-Anbieter

3.7.2025
Gemeinsame Abschluß-veranstaltung

Veröffentlichung Leitlinien und Praxisleitfäden in den kommenden Tagen?

Art. 56 – Praxisleitfäden Segelanweisung

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

AI-Office und AI-Board

- ***„streben an**, sicherzustellen, dass in Praxisleitfäden spezifische Ziele eindeutig festgelegt sind und Verpflichtungen oder Maßnahmen … enthalten, um Verwirklichung dieser Ziele gewährleisten, und dass sie Bedürfnissen und Interessen aller interessierten Kreise, inkl. betroffener Personen … gebührend Rechnung tragen“* (Abs. 4)
- ***„bewerten**, ob Praxisleitfäden die in Art. 53 und 55 vorgesehenen Pflichten abdecken + überwachen und bewerten … Verwirklichung von deren Zielen durch Beteiligte und deren Beitrag zur ordnungsgemäßen Anwendung. Sie veröffentlichen ihre Bewertung der Angemessenheit der Praxisleitfäden“* (Abs. 6)

AI-Office

- ***kann** alle Anbieter von GPAI-Modellen **ersuchen**, die Praxisleitfäden zu befolgen. Für Anbieter von GPAI-Modellen ohne systemische Risiken kann Befolgung Art. 53er Pflichten beschränkt werden* (Abs. 3)

Kann bis zum 2.8.2025 ein Praxisleitfaden nicht fertiggestellt werden oder erachtet das AI-Office diesen nach seiner Bewertung gem. Abs. 6 für nicht angemessen, kann die Kommission im Wege von Durchführungsrechtsakten gemeinsame Vorschriften für die Umsetzung der in den Artikeln 53 und 55 vorgesehenen Pflichten, einschließlich der in Abs. 2 des vorliegenden Artikels genannten Aspekte, festlegen.

Art. 53 – allg. Anbieterpflichten

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

➔ **An AI-Office**

a) Technische Dokumentation des Modells erstellen + aktualisieren Informationen (Trainings- und Testverfahrens + Ergebnisse seiner Bewertung)

➔ **AI-System-Anbieter**

b) Informationen/Dokumentation, damit diese Fähigkeiten + Grenzen GPAI-Modell gut verstehen und ihren Pflichten gemäß dieser Verordnung nachzukommen können

AUSN zu a) / b): OS-GPAI Modelle (außer system. Risiko) - Abs. 2

➔ **Urheberrecht**

c) Bringen Strategie zur Einhaltung des Urheberrechts und insbesondere zur Ermittlung und Einhaltung eines Rechtevorbehalts gem. Art. 4 (3) der Richtlinie (EU) 2019/790 geltend gemachten Rechtsvorbehalts, auch durch modernste Technologien, auf den Weg;

d) Erstellen + veröffentlichen hinreichend detaillierte Zusammenfassung der für das Training des GPAI-Modells verwendeten Inhalte nach einer vom AI-Office bereit-gestellten Vorlage

Anbieter von GPAI-Modellen können sich zunächst auf Praxisleitfäden iSd Art. 56 stützen, um Einhaltung der Pflichten aus Art. 53 (1) nachzu-weisen. (Abs. 4)

Art. 55 – Pflichten Anbieter systemische Risiken

DEEP DIVE
DIGITALLEGAL ACADEMY 2025
by TaylorWessing

a) Modellbewertung mit standardisierten Protokollen und Instrumenten durchführen, die dem Stand der Technik entsprechen, wozu auch die Durchführung und Dokumentation von Angriffstests beim Modell gehören, um systemische Risiken zu ermitteln und zu mindern;

b) Bewertung möglicher systemische Risiken auf Unionsebene – inkl. Ursachen – , die sich aus Entwicklung, Inverkehrbringen oder Verwendung von GPAI-Modellen systemischem Risiko ergeben können;

c) Erfassung und Dokumentation einschlägiger Informationen über schwerwiegende Vorfälle und mögliche Abhilfemaßnahmen + AI-Office + zuständige nationale Behörden unverzüglich darüber unterrichten;

d) angemessenes Maß an Cybersicherheit für GPAI-Modelle mit systemischem Risiko und für physische Infrastruktur des Modells gewährleisten.

Anbieter von GPAI-Modellen können sich zunächst auf Praxisleitfäden iSd Art. 56 stützen, um Einhaltung der Pflichten aus Art. 53 (1) nachzuweisen. (Abs. 4)

Protokoll – Leitlinienthemen

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Hauptkritikpunkte der Stakeholder

1. Schwellenwert für GPAI-Modelle

- Anbieter, Industrievertreter und Behörden:
  Bisheriger Schwellenwert von 10^{22} FLOP zu *niedrig*:
  - Vorschlag: Anhebung auf 10^{23} FLOP, was typischen heutigen Modellen mit ca. 1 Milliarde Parametern entspricht (vgl. Erwägungsgrund 98)
- Urheberrechtsinhaber:
  Bisheriger Schwellenwert von 10^{22} FLOP zu *hoch*, zudem zusätzliche Kriterien nötig.

2. Open-Source-Ausnahme und Monetarisierung

- Anbieter, Industrie und Wissenschaft wollen Klarstellungen:
  - Wann gilt die Open-Source-Ausnahme?
  - Was zählt als Monetarisierung?
- Vorschläge Stakeholder:
  - Präzisierung Voraussetzungen für Ausnahme.
  - Konkrete Beispiele für Monetarisierung im Kontext GPAI.

3. Rolle von Downstream-Modifikatoren

- Downstream-Modifizierer (Feinjustierung, Optimierung Effizienz, Systemintegration) wollen nicht als Anbieter im Sinne des AI-Acts qualifiziert werden
- Vorschlag: Nur Anbieter, wenn Modifikationen > 1/3 des ursprünglichen Trainings-Rechenleistung beanspruchen.
- Ziel: Die meisten, insb. kleinere Modifizierer sollen nicht unter die Anbieterpflichten fallen

Protokoll – Leitlinienthemen

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Hauptkritikpunkte der Stakeholder

1. **Schwellenwert für GPAI-Modelle**

   - Anbieter, Industrievertreter und Behörden:
     Bisheriger Schwellenwert von 10^{22} FLOP zu *niedrig*:
     - Vorschlag: Anhebung auf 10^{23} FLOP, was typischen heutigen Modellen mit ca. 1 Milliarde Parametern entspricht (vgl. Erwägungsgrund 98)
   - Urheberrechtsinhaber:
     Bisheriger Schwellenwert von 10^{22} FLOP zu *hoch*, zudem zusätzliche Kriterien nötig.

Schwellenwert steht NICHT im AI-Act selber (ErwG 98 tanzt herum)
AI-Office 22.4.2025 – Bedingungen für ausreichende Allgemeinheit und Fähigkeiten, Ziffer 3.1.1:

- Modell, das Text/ Bilder generieren kann + Trainingsrechenleistung > 10^{22} FLOP: Widerlegbare Vermutung = GPAI-Modell;
- Ohne Text/Bilder möglich, so vergleichbar breiter Verwendungszweck
- < 10^{22} FLOP: Widerbare Vermutung zu enger Verwendungszweck

   - Was zählt als Monetarisierung?
   - Vorschläge Stakeholder:
     - Präzisierung Voraussetzungen für Ausnahme.
     - Konkrete Beispiele für Monetarisierung im Kontext GPAI.

   - Vorschlag: Nur Anbieter, wenn Modifikationen > 1/3 des ursprünglichen Trainings-Rechenleistung beanspruchen.
   - Ziel: Die meisten, insb. kleinere Modifizierer sollen nicht unter die Anbieterpflichten fallen

Protokoll – Leitlinienthemen

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Hauptkritikpunkte der Stakeholder

2. **Open-Source-Ausnahme und Monetarisierung**
   - Anbieter, Industrie und Wissenschaft wollen Klarstellungen:
     - Wann gilt die Open-Source-Ausnahme?
     - Was zählt als Monetarisierung?
   - Vorschläge Stakeholder:
     - Präzisierung Voraussetzungen für Ausnahme.
     - Konkrete Beispiele für Monetarisierung im Kontext GPAI.

AI-Office Ziffer 3.3.2: Drei Kriterien für OS-Ausnahme

1. GPAI-Modell wird in kostenloser OS-Lizenz bereitgestellt, die Zugriff, Nutzung, Änderung und Verbreitung erlaubt: dezidierte Bezugnahme auf ErwG 102, 103.
2. Parameter, inkl. Gewichtung, Informationen zur Modellarchitektur und zur Modellnutzung, müssen werden öffentlich zugänglich gemacht
3. Kein systemisches Risiko

werden

- Vorschlag: Nur Anbieter, wenn Modifikationen > 1/3 des ursprünglichen Trainings-Rechenleistung beanspruchen.
- Ziel: Die meisten, insb. kleinere Modifizierer sollen nicht unter die Anbieterpflichten fallen

Protokoll – Leitlinienthemen

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Hauptkritikpunkte der Stakeholder

3. **Rolle von Downstream-Modifikatoren**

   - Downstream-Modifizierer (Feinjustierung, Optimierung Effizienz, Systemintegration) wollen nicht als Anbieter im Sinne des AI-Acts qualifiziert werden
   - Vorschlag: Nur Anbieter, wenn Modifikationen > 1/3 des ursprünglichen Trainings-Rechenleistung beanspruchen.
   - Ziel: Die meisten, insb. kleinere Modifizierer sollen nicht unter die Anbieterpflichten fallen

AI-Office 3.2.2 Downstream Modifikatoren als GPAI-Modell-Anbieter:

A entwickelt GPAI-Modell, B modifiziert und bringt es auf den Markt:

- A = Anbieter urspr. Modell, muss Pflichten GPAI-Anbieter erfüllen,
- B = Anbieter geänd. Modell, muss Pflichten GPAI-Anbieter erfüllen, es sei denn Änderung entfernt GP-Natur

ErwG 97, 109 + nur *signifikante* Änderungen lösen Qualifikation aus

- > Schwellenwert:

Vermutung DM = GPAI-Modell-Anbieter, so für Änderung verwendete Trainings-rechenleistung > 1/3 Schwellenwert Trainingsrechenleistung des urspr. Modells

Ähnlicher Ansatz GPAI-Modell mit system. Risiko:

- Reine Änderung: > 1/3
- Risikoerhöhende Änderung: ∑ Schwellenwert Ersterstellung + Schwellenwert Änderung > Art. 51(2) Schwellenwert

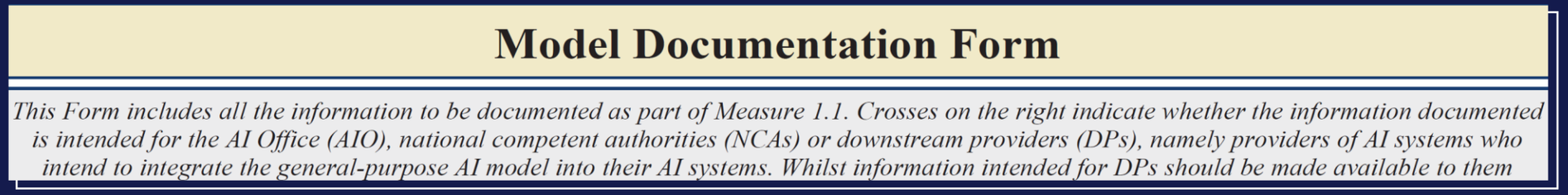
Protokoll Transparenzpflichten – Praxisleitfaden

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

1. **Modell-Dokumentation erstellen & pflegen**
   - Erstellung und Aktualisierung der Modell Dokumentation
   - Verwendung des offiziellen Templates
   - Aufbewahrungspflicht für 10 Jahre nach Vermarktungsende
   - Nachvollziehbar, versioniert, überprüfbar

2. **Relevante Informationen bereitstellen**
   - Kontaktstelle für Behörden und Downstream-Anbieter
   - Bereitstellung auf Anfrage (AI-Office, nationale Behörden)
   - Offenlegung relevanter zusätzlicher Informationen
   - Wahrung von IP-Schutz und Vertraulichkeit (gemäß Art. 78 AI-Act)

3. **Qualität, Integrität & Sicherheit**
   - Sicherstellung von Qualität und Konsistenz der Informationen
   - Schutz vor unbeabsichtigten Änderungen (z.B. durch Versionierung)
   - Orientierung an anerkannten Sicherheitsstandards und Protokollen



Model Documentation Form

This Form includes all the information to be documented as part of Measure 1.1. Crosses on the right indicate whether the information documented is intended for the AI Office (AIO), national competent authorities (NCAs) or downstream providers (DPs), namely providers of AI systems who intend to integrate the general-purpose AI model into their AI systems. Whilst information intended for DPs should be made available to them

Protokoll Transparenzpflichten – Praxisleitfaden

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

1. Modell-Dokumentation erstellen & pflegen
2. Relevante Informationen bereitstellen
3. Qualität, Integrität & Sicherheit
   - Sicherstellung von Qualität und

Main Points of stakeholder feedback addressed and what we preserved

Modelldokumentation	Ausfüllen offiziellen Model Dokumentation Form ist nicht mehr verpflichtend, solange entspr. Informationen an anderer Stelle ausreichend dokumentiert sind.
Informationen für Downstream-Anbieter	Klarstellung, welche Zusatzinformationen Downstream-Anbieter gemäß Art. 53(1)(b) anfordern dürfen.
Schutz vertraulicher Informationen	Leitfaden berücksichtigt nun alle Vorschriften des AI-Acts zum Schutz von Geschäfts-geheimnissen und vertraulichen Informationen
Abgleich mit Trainingsdaten-Template	Kategorien zur Herkunft von Trainingsdaten wurden mit dem bald erscheinenden Template für die Trainingsdatendokumentation abgestimmt.
Angaben überabeitet	Änderungen Angaben „Modellabhängigkeiten“, „Verbreitungsmethoden“, „Lizenzen“, um sicherzustellen, dass abgefragte Informationen ihren Zweck erfüllen
Energieverbrauch	So Energieverbrauch während Trainings nicht abschätzbar, dürfen Anbieter dies angeben – mit Erläuterung, welche Informationen fehlen, um Schätzung zu ermöglichen

This Form includes all the information to be documented as part of Measure 1.1. Crosses on the right indicate whether the information documented is intended for the AI Office (AIO), national competent authorities (NCAs) or downstream providers (DPs), namely providers of AI systems who intend to integrate the general-purpose AI model into their AI systems. Whilst information intended for DPs should be made available to them

Protokoll Pflichten Urheberrecht – Praxisleitfaden

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Policy erstellen & umsetzen

- Policy mit allen Verpflichtungen
- Interne Verantwortlichkeiten
- Veröffentlichung einer Kurzfassung empfohlen

Bei Web-Crawling: Nur rechtmäßig zugängliche Inhalte crawlen

- Keine Umgehung technischer Schutzmaßnahmen (Paywalls etc.)
- Reasonable efforts („RE“) zum Ausschluss von „Piraterie-Domains“

Rechtevorbehalte beim Web-Crawling beachten

- Beachtung von robots.txt (RFC 9309), „best efforts“ zu anderen Protokollen
- Andere Vorbehaltserklärung unberührt
- Veröffentlichung von Infos zu Crawlern (RE) um Veröffentlichung von, Suchmaschine

Wenn kein eigenes Web-Crawling:

- Prüfung auf rechtskonformes Crawling durch Dritte
- Keine Verpflichtung zu individuellem Rechtecheck

Risiko verletzender Outputs mindern

- RE dagegen, dass Modell urheberrl. geschützte Inhalte „einbrennt“ + wiederholt ausgibt
- Verbot in AGB
- Gilt nicht für Open Source Modelle

Rechteinhaber-Beschwerden ermöglichen

- Kontaktstelle
- Online-Beschwerdesystem
- Ablehnung bei offensichtlich unbegründeten / exzessiven Beschwerden möglich

Protokoll Pflichten Urheberrecht – Praxisleitfaden

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Policy erstellen & umsetzen

- Policy mit allen Verpflichtungen

Bei Web-Crawling: Nur rechtmäßig zugängliche Inhalte crawlen

Rechtevorbehalte beim Web-Crawling beachten

Main Points of stakeholder feedback addressed and what we preserved

Verhältnis zum Urheberrecht	Weitere Klarstellungen zum Zusammenspiel Leitfaden vs. EU-Urheberrecht; explizite Bezugnahme auf urheberrechtliche Grundprinzipien der EU
Verhältnis zur Unternehmensgröße	Präambel klärt: Einhaltung Best-Effort-Verpflichtungen soll verhältnismäßig zur Unternehmensgröße sein
Technische & rechtliche Umsetzbarkeit	Verweis auf künftiges IETF-Protokoll zu robots.txt Fokus auf „Einbrennen “ (Reproduktion geschützter Inhalte durch Modell) neu bewertet Maßnahme zu Drittanbieter-Datensätzen wird überarbeitet
Verpflichtungen stärken	Bestimmte Pflichten wurden gestärkt, um besser an bestehendes Recht angepasst zu sein Klarstellung zum Umgang mit Beschwerden von Rechteinhaber

- Crawling durch Dritte
- Keine Verpflichtung zu individuellem Rechtecheck

- geschützte Inhalte “einbrennt“ + wiederholt ausgibt
- Verbot in AGB
- Gilt nicht für Open Source Modelle

- Kontaktstelle
- Online-Beschwerdesystem
- Ablehnung bei offensichtlich unbegründeten / exzessiven Beschwerden möglich

Protokoll GPAI mit systemischem Risiko – Praxisleitfaden

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

(1) Safety and Security Framework

1. Safety and Security Governance Framework
   Aufbau eines strukturierten Governance-Frameworks für Sicherheitsprozesse im gesamten Lebenszyklus.
2. Risk Tiers Definition
   Definition von verschiedenen Risikostufen (Tiers) zur systematischen Einordnung.
3. Risk Forecasting
   Prognose zukünftiger Entwicklungen bzgl. sicherheits-relevanter Risiken auf Basis aktueller Forschung.

(2) Bewertung systemischer Risiken

4. Lifecycle Risk Assessment
   Durchführung einer Risikoanalyse über den gesamten Modelllebenszyklus hinweg.
5. Capability Discovery
   Analyse und Dokumentation von emergenten oder besonders leistungsfähigen Fähigkeiten.
6. Risk Monitoring
   Kontinuierliche Überwachung möglicher Sicherheitsvorfälle, Missbrauch und ungewollter Effekte.
7. Incident Reporting
   Etablierung eines Prozesses zur internen und ggf. externen Meldung sicherheitsrelevanter Zwischenfälle.

Protokoll GPAI mit systemischem Risiko – Praxisleitfaden

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

(3) Minderung systemischer Risiken

8. Red-Teaming
   Interne und externe Red-Teaming-Maßnahmen zur Erkennung von Schwachstellen.
9. Third Party Testing & Audits
   Durchführung unabhängiger Prüfungen sicherheitsrelevanter Funktionen.
10. Use Prevention Measures
    Einsatz technischer und organisatorischer Maßnahmen zur Verhinderung missbräuchlicher Nutzung (z.B. API-Limits).
11. Alignment Techniques
    Einsatz von Techniken wie Reinforcement Learning from Human Feedback (RLHF) zur Steuerung des Modellverhaltens.
12. Release Practices
    Risikogerechte Veröffentlichung (z.B. gestaffelte Releases, Closed vs. Open).
13. Emergency Pause & Withdrawal
    Möglichkeit zur sofortigen Deaktivierung oder Rücknahme bei schwerwiegenden Vorfällen.

(4) Model Report & Dokumentation

14. Safety Disclosures
    Offenlegung sicherheitsrelevanter Informationen gegenüber AI-Office, Behörden und ggf. der Öffentlichkeit.
15. Risk Documentation
    Strukturierte Dokumentation aller sicherheitsbezogenen Einschätzungen und Entscheidungen.
16. Risk Management Record Keeping
    Pflicht zur langfristigen Archivierung der Sicherheitsdokumentation und Audit Trails.

Protokoll GPAI mit systemischem Risiko – Praxisleitfaden

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Main Points of stakeholder feedback addressed and what we preserved	
Bewertungsprozess	Klarstellungen und Optimierungen eingearbeitet
Risiko Klassifikation	Offene Risikoidentifizierung verpflichtend
Information zu Bewertungsmethoden	Modellbericht muss mehr Information zu Bewertungsmethoden enthalten, damit AI-Office Qualität Bewertung unabhängig beurteilen kann
Anzahl Verpflichtungen	Redaktionell auf 10 reduziert (gleicher Inhalt, nur optimiert + vereinfacht)
Modellbericht	Vereinfachung des Modellberichts, fokussiert auf Schlüsselinformationen
Safety and Security Framework	Solides Framework, dem aktuellen Stand der Technik entsprechend, optimiert für höhere Klarheit
Sicherheit	Umstellung auf ergebnisorientierte Formulierung der Ziele der Minderung von Sicherheitsrisiken
Referenzen andere Standards	Entfernt; Code nun autark
Berichtsanforderungen	Angepasst an breitere Definition Modell; Berichtspflichten reduziert, Informationen ergänzt umgestellt
Externe Bewertungen	Verpflichtung zu unabhängiger externer Bewertung während Risikobewertung in bestimmten Fällen
Whistle Blower Schutz	Nur Indikator für gesunde Risikokultur
Öffentliche Transparenz	Gestrichen, da AI-Act keine öffentliche Transparenz erfordert
Zuweisung der Verantwortlichkeit für systemische Risiken	Nicht EU-Standards wurden entfernt

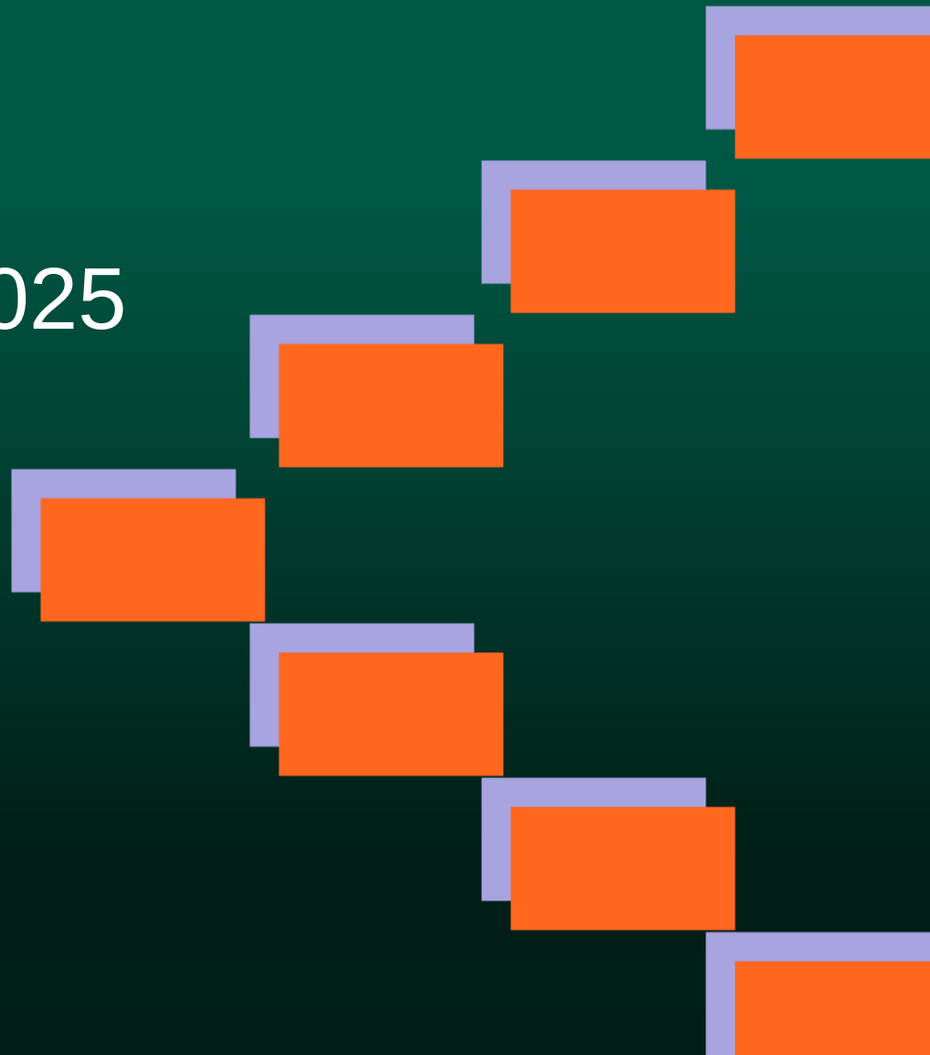
Fazit

DEEP DIVE
DIGITALLEGAL ACADEMY 2025
by TaylorWessing

Ergebnis:

Leitlinien kommen vor 2. August 2025

Praxisleitfaden kommt vor 2. August 2025



Speaker

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Dr. Christian Frank

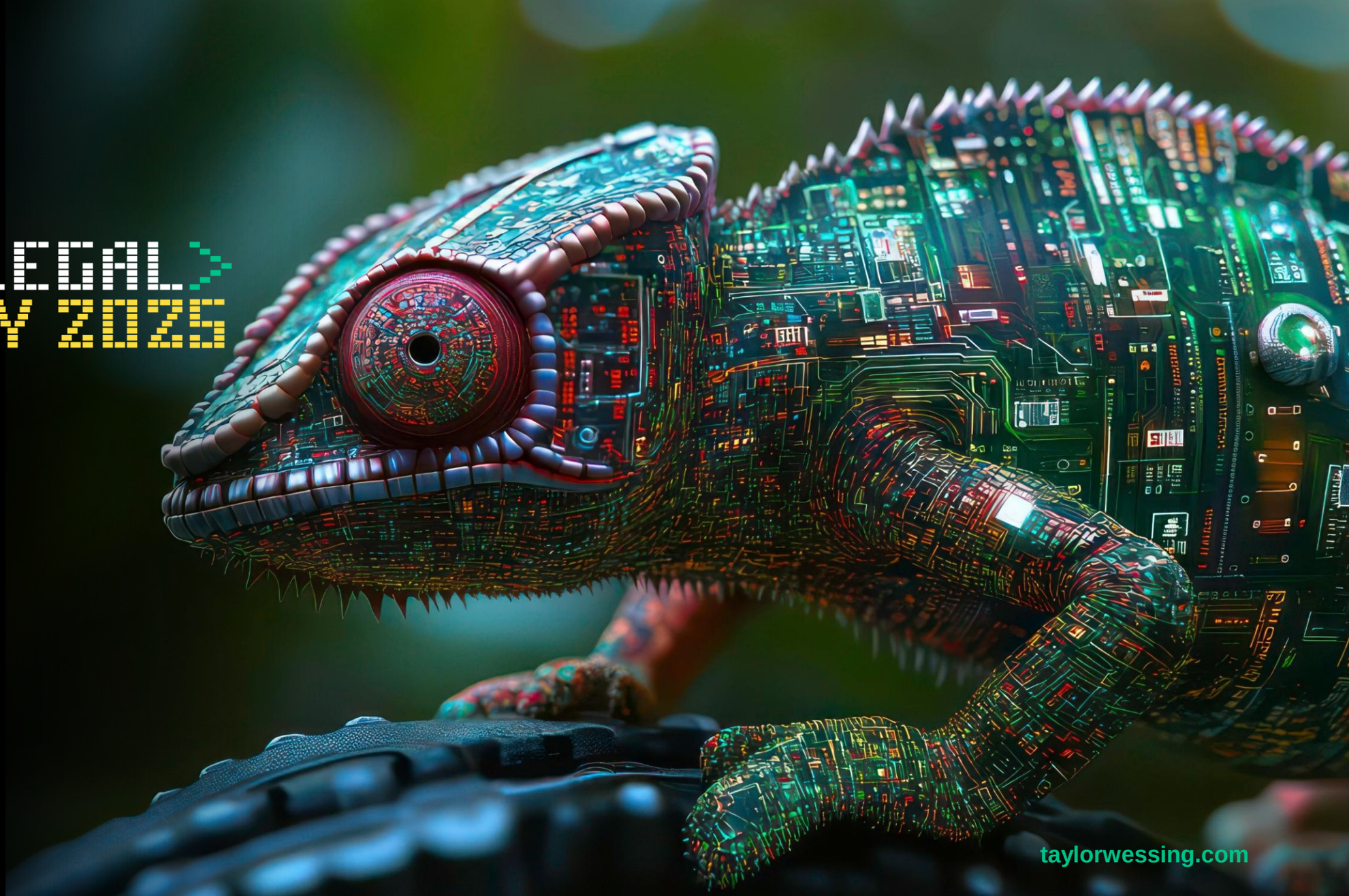
Partner, Taylor Wessing

DEEP DIVE

TaylorWessing

DIGITAL LEGAL ACADEMY 2025

Ready for AI



taylorwessing.com