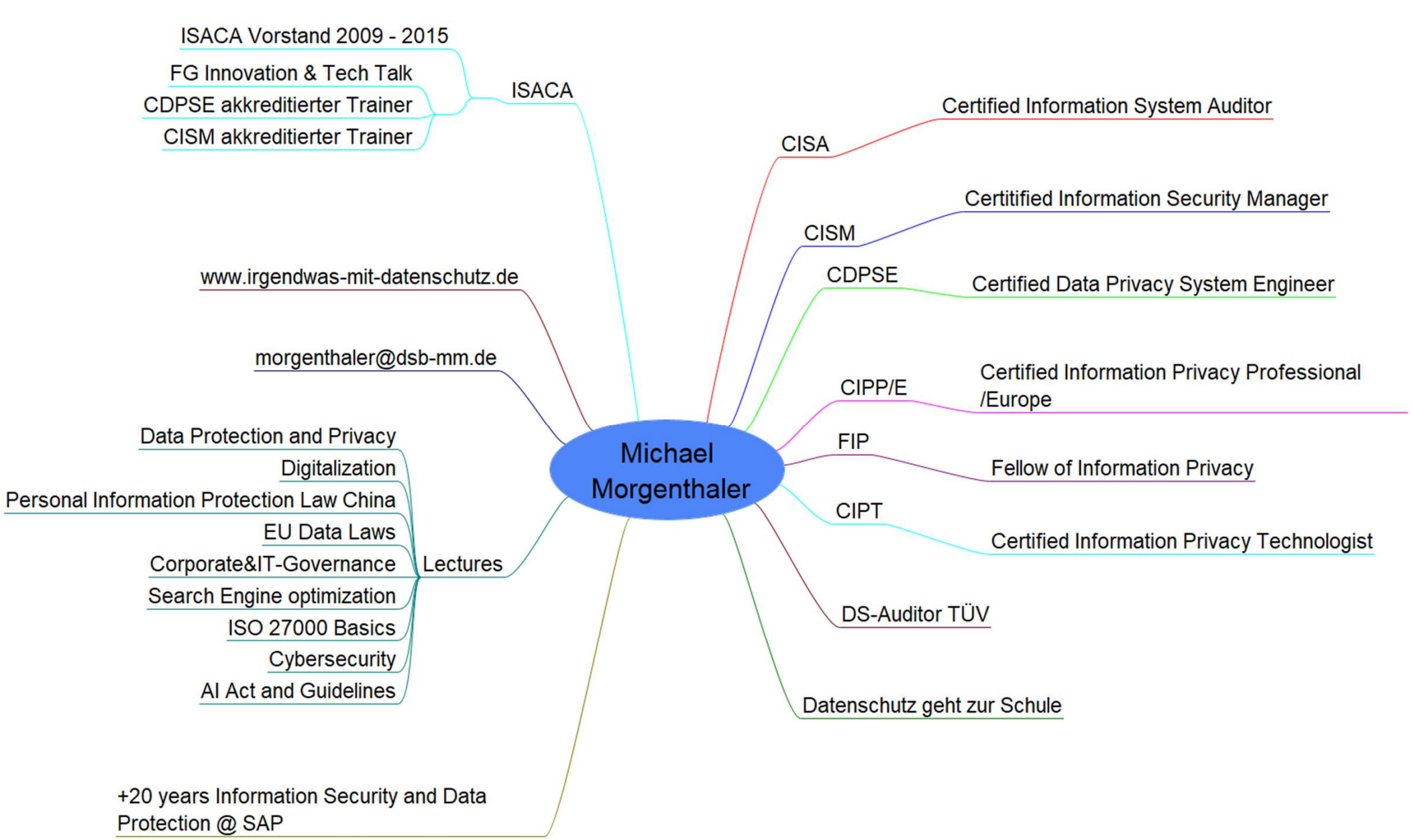
Bildquelle Pixabay – Gerd Altmann

Referent:
Michael Morgenthaler
CISA, CISM, CDPSE, CIPP/E, CIPT, FIP, DS-Auditor (TÜV)


Michael Morgenthaler
ISACA
ISACA Vorstand 2009 - 2015
FG Innovation & Tech Talk
CDPSE akkreditierter Trainer
CISM akkreditierter Trainer
www.irgendwas-mit-datenschutz.de
morgenthaler@dsb-mm.de
Lectures
Data Protection and Privacy
Digitalization
Personal Information Protection Law China
EU Data Laws
Corporate&IT-Governance
Search Engine optimization
ISO 27000 Basics
Cybersecurity
AI Act and Guidelines
+20 years Information Security and Data Protection @ SAP
CISA
Certified Information System Auditor
CISM
Certitified Information Security Manager
CDPSE
Certified Data Privacy System Engineer
CIPP/E
Certified Information Privacy Professional /Europe
FIP
Fellow of Information Privacy
CIPT
Certified Information Privacy Technologist
DS-Auditor TÜV
Datenschutz geht zur Schule

KI-Verordnung (KI-VO / AI-ACT)
=
DSGVO 2.0 ?

KI-Verordnung (KI-VO / AI-ACT)

=

DSGVO 2.0 ?

DSGVO:

schützt Grundrechte und definiert Regeln zur Nutzung Personenbezogener Daten, um den Schutz von Persönlichkeitsrechten zu gewährleisten!

KI-Verordnung:

Produktregulierung, zur Herstellung der Produktkonformität zur Inverkehrbringung im EU-Binnenmarkt

KI Verordnung (aka AI Act)

- Verordnung (EU) 2024/1689 …vom 13. Juni 2024 zur **Festlegung harmonisierter Vorschriften für künstliche Intelligenz** und zur Änderung der Verordnungen ….
- Kurzform: Verordnung über künstliche Intelligenz
- **Artificial Intelligence Act,** laying down harmonised rules on artificial intelligence
- Erster Entwurf: 2019
- Datum des Rechtsakts: 13. Juni 2024
- Veröffentlichungsdatum: 12. Juli 2024
- Inkrafttreten: 1. August 2024
- Kritik der Industrie: zu streng, Kritik von Bürgerrechtlern/DGB: nicht weit genug, zu viele Schlupflöcher

Bildquelle: Pixabay
Gerd Altmann

Zeitplan der Anwendung

1. August 2024

Startdatum: Der AI Act tritt formell in Kraft, es beginnt jedoch eine Übergangsphase, in der zentrale Regelungen noch nicht greifen.

2. Februar 2025

Verbote: Bestimmte KI-Praktiken („unannehmbare Risiken“) sind ab jetzt EU-weit verboten.

KI-Kompetenz: Unternehmen müssen Maßnahmen zur Förderung der AI Literacy treffen (z.B. Schulungen für Beschäftigte, die mit KI arbeiten).

Bildquelle: Pixabay
Gerd Altmann

Zeitplan der Anwendung

2. August 2025

General Purpose AI: Neue Anforderungen an Anbieter von allgemeinen KI-Modellen, insbesondere Transparenz- und Dokumentationspflichten sowie Umgang mit Trainingsdaten.

Aufsicht und Behörden: Das European AI Office beginnt mit der Arbeit; nationale Zuständigkeiten müssen benannt sein.

Governance und Sanktionen: Regeln über Bußgelder und Verwaltungsmaßnahmen werden konkretisiert.

Bildquelle: Pixabay
Gerd Altmann

Zeitplan der Anwendung

2. August 2026

Vollständige Anwendung: Die meisten Regeln, insbesondere für Hochrisiko-KI-Systeme (z.B. in kritischer Infrastruktur, Bildung, Justiz), werden verbindlich. Unternehmen müssen jetzt alle grundlegenden Anforderungen erfüllen und rechtmäßige Konformitätsbewertungen durchgeführt haben.

Sandboxes: Jeder Mitgliedstaat muss mindestens einen Erprobungsraum (regulatory sandbox) für KI eingerichtet haben.

2. August 2027

Letzte Phase: Besondere Hochrisiko-KI-Systeme, die als Sicherheitsbestandteil in unter EU-Vorschriften geregelten Produkten (wie Medizinprodukten, Autos) fungieren, fallen endgültig unter die neuen Regelungen.

Der AI Act ist nun vollständig anwendbar

Bildquelle: Pixabay
Gerd Altmann

Und warum das alles?

Ziele der EU-Kommission:

- Risikominimierung durch klare Vorgaben für KI-Systeme
- Förderung von Vertrauen in KI-Technologie
- Harmonisierung des Binnenmarkts bei KI-Anwendungen

Bildquelle: Pixabay
Peggy + Marco Lachmann

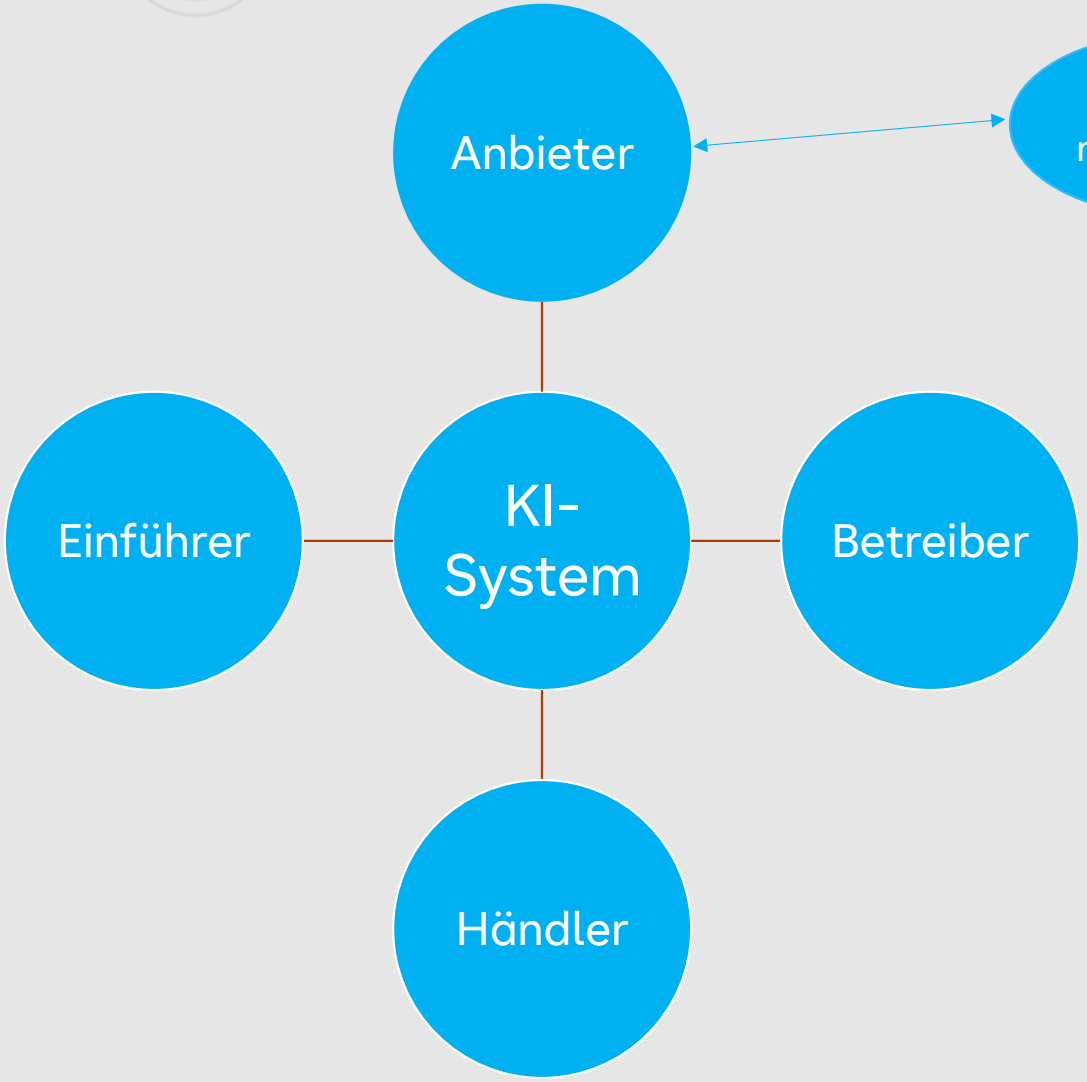
Definition „KI-System“

Laut KI-Verordnung Art 3 (1)

„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;

Bildquelle: Pixabay
Peggy + Marco Lachmann

Marktakteure



Marktakteure

Anbieter/Provider

Eine natürliche oder juristische Person oder Behörde, die ein AI-System bzw. ein General-Purpose AI Model (GPAI-Modell) entwickelt oder entwickeln lässt und unter ihrem Namen in der EU in Verkehr bringt oder in Betrieb nimmt – bezahlt oder kostenlos

Betreiber/Deployer

Eine natürliche oder juristische Person oder Behörde, die ein AI-System unter ihrer Leitung verwendet – **nicht** für rein private/private-nicht-professionelle Nutzung

Bildquelle: Pixabay
Peggy + Marco Lachmann

Marktakteure

Einführer/Importer

Jemand (natürlich/juristisch in der EU), der ein AI-System auf den EU-Markt bringt, das den Namen bzw. die Marke eines Anbieters außerhalb der EU trägt

Händler/Distributor

Ein Zwischenhändler (nicht Provider oder Importeur), der das AI-System auf dem EU-Markt verfügbar macht, z. B. Reseller oder Online-Marktplatz

Verbreitung von AI-Systemen gegenüber Endnutzern;

Bildquelle: Pixabay
Peggy + Marco Lachmann

Marktakteure

Authorised Representative

Eine Person oder juristische Einheit in der EU, die vom Provider außerhalb der EU schriftlich bevollmächtigt wurde, dessen Pflichten nach der Verordnung in der EU zu erfüllen

Vertritt Provider außerhalb der EU in der EU – übernimmt Pflichten wie Kommunikation mit Behörden, Behördeninformierung, Dokumentation usw.

Bildquelle: Pixabay
Peggy + Marco Lachmann

Verantwortlichkeiten entlang der KI-Wertschöpfungskette

Pflichten für alle Beteiligten:

- Zusammenarbeit zur Sicherstellung der Konformität
- Weitergabe relevanter Informationen
- Klare Zuweisung von Verantwortlichkeiten

Implikation:

- Verträge müssen Rollen und Pflichten eindeutig regeln

Bildquelle: Pixabay
Peggy + Marco Lachmann

Risikokategorien im Überblick

- **Verbotene KI-Systeme**

  z.B. soziale Bewertung, manipulative Systeme

- **Hochrisiko-KI**

  z. B. biometrische Identifikation, kritische Infrastrukturen

- **Geringes Risiko**

  z. B. Chatbots, Empfehlungsalgorithmen (mit Transparenzpflicht)

- **Minimalrisiko**

  z. B. Spamfilter, Spiele-KI

Bildquelle: Pixabay
Peggy + Marco Lachmann

Verbotene KI-Praktiken (Art. 5) - Auszug

Laut Artikel 5 sind folgende Praktiken, von denen unannehmbare Risiken ausgehen untersagt:

- KI-Anwendungen, die Menschen manipulieren könnten oder gegen ihre Grundrechte verstoßen
  - Social Scoring: Dabei klassifiziert Künstliche Intelligenz Menschen basierend auf ihrem sozialen Verhalten oder persönlicher Eigenschaften.
  - KI-Systeme, die Menschen manipulieren könnten und soziale Benachteiligungen wie das Alter, Armut oder Behinderungen ausnutzen.
  - Biometrische Erkennungssysteme, die Rückschlüsse auf persönliche Merkmale zulassen, zum Beispiel auf religiöse oder politische Einstellungen, Zugehörigkeit zu einer Gewerkschaft, die Rasse oder das Sexualleben.

Bildquelle: Pixabay
Peggy + Marco Lachmann

Verbotene KI-Praktiken (Art. 5) - Auszug

- Manipulation & Täuschung
- Ausnutzen von Schwachstellen
- Social Scoring
- Fernbeobachtung für Strafverfolgung
- Vorhersage von Straftaten
- Biometrische Kategorisierung
- Emotionserkennung
- Scraping von Gesichtsbildern
- ....

Aber:
im Gesetzestext gibt es Ausnahmen und Einschränkungen dieser Verbote

Einstufung als Hochrisiko-KI (Art. 6 & Anhang III)

Kriterien laut AI Act:

- Einsatz in sensiblen Bereichen wie Bildung, Beschäftigung, Strafverfolgung
- Automatisierte Entscheidungen mit erheblicher Wirkung auf Grundrechte
- Auflistung konkreter Anwendungsfälle im Anhang III

Pflicht für Unternehmen:

- Prüfung, ob das eigene System unter die Kategorien fällt
- Dokumentation der Einstufung und Begründung

Bildquelle: Pixabay
Peggy + Marco Lachmann

Anhang III Hoch-Risiko-Systeme

Anbieter

1. **Biometrie**

- Biometrische Fernidentifizierungssysteme (z. B. Gesichtserkennung in Echtzeit im öffentlichen Raum)
- KI-Systeme zur biometrischen Kategorisierung nach sensiblen oder geschützten Merkmalen (z. B. Erkennung von Geschlecht, Ethnie, etc.)
- KI-Systeme zur Emotionserkennung

2. **Kritische Infrastrukturen**

KI-Systeme als **Sicherheitsbauteile für Verwaltung und Betrieb** kritischer digitaler Infrastruktur, des Verkehrs oder Versorgungssektoren (Wasser, Gas, Wärme, Strom)

Bildquelle: Pixabay
Peggy + Marco Lachmann

Anhang III Hoch-Risiko-Systeme

Anbieter

3. **Bildung**

- KI-Systeme für Zugang und Zuweisung zu Bildungseinrichtungen (Schulen, Universitäten)
- KI-Systeme zur Bewertung von Schülern und Studenten

4. **Beschäftigung, Personalmanagement**

- KI-Systeme zur Personalbeschaffung (Stellenausschreibung, Auswahl oder Bewertung von Bewerbungen)
- KI-Systeme zum Management von Beschäftigten (Zuweisung von Aufgaben, Überwachung, Leistungsbeurteilung, Entscheidungen über Beförderung und Kündigung)

Bildquelle: Pixabay
Peggy + Marco Lachmann

Anhang III Hoch-Risiko-Systeme

Anbieter

5. Zugang zu wesentlichen privaten und öffentlichen Diensten

- KI-Systeme für Entscheidungen über Zugang zu privaten Leistungen (wie Kreditvergabe/Kreditwürdigkeitsprüfung)
- KI-Systeme für entscheidende öffentliche Dienstleistungen (wie Sozialleistungen, Gesundheitsleistungen, Notfallmaßnahmen)
- KI-Systeme im Bereich Migration, Asyl und Grenzmanagement (z. B. Visumserteilung, Asylverfahren)

Bildquelle: Pixabay
Peggy + Marco Lachmann

Anhang III Hoch-Risiko-Systeme

Anbieter

6. **Strafverfolgung, Justiz und demokratische Verfahren**

- KI-Systeme zur Bewertung von Beweismitteln, Vorhersage von Delikten, Strafzumessung, Verfahrensführung und ähnliches im Bereich Justiz und Strafverfolgung
- KI-Systeme zur Unterstützung von Entscheidungen im polizeilichen Kontext oder für andere Maßnahmen, die wesentliche Grundrechte berühren
- KI-Systeme für Migration, Asyl und Grenzkontrolle
- Ki-Systeme zur Rechtspflege und demokratische Prozesse
  - die bestimmungsgemäß von einer Justizbehörde verwendet werden, um diese bei der Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften und bei der Anwendung des Rechts auf konkrete Sachverhalte zu unterstützen

Bildquelle: Pixabay
Peggy + Marco Lachmann

Anforderungen an Hochrisiko-KI (Art. 8–15)

Anbieter

Pflichten laut Gesetz:

- Risikomanagementsystem (Art. 9)
- Datenqualität & Governance (Art. 10)
- Technische Dokumentation (Art. 11)
- Logging & Nachvollziehbarkeit (Art. 12)
- Transparenz gegenüber Nutzern (Art. 13)
- Menschliche Kontrolle („Human Oversight", Art. 14)
- Robustheit & Cybersicherheit (Art. 15)

Bildquelle: Pixabay
Peggy + Marco Lachmann

Risikomanagementsystem (Art. 9)

Anbieter

Anforderungen:

- Identifikation und Bewertung potenzieller Risiken
  - Bei bestimmungsgemäßen Gebrauch
- Maßnahmen zur Risikominderung
- Kontinuierliche Überwachung und Aktualisierung
  - Während des gesamten Lebenszyklus

Bildquelle: Pixabay
Peggy + Marco Lachmann

Ziel: jedes mit einer bestimmten Gefahr verbundene relevante Restrisiko sowie das Gesamtrestrisiko der Hochrisiko-KI-Systeme wird als vertretbar beurteilt.

Datenqualität & Governance (Art. 10)

Anbieter

Pflichten:

- Verwendung repräsentativer, fehlerfreier und relevanter Daten
- Dokumentation der Herkunft und Verarbeitung
- Schutz vor Bias und Diskriminierung
- Liste von Tatbeständen zur gesonderten Verarbeitung Personenbezogener Daten

Empfehlung:

- Zusammenarbeit mit Datenschutzbeauftragten und Data Scientists

Bildquelle: Pixabay
Peggy + Marco Lachmann

Technische Dokumentation (Art. 11)

Anbieter

- **Inhalte:**
- Beschreibung des KI-Systems und seiner Funktionen
  - Bevor es in Verkehr gebracht wird
- Informationen zur Trainings-, Validierungs- und Testphase
- Nachvollziehbarkeit der Entscheidungslogik
  - Und Nachweis, der Erfüllung des Kapitel III

Praxisbezug:

- Grundlage für Konformitätsbewertung und CE-Kennzeichnung

Bildquelle: Pixabay
Peggy + Marco Lachmann

Logging & Aufzeichnungspflichten (Art. 12)

Anbieter

Pflicht zur Protokollierung:

- Automatisierte Entscheidungen
- Systeminteraktionen und Eingaben
- Fehler und Abweichungen

Ziel:

- Nachvollziehbarkeit für Audits und Rechtsstreitigkeiten

Bildquelle: Pixabay
Peggy + Marco Lachmann

Transparenz für die Betreiber (Art. 13)

Anbieter

Erforderlich:

- Information über den Einsatz von KI
- Erläuterung der Funktionsweise in verständlicher Sprache
- Hinweis auf mögliche Einschränkungen
- Auflistung der Inhalte von Betriebsanleitungen

Ziel: die Betreiber können die Ausgaben eines Systems angemessen interpretieren und verwenden

Bildquelle: Pixabay
Peggy + Marco Lachmann

Menschliche Kontrolle („Human Oversight“, Art. 14)

Anbieter

Pflichten:

- Festlegung von Eingriffsmöglichkeiten
- Schulung der verantwortlichen Personen
- Verhinderung automatisierter Entscheidungen ohne menschliche Prüfung
- Vermeidung des Automatisierungsbias
- Nicht-Verwendung des KI-Systems und Stopp-Taste
- Z.T. 4 Augen-Prinzip

Empfehlung:

- Governance-Richtlinien und Betriebsvereinbarungen

Bildquelle: Pixabay
Tumisu

Robustheit & Cybersicherheit (Art. 15)

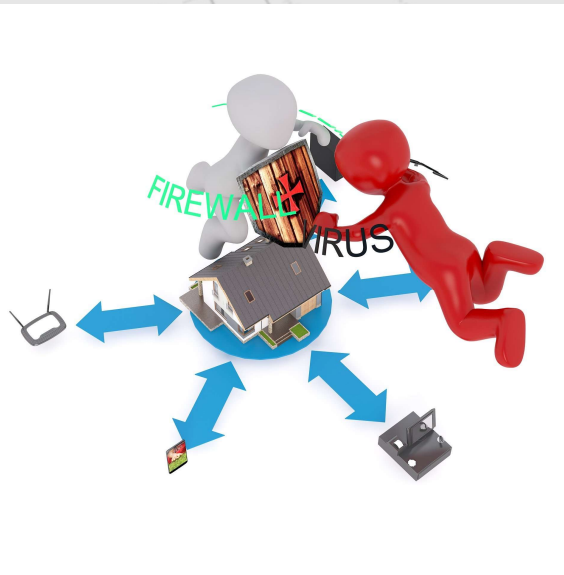
Anbieter

Technische Anforderungen:

- Schutz vor Manipulation und Angriffen
  - Data Poisoning und Model Poisoning
  - Erkennung von Eingabedaten, die das KI-Modell zu Fehlern verleiten
- Fehlertoleranz und Stabilität
- Bei lernenden Systemen: Maßnahmen zur Vermeidung verzerrter Ausgaben
- Notfallmechanismen bei Systemversagen

Rechtlicher Bezug:

- Haftung bei Sicherheitslücken oder Datenverlust



Bildquelle: Pixabay
Peggy + Marco Lachmann

Pflichten der Anbieter von Hochrisiko-KI-Systemen

Anbieter

Pflichten für Unternehmen, die Hochrisiko-KI bereitstellen:

- Einrichtung eines Qualitätsmanagementsystems (Art. 17)
- Aufbewahrung technischer Unterlagen (Art. 18)
- Protokollierung automatisierter Entscheidungen (Art. 19)
- Korrekturmaßnahmen bei Problemen (Art. 20)
- Zusammenarbeit mit Behörden (Art. 21)
- Benennung eines Bevollmächtigten (Art. 22)
- Konformitätsbewertung (Art. 43)
- Transparenzpflichten (Art. 50)

Bildquelle: Pixabay
Peggy + Marco Lachmann

Qualitätsmanagementsystem für KI-Systeme (Art. 17)

Anbieter

- Verpflichtung zur Einrichtung eines Qualitätsmanagementsystems.
- Regelmäßige Überprüfung und Anpassung
- Integration in bestehende Unternehmensprozesse

...

Praxisbezug:

- Schnittstelle zu ISO-Normen und internen Auditverfahren
- Integration in andere Managementsysteme möglich

Bildquelle: Pixabay
Peggy + Marco Lachmann

Dokumentationspflichten für KI-Systeme (Art.18)

Anbieter

- Verpflichtung zur Aufbewahrung umfassender Dokumentation
  - 10 Jahre ab Inverkehrbringen
- Inhalte der Dokumentation
  - Entwicklung
  - Tests
  - Funktionsweise
- Bedeutung für Transparenz und Nachvollziehbarkeit.

Bildquelle: Pixabay
Peggy + Marco Lachmann

Automatisierte Protokollierung von KI-Aktivitäten (Art.19)

Anbieter

- Verpflichtung zur automatischen Erstellung von Protokollen.
  - Aufbewahrung mind. 6 Monate
- Inhalte der Protokolle (Aktivitäten, Entscheidungen).
- Nachvollziehbarkeit und Überprüfbarkeit der KI-Entscheidungen.

Ziel:

- sicherstellen, dass die Entscheidungen der KI nachvollziehbar und überprüfbar sind.

Bildquelle: Pixabay
Peggy + Marco Lachmann

Korrekturmaßnahmen und Informationspflicht (Art.20)

Anbieter

- Verpflichtung zur unverzüglichen Ergreifung von Korrekturmaßnahmen
- Information der zuständigen Behörden
- Sicherstellung der Sicherheit der KI-Systeme

Ziel:

- kontinuierliche Verbesserung der KI-Systeme

Bildquelle: Pixabay
Peggy + Marco Lachmann

Zusammenarbeit mit Behörden (Art.21)

Anbieter

- Verpflichtung zur Zusammenarbeit mit den zuständigen Behörden
- Konformität des Hochrisiko-KI-Systems mit den in Abschnitt 2 festgelegten Anforderungen nachzuweisen
- in einer Sprache, die für die Behörde leicht verständlich ist ;-)
- zuständige Behörde wahrt Vertraulichkeit

Bildquelle: Pixabay
Peggy + Marco Lachmann

Bevollmächtigte für nicht-EU-Anbieter (Art.22)

Anbieter

- Verpflichtung zur Benennung eines Bevollmächtigten in der EU.
  - vor der Bereitstellung ihrer Hochrisiko-KI-Systeme auf dem Unionsmarkt
  - Im Auftrag des Anbieters
  - als Ansprechpartner für Behörden.
- Zur Sicherstellung der Einhaltung der Verordnung durch den Anbieter

Aufgaben (nicht abschliessend)

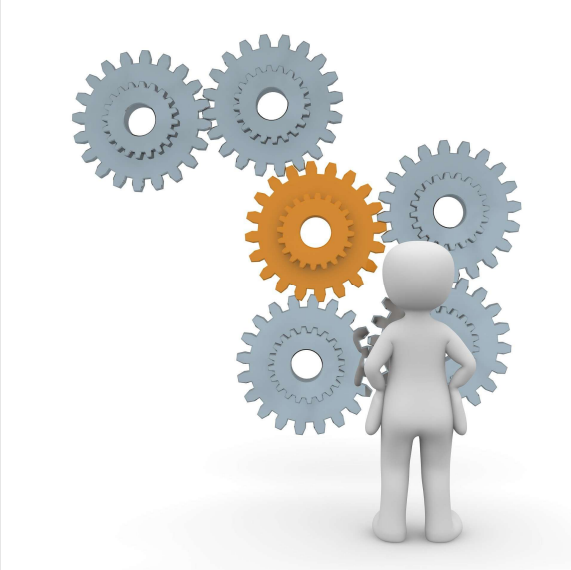
- Überprüfung, ob die EU-Konformitätserklärung und die technische Dokumentation erstellt wurden und ob der Anbieter ein angemessenes Konformitätsbewertungsverfahren durchgeführt hat
- Bereithalten der EU-Konformitätserklärung und der technischen Dokumentation

Bildquelle: Pixabay
Peggy + Marco Lachmann

Pflichten der Betreiber von Hochrisiko-KI-Systemen I

Betreiber

- Verwendung gemäß Anleitung des Anbieters
- Zuweisung menschlicher **Aufsicht an qualifizierte Personen**
- Sicherstellung relevanter und repräsentativer Eingabedaten
- Organisation der Aufsicht liegt im Ermessen des Betreibers
- Laufende Systemüberwachung gemäß Anleitung
- Meldung von Risiken oder **schwerwiegenden Vorfällen** an Anbieter & Behörden



Bildquelle: Pixabay
Peggy + Marco Lachmann

KI-Kompetenz (AI Literacy)

Artikel 4 KI-Kompetenz

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.

Art 3 (56) Begriffsbestimmungen

„KI-Kompetenz" 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.

Schwerwiegender Vorfall (Serious Incident)

Artikel 73 Meldung schwerwiegender Vorfälle

(1) Anbieter von in der Union in Verkehr gebrachten Hochrisiko-KI-Systemen melden schwerwiegende Vorfälle den Marktüberwachungsbehörden der Mitgliedstaaten, in denen der Vorfall stattgefunden hat.

(2) Die Meldung nach Absatz 1 **erfolgt unmittelbar**, nachdem der Anbieter den kausalen Zusammenhang zwischen dem KI-System und dem schwerwiegenden Vorfall oder die naheliegende Wahrscheinlichkeit eines solchen Zusammenhangs festgestellt hat **und in jedem Fall spätestens 15 Tage**, nachdem der Anbieter oder gegebenenfalls der Betreiber Kenntnis von diesem schwerwiegenden Vorfall erlangt hat.

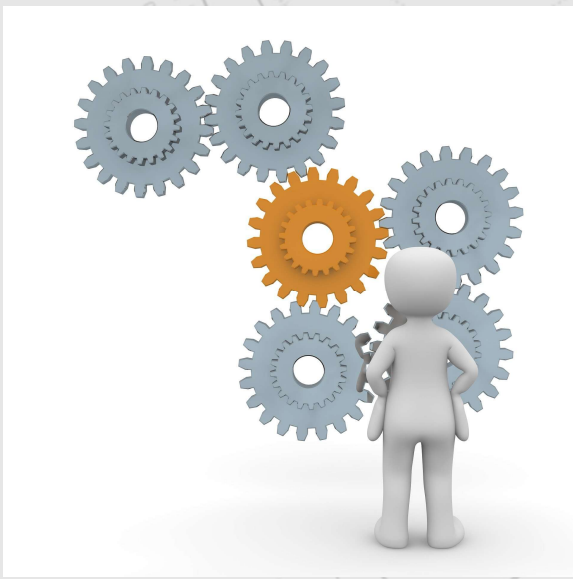
Art 3 (49) Begriffsbestimmungen

„schwerwiegender Vorfall" einen Vorfall oder eine Fehlfunktion bezüglich eines KI-Systems, das bzw. die direkt oder indirekt eine der nachstehenden Folgen hat:
a) den Tod oder die schwere gesundheitliche Schädigung einer Person;
b) eine schwere und unumkehrbare Störung der Verwaltung oder des Betriebs kritischer Infrastrukturen;
c) die Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte;
d) schwere Sach- oder Umweltschäden;

Pflichten der Betreiber von Hochrisiko-KI-Systemen II

Betreiber

- Protokollierung automatisch erzeugter Logs (mind. 6 Monate)
- Information der Beschäftigte vor Einsatz am Arbeitsplatz
- Öffentliche Stellen müssen Systeme vor Einsatz registrieren
- Nutzung nur bei Eintrag in EU-Datenbank erlaubt
- Pflicht zur Datenschutz-Folgenabschätzung (DSFA) bei personenbezogener Verarbeitung
- Einsatz biometrischer Fernidentifikation nur mit richterlicher Genehmigung
- Betroffene Personen müssen über KI-Einsatz informiert werden

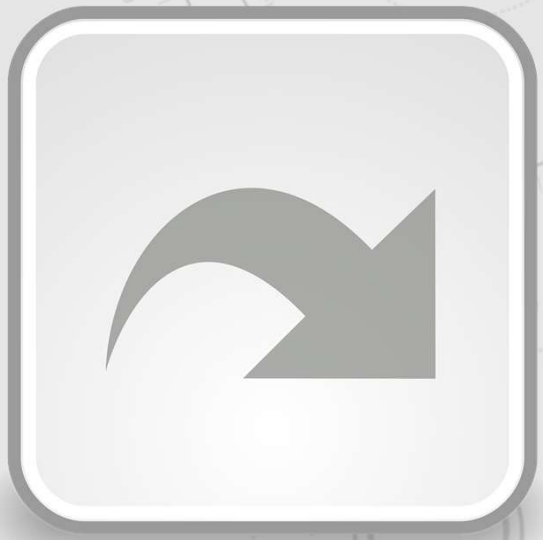


Bildquelle: Pixabay
Peggy + Marco Lachmann

Pflichten der Einführer von Hochrisiko-KI-Systemen (Art. 23)

Einführer

- Einführer müssen sicherstellen, dass das KI-System den EU-Vorgaben entspricht.
- Prüfung CE-Kennzeichnung, Konformitätserklärung und technische Dokumentation.
- Bei Risiken oder Nichtkonformität: Information an Behörden und Rücknahme vom Markt.
- Zusammenarbeit mit Marktüberwachungsbehörden ist verpflichtend.



Bildquelle: Pixabay
OpenIcons

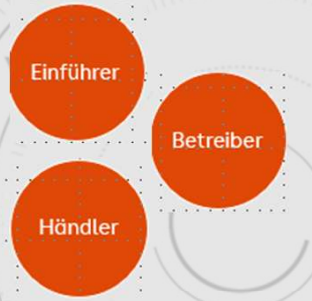
Pflichten der Händler von Hochrisiko-KI-Systemen

Händler

- Händler dürfen nur konforme Hochrisiko-KI-Systeme vertreiben.
- Sie müssen CE-Kennzeichnung, Konformitätserklärung und Anleitung prüfen.
- Bei Verdacht auf Risiko: keine Bereitstellung, Information an Anbieter und Behörden.
- Verantwortung für Lagerung und Transport liegt beim Händler.

Bildquelle: Pixabay
Mohamed Hassan

Erweiterung der Anbieter-Eigenschaft (Art.25)



- Wer ein KI-System wesentlich verändert oder neu kennzeichnet, wird zum Anbieter.
- Hersteller von Produkten mit integrierter Hochrisiko-KI gelten ebenfalls als Anbieter.
- Schriftliche Vereinbarungen mit Drittanbietern sind erforderlich.
- Schutz von Geschäftsgeheimnissen und IP-Rechten bleibt gewahrt.

Bildquelle: Pixabay
Peggy + Marco Lachmann

Sanktionen bei Verstößen (Art. 99)

Geldbußen:

- Bis zu 35 Mio. € oder 7 % des weltweiten Jahresumsatzes bei Verstoß gegen Art. 5
- Ansonsten bezogen Verstöße gegen einzelne Artikel
  - Bis zu 15 Mio. € oder 3 % des weltweiten Jahresumsatzes
  - Bis zu 7,5 Mio. € oder 1 % des weltweiten Jahresumsatzes
- Sonderregelung für KMU, einschließlich Start-up-Unternehmen

Bildquelle: Pixabay
Gerd Altmann

General Purpose AI (GPAI)

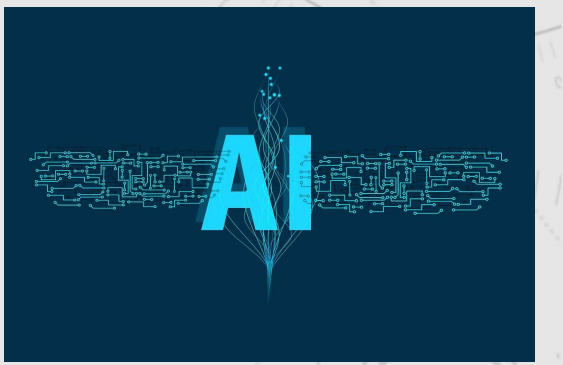
General Purpose AI = KI-Modell mit allgemeinem Verwendungszweck

Art 3 (63) Ki-VO

ein 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, <..>

Art 3 (64) Ki-VO

„Fähigkeiten mit hoher Wirkkraft“ bezeichnet Fähigkeiten, die den bei den **fortschrittlichsten KI-Modellen mit allgemeinem Verwendungszweck festgestellten Fähigkeiten entsprechen oder diese übersteigen;**

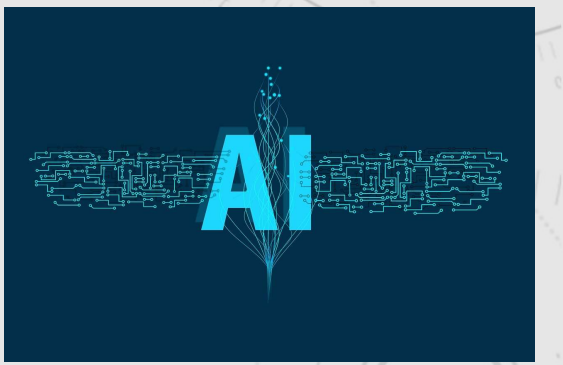


Bildquelle: Pixabay
Gerd Altmann

General Purpose AI (GPAI)

Art 3 (65) Ki-VO

„systemisches Risiko“ ein Risiko, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund **deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen** auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können;



Bildquelle: Pixabay
Gerd Altmann

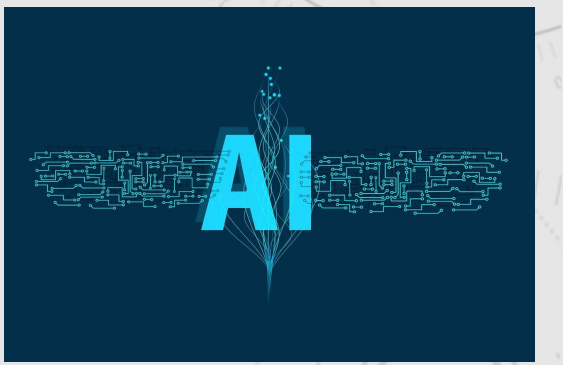
General Purpose AI (GPAI)

Was sind GPAI-Modelle?

- KI-Modelle, die für eine Vielzahl von Anwendungen genutzt werden können
- Beispiele: Sprachmodelle, Bildgeneratoren, Entscheidungsalgorithmen
- Regulierung ab 2. August 2025

Systemisches Risiko

- Modelle mit besonders großer Reichweite und Einfluss können als „systemisch riskant“ eingestuft werden
- Meldung erforderlich, dann Einstufung durch das KI-Büro der EU **(Art. 52)**

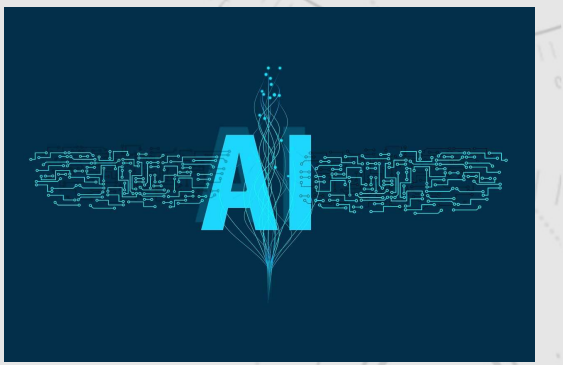


Bildquelle: Pixabay
Gerd Altmann

Allgemeine Pflichten für GPAI-Anbieter

Pflichten:

- Technische Dokumentation
- Zusammenfassung des Trainingsdatensatzes
- Urheberrechtskonformität: Einhaltung von Urheberrecht und Datenschutz
- Schutz vor Missbrauch
- Transparenz & Nachvollziehbarkeit
  - Offenlegung der Funktionsweise
  - Beschreibung der Systemarchitektur
  - Zugang zu Informationen für Behörden und Nutzer



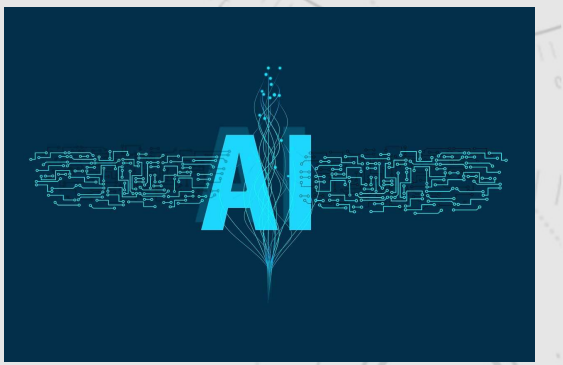
Bildquelle: Pixabay
Gerd Altmann

Bevollmächtigte & Vertretung

Pflicht zur Benennung eines Bevollmächtigten

- Auch wenn es kein Hochrisiko-System ist
- Für Anbieter außerhalb der EU
- Zuständig für Kommunikation mit Behörden
- Muss Zugang zu technischer Dokumentation haben

Entspricht dem Beauftragten gemäß Art 22 bei Hochrisiko-Systemen



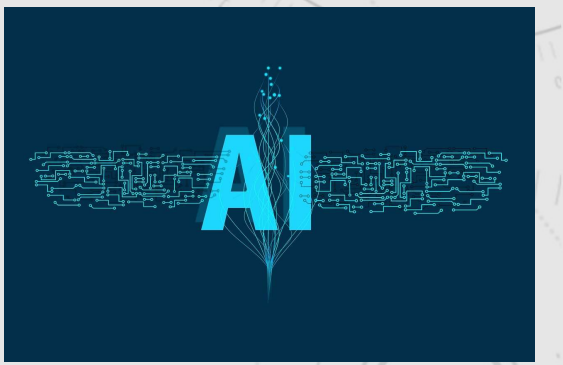
Bildquelle: Pixabay
Gerd Altmann

Zusätzliche Pflichten bei systemischem Risiko

Anbieter

- Durchführung von Modellbewertungen (z. B. Bias, Robustheit)
- Veröffentlichung von Berichten zur Systemleistung
- Einrichtung eines Compliance-Programms
- Meldung schwerwiegender Vorfälle an das KI-Büro
- Gewährleisten angemessenes Maß an Cybersicherheit für die KI-Modelle <…> und die physische Infrastruktur des Modells

Hinweis:
Diese Pflichten gelten zusätzlich zu den allgemeinen Anforderungen aus Art. 53



Bildquelle: Pixabay
Gerd Altmann

Sanktionen bei Verstößen bei GPAI (Art. 101)

Geldbußen:

- Bis zu 15 Mio. € oder 3 % des weltweiten Jahresumsatzes
- Gilt für systemische GPAI-Verstöße
- Geldbußen müssen wirksam, verhältnismäßig und abschreckend

Zusätzlich:

- Veröffentlichung der Sanktion
- Einschränkung des Modells

Bildquelle: Pixabay
Gerd Altmann

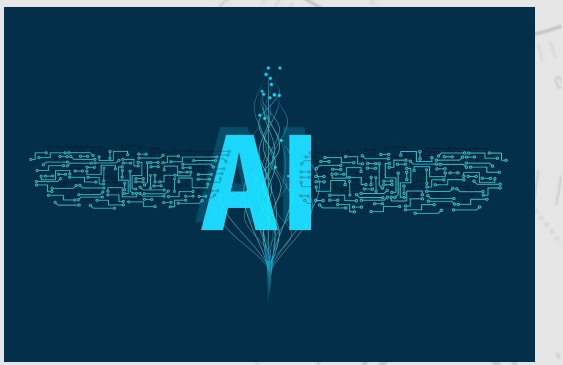
Praxisleitfäden & freiwillige Standards

Unterstützende Maßnahmen:

- EU-Kommission kann Praxisleitfäden veröffentlichen
- Anbieter können freiwillige Standards anwenden (z. B. Ethikrichtlinien, Transparenzlabels)

Strategischer Nutzen:

- Wettbewerbsvorteil durch vertrauenswürdige KI
- Minderung regulatorischer Risiken



Bildquelle: Pixabay
Gerd Altmann

Leitlinien

- Die EU-Kommission hat Leitlinien zur Auslegung der **Pflichten für GPAI-Modelle** gemäß AI Act veröffentlicht (18.Juli 2025)

Ziele

- Einheitliche Anwendung und Unterstützung für Anbieter, Behörden und Nutzer
- den Akteuren in der gesamten KI-Wertschöpfungskette Rechtssicherheit zu bieten
- Präziseren Umfang der Verpflichtungen
  - Worum geht es
  - Wer ist betroffen
  - Ausnahmen
  - Durchsetzung

Bildquelle: Pixabay
Peggy + Marco Lachmann

Guidelines_on_the_scope_of_the_obligations_for_generalpurpose_AI_models_establi...

Leitlinien - Definition der GPAI-Modelle

Ein GPAI-Modell ist definiert als jedes Modell, das mit **mehr als 10^{23} FLOPS** (Gleitkommaoperationen pro Sekunde) trainiert wurde und in der Lage ist, Sprach- (Text/Audio), Text-zu-Bild- oder Text-zu-Video-Ausgaben zu erzeugen.

Erfordernis der funktionalen Allgemeinheit:

Modelle, die den Schwellenwert von 10^{23} FLOPS überschreiten, aber spezialisiert sind (z. B. für die Transkription, die Hochskalierung von Bildern, die Wettervorhersage oder Spiele), **werden ausgeschlossen**, wenn ihnen allgemeine Fähigkeiten für ein breites Spektrum von Aufgaben fehlen.

Bildquelle: Pixabay
Peggy + Marco Lachmann

Guidelines_on_the_scope_of_the_obligations_for_generalpurpose_AI_models_establi...

Leitlinien - GPAI-Modelle mit systemischem Risiko

Modelle, die mit **≥10^{25} FLOPS** trainiert wurden, wird davon ausgegangen, dass es eine hohe Auswirkung hat und als **GPAI mit systemischem Risiko** eingestuft werden kann.

Zusätzliche Verpflichtungen:

- Umfassende **Risikobewertung** und -minderung während des gesamten Lebenszyklus, einschließlich Modellbewertungen.
- Robuste **Cybersicherheitsmaßnahmen**
- Verfolgung von und Berichterstattung über ernste **Zwischenfälle**
- Kommission innerhalb von zwei Wochen benachrichtigen

Bildquelle: Pixabay
Peggy + Marco Lachmann

Guidelines_on_the_scope_of_the_obligations_for_generalpurpose_AI_models_establi...

Leitlinien - Lebenszyklus des Modells und Verpflichtungen

Es gelten die lebenszyklusweiten Verpflichtungen ab dem Beginn seines Pre-Trainingslaufs und für Entwicklungsphasen, inkl. Änderungen nach dem Inverkehrbringen.

- **Dokumentation**: Muss gepflegt und aktualisiert werden und den nachgeschalteten Anbietern sowie auf Anfrage dem AI-Büro oder den zuständigen nationalen Behörden zur Verfügung gestellt werden.
- **Zusammenfassung der Ausbildungsdaten**: Die Anbieter müssen eine Zusammenfassung unter Verwendung der noch zu erstellenden AI Office-Vorlage veröffentlichen.
- **Copyright-Richtlinie:** Muss die Einhaltung des Urheberrechts regeln und kann für alle Modelle gelten.

Bildquelle: Pixabay
Peggy + Marco Lachmann

Verhaltenskodex (Code of Practice)

Die EU-Kommission hat am 10.Juli 2025 einen mehrteiligen, freiwilligen Verhaltenskodex ausgearbeitet (der der Industrie dabei helfen soll, die Verpflichtungen des KI-Gesetzes für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck zu erfüllen

Ziele:

- soll Anbietern helfen, ihre Pflichten zu erfüllen
- soll der KI-Behörde die Bewertung der Einhaltung ermöglichen

Bisher unterzeichnet von (Stand 18.09.2025):

Accexible, AI Alignment Solutions, Aleph Alpha, Almawave, Amazon, Anthropic, Bria AI, Cohere, Cyber Institute, Domyn, Dweve, Euc Inovação Portugal, Fastweb, Google, Humane Technology, IBM, Lawise, LINAGORA, Microsoft, Mistral AI, Open Hippo, OpenAI, Pleias, re-inventa, ServiceNow, Virtuo Turing, WRITER

Bildquelle: Pixabay
Peggy + Marco Lachmann

Kapitel Transparenz: Dokumentationspflichten

- Anbieter müssen technische Dokumentation bereitstellen
- Verwendung des „Model Documentation Form“ zur strukturierten Erfassung
- Informationen zu Trainingsdaten, Modellarchitektur, Energieverbrauch, Lizenzierung
- Pflicht zur Bereitstellung relevanter Informationen für:
  - EU AI Office
  - Nationale Behörden
  - Downstream-Anbieter

Anfragen müssen über das AI Office laufen und begründet sein

Bildquelle: Pixabay
Peggy + Marco Lachmann

Code_of_Practice_for_GeneralPurpose_AI_Models_Transparency_Chapter_2_U

Kapitel Transparenz: Dokumentationspflichten

- Anbieter müssen technische Dokumentation bereitstellen
- Verwendung des „Model Documentation Form“ zur strukturierten Erfassung

Struktur des Modell-Dokumentationsformulars

Kategorien der Informationen:

Verteilungsmethoden und Lizenzen: Verteilungswege und Lizenzbedingungen
Allgemeine Informationen: Name des Anbieters, Modellname, Freigabedatum, etc.
Modelleigenschaften: Architektur, Designspezifikationen, Eingabe- und AusgabeModalitäten
Verwendung: Zulässige Nutzungsrichtlinien, beabsichtigte Verwendungszwecke, technische Mittel für die Modellintegration
Trainingsprozess: Designspezifikationen des Trainingsprozesses, Entscheidungsrationalen
Daten für Training, Test und Validierung: Datentypen, Herkunft, Umfang und Hauptmerkmale, Datenbereinigungsmethoden
Energieverbrauch: Energieverbrauch während des Trainings und der Inferenz
Rechenressourcen: Trainingszeit, Rechenaufwand, Messmethoden

Kapitel Transparenz: Dokumentationspflichten

- Anbieter müssen technische Dokumentation bereitstellen
- Verwendung des „Model Documentation Form“ zur strukturierten Erfassung
- Informationen zu Trainingsdaten, Modellarchitektur, Energieverbrauch, Lizenzierung
- Pflicht zur Bereitstellung relevanter Informationen für:
  - EU AI Office
  - Nationale Behörden
  - Downstream-Anbieter

Anfragen müssen über das AI Office laufen und begründet sein

Bildquelle: Pixabay
Peggy + Marco Lachmann

Code_of_Practice_for_GeneralPurpose_AI_Models_Transparency_Chapter_2_U

Kapitel Transparenz: Aktualisierung & Aufbewahrung

- Dokumentation muss bei Änderungen aktualisiert werden
- Frühere Versionen sind mindestens 10 Jahre aufzubewahren
- Kontaktstelle für Informationsanfragen muss benannt werden
- Qualitätskontrolle
- Schutz der Informationen vor unbeabsichtigten Veränderungen

Bildquelle: Pixabay
Peggy + Marco Lachmann

Code_of_Practice_for_GeneralPurpose_AI_Models_Transparency_Chapter_2_U

Commitment 1 Documentation

LEGAL TEXT: Articles 53(1)(a), 53(1)(b), 53(2), 53(7), and Annexes XI and XII AI Act

In order to fulfil the obligations in Article 53(1), points (a) and (b), AI Act, Signatories commit to drawing up and keeping up-to-date model documentation in accordance with Measure 1.1, providing relevant information to providers of AI systems who intend to integrate the general-purpose AI model into their AI systems ('downstream providers' hereafter), and to the AI Office upon request (possibly on behalf of national competent authorities upon request to the AI Office when this is strictly necessary for the exercise of their supervisory tasks under the AI Act, in particular to assess the compliance of a high-risk AI system built on a general-purpose AI model where the provider of the system is different from the provider of the model[1]), in accordance with Measure 1.2, and ensuring quality, security, and integrity of the documented information in accordance with Measure 1.3. In accordance with Article 53(2) AI Act, these Measures do not apply to providers of general-purpose AI models released under a free and open-source license that satisfy the conditions specified in that provision, unless the model is a general-purpose AI model with systemic risk.

Measure 1.1 Drawing up and keeping up-to-date model documentation

Signatories, when placing a general-purpose AI model on the market, will have documented at least all the information referred to in the Model Documentation Form below (hereafter this information is referred to as the 'Model Documentation'). Signatories may choose to complete the Model Documentation Form provided in the Appendix to comply with this commitment.

Signatories will update the Model Documentation to reflect relevant changes in the information contained in the Model Documentation, including in relation to updated versions of the same model, while keeping previous versions of the Model Documentation for a period ending 10 years after the model has been placed on the market.

wahrung

Bildquelle: Pixabay
Peggy + Marco Lachmann

Code_of_Practice_for_GeneralPurpose_AI_Models_Transparency_Chapter_2_U

Kapitel Urheberrecht

Anbieter

Anbieter müssen eine Urheberrechtspolitik erstellen und aktualisieren, die sicherstellt, dass sie Unionrecht zum Urheberrecht einhalten

Maßnahmen im Einzelnen:

- Erstellung und Implementierung einer Urheberrechtspolitik
- Rechtmäßige Nutzung beim Crawlen des Internets
- Identifizierung und Einhaltung von Rechtevorbehalten
- Vermeidung von urheberrechtsverletzenden Ausgaben
- Kontaktstelle und Beschwerdemechanismus
- Unterstützung und Zusammenarbeit

Bildquelle: Pixabay
Peggy + Marco Lachmann

Code_of_Practice_for_GeneralPurpose_AI_Models_Copyright_Chapter_

Commitment 1 Copyright policy

LEGAL TEXT: Article 53(1)(c) AI Act

(1) In order to demonstrate compliance with their obligation pursuant to Article 53(1), point (c) of the AI Act to put in place a policy to comply with Union law on copyright and related rights, and in particular to identify and comply with, including through state-of-the-art technologies, a reservation of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790, Signatories commit to drawing up, keeping up-to-date and implementing such a copyright policy. The Measures below do not affect compliance with Union law on copyright and related rights. They set out commitments by which the Signatories can demonstrate compliance with the obligation to put in place a copyright policy for their general-purpose AI models they place on the Union market.

(2) In addition, the Signatories remain responsible for verifying that the Measures included in their copyright policy as outlined below comply with Member States' implementation of Union law on copyright and related rights, in particular but not only Article 4(3) of Directive (EU) 2019/790, before carrying out any copyright-relevant act in the territory of the relevant Member State as failure to do so may give rise to liability under Union law on copyright and related rights.

Measure 1.1 Draw up, keep up-to-date and implement a copyright policy

(1) Signatories will draw up, keep up-to-date and implement a policy to comply with Union law on copyright and related rights for all general-purpose AI models they place on the Union market. Signatories commit to describe that policy in a single document incorporating the Measures set out in this Chapter. Signatories will assign responsibilities within their organisation for the implementation and overseeing of this policy.

(2) Signatories are encouraged to make publicly available and keep up-to-date a summary of their

Anbieter

Bildquelle: Pixabay
Peggy + Marco Lachmann

tice_for_GeneralPurpose_AI_Models_Copyright_Chapter_

Urheberrecht: Grundsätze

- Anbieter dürfen nur rechtmäßig zugängliche Inhalte verwenden
- Keine Umgehung technischer Schutzmaßnahmen (z. B. robots.txt)
- Verpflichtung zur Einhaltung der EU-Urheberrechtsrichtlinie

Urheberrecht: Webcrawler & Rechtewahrung

- Webcrawler müssen Rechtevorbehalte respektieren
- Veröffentlichung von Informationen über verwendete Crawler
- Automatische Benachrichtigung betroffener Rechteinhaber bei Änderungen
- Technische Maßnahmen zur Verhinderung urheberrechtsverletzender Outputs
- Verbot solcher Nutzungen in den Nutzungsbedingungen
- Einrichtung eines Beschwerdemechanismus für Rechteinhaber

Bildquelle: Pixabay
Peggy + Marco Lachmann

Kapitel Sicherheit und Gefahrenabwehr

Anbieter

Konkrete State-of-the-Art-Praktiken für das Management systemischer Risiken, d.h. Risiken aus den fortschrittlichsten Modellen.

Ziele

- Kontinuierliche Risikobewertung
  - Prozess der Risikoidentifikation
  - Elemente der Risikoanalyse
  - Kontextbezogene Risikobewertung und -minderung
- Sicherheitsmaßnahmen und –ziele
- Rolle der EU und des AI Office

Bildquelle: Pixabay
Peggy + Marco Lachmann

Code_of_Practice_for_GeneralPurpose_AI_Models_Safety_and_Security_Chapter_

Kapitel Sicherheit und Gefahrenabwehr

Anbieter

Konkrete State-of-the-Art-Praktiken für das Management systemischer Risiken, d.h. Risiken aus den fortschrittlichsten Modellen.

Ziele

- *kontinuierliche Risikobewertung*
  - *Prozess der Risikoidentifikation*
  - *Elemente der Risikoanalyse*
  - *Kontextbezogene Risikobewertung und -minderung*
- Sicherheitsmaßnahmen und –ziele
- Rolle der EU und des AI Office

Bildquelle: Pixabay
Peggy + Marco Lachmann

Kapitel Sicherheit und Gefahrenabwehr

Konkrete State-of-the-Art-Praktiken für das Management systemischer Risiken, d.h. Risiken aus den fortschrittlichsten Modellen.

Ziele

- kontinuierliche Risikobewertung
  - Prozess der Risikoidentifikation
  - Elemente der Risikoanalyse
  - Kontextbezogene Risikobewertung und -minderung
- *Sicherheitsmaßnahmen und –ziele*
- Rolle der EU und des AI Office

Bildquelle: Pixabay
Peggy + Marco Lachmann

Kapitel Sicherheit und Gefahrenabwehr

Konkrete State-of-the-Art-Praktiken für das Management systemischer Risiken, d.h. Risiken aus den fortschrittlichsten Modellen.

Ziele

- kontinuierliche Risikobewertung
  - Prozess der Risikoidentifikation
  - Elemente der Risikoanalyse
  - Kontextbezogene Risikobewertung und -minderung
- Sicherheitsmaßnahmen und –ziele
- *Rolle der EU und des AI Office*

Bildquelle: Pixabay
Peggy + Marco Lachmann

Commitment 1 Safety and Security Framework

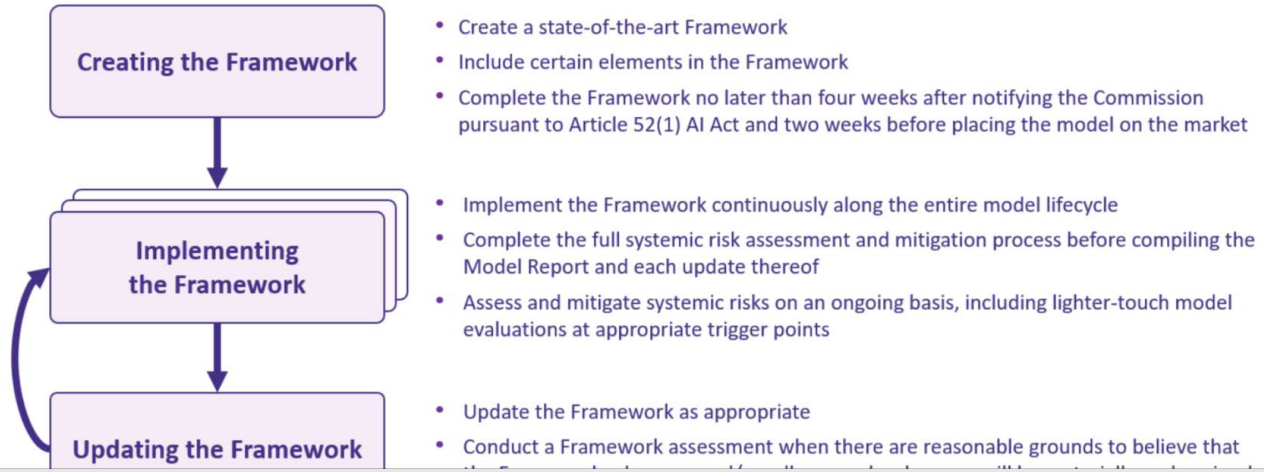
LEGAL TEXT: Articles 55(1) and 56(5), and recitals 110, 114, and 115 AI Act

Signatories commit to adopting a state-of-the-art Safety and Security Framework ("Framework"). The purpose of the Framework is to outline the systemic risk management processes and measures that Signatories implement to ensure the systemic risks stemming from their models are acceptable.

Signatories commit to a Framework adoption process that involves three steps:

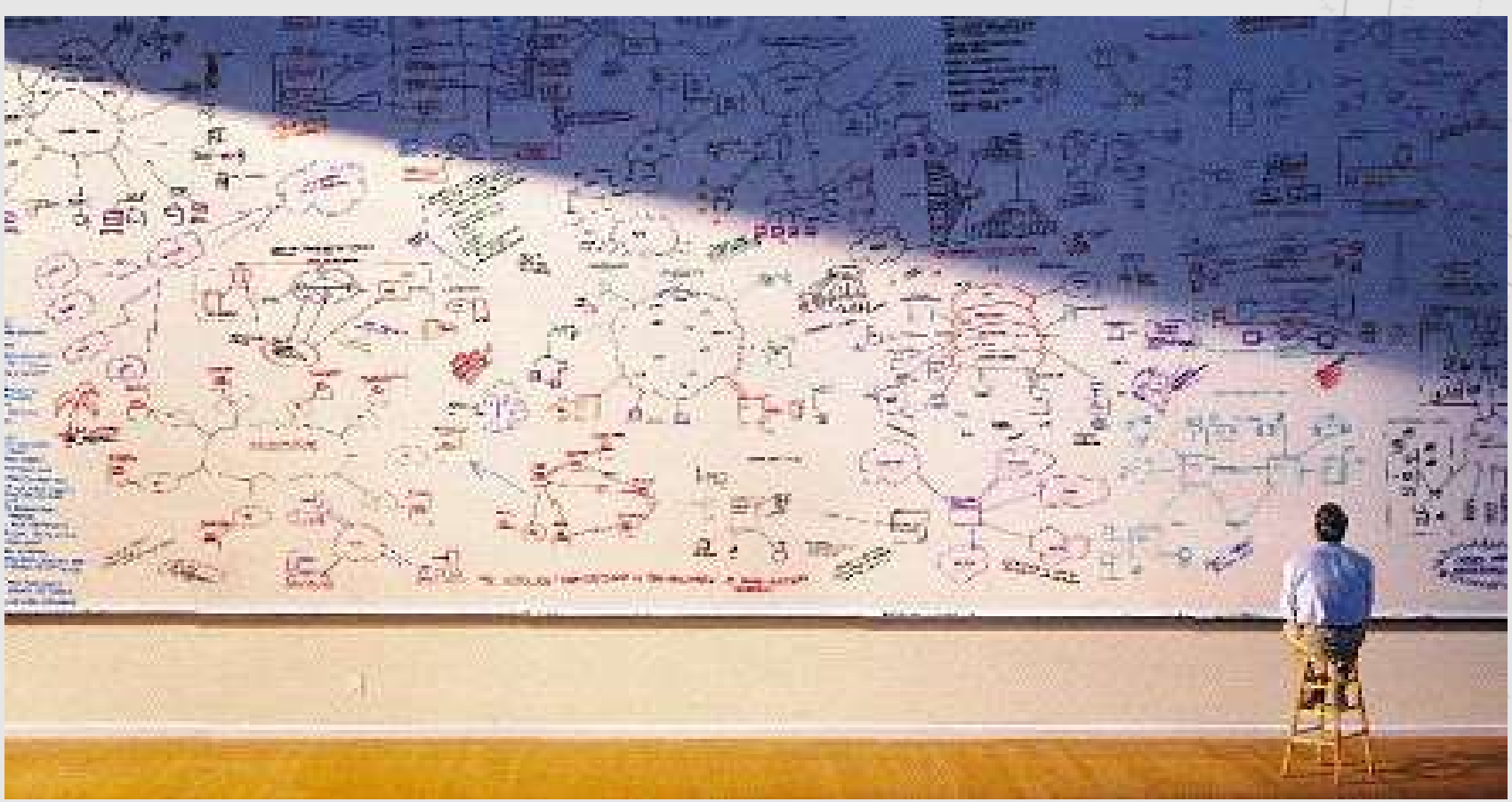
(1) creating the Framework (as specified in Measure 1.1);
(2) implementing the Framework (as specified in Measure 1.2); and
(3) updating the Framework (as specified in Measure 1.3).

Further, Signatories commit to notifying the AI Office of their Framework (as specified in Measure 1.4).



Bildquelle: Pixabay
Peggy + Marco Lachmann

Vielen Dank für die Aufmerksamkeit! Fragen?



Anhang – Governance Strukturen

Governance-Strukturen im AI Act (Kapitel VII)

Büro für Künstliche Intelligenz (AI Office)

- EU-weite Harmonisierung der Umsetzung und Durchsetzung des AIA
- Unterstützung der Kommission bei Risikoanalyse und Klassifikation
- Pflege einer öffentlichen Datenbank zu Hochrisiko-Systemen
- Kommunikation mit nationalen Marktüberwachungsbehörden
- Einrichtung von Compliance-Programmen für GPAI-Modelle mit systemischem Risiko
- Förderung freiwilliger Standards und Ethikrichtlinien

Bildquelle: Pixabay
Gerd Altmann

Governance-Strukturen im AI Act (Kapitel VII)

KI-Kremium (EU AI Board)

- Berät die Kommission
- Koordinierung der zuständigen nationalen Behörden
- Harmonisierung der Verwaltungspraktiken
- Besteht aus Vertretern aller Mitgliedstaaten
- Kann Stellungnahmen zu technischen Standards und Klassifizierungen abgeben
- Sammlung von Rückmeldungen zu GPAI-bezogenen Warnmeldungen

Bildquelle: Pixabay
Gerd Altmann

Governance-Strukturen im AI Act (Kapitel VII)

Stakeholder-Einbindung (Advisory Forum)

- Plattform für Experten, Unternehmen und Zivilgesellschaft
  - Bereitstellung von technischem Fachwissen
- Beitrag zur Weiterentwicklung der Regulierung
- Förderung von Transparenz und partizipativer Governance

Bildquelle: Pixabay
Gerd Altmann

Governance-Strukturen im AI Act (Kapitel VII)

Stakeholder-Einbindung (Advisory Forum)

- Plattform für Experten, Unternehmen und Zivilgesellschaft
- Beitrag zur Weiterentwicklung der Regulierung
- Förderung von Transparenz und partizipativer Governance

Pixabay
ann

CALL FOR TENDERS | Publication 17 July 2025

European Commission launches call for applications to join AI Act Advisory Forum

Opening: 17 July 2025

Closing: 14 September 2025

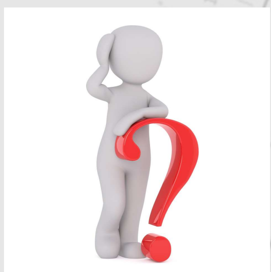
Governance-Strukturen im AI Act (Kapitel VII)

Nationaler Marktüberwachungsbehörden (market surveillance authorities)

- Zuständig für Kontrolle auf nationaler Ebene
- Durchführung von Audits und Vor-Ort-Prüfungen
- Zusammenarbeit mit dem EU AI-Büro
- Möglichkeit zur Untersagung von Systemen bei Nichtkonformität
- Unterstützung von Verbraucherschutz und fairem Wettbewerb

Bildquelle: Pixabay
Gerd Altmann

Governa  ukturen im AI  itel VII)



Nationaler Marktüberwach  ehörden (market surveillance authorities)

- Zuständig für Kontrolle auf
- Durchführung von Audits und
- Zus  mit dem EU
- Mö Untersagung

Bildquelle: Pixabay
Gerd Altmann