

Künstliche Intelligenz in der Verwaltung von Forschungseinrichtungen

Rechtliche Grundlagen für die
Anwendung von KI

Michael Löffler

25.06.2026



Funded by



EuroHPC
Joint Undertaking



**Co-funded by
the European Union**

 **Federal Ministry
Innovation, Mobility
and Infrastructure
Republic of Austria**

under discussion with



AI Factory Austria AI:AT has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101253078. The JU receives support from the Horizon Europe Programm of the European Union and Austria (BMIMI / FFG).

AI Factory Austria AI:AT – PUBLIC



AI Factory Austria AI:AT - Consortium

Disclaimer:

The speakers are solely sharing their personal experiences. Therefore, this talk is no substitute for professional/legal advice.

Beneficiaries



Affiliated Entities



Agenda: Künstliche Intelligenz

01

Künstliche Intelligenz

Definitionen, Risikoklassen des AI Acts, Rollen & Pflichten für Anbieter und Betreiber.

02

Datenschutz

DSGVO-Grundlagen, datenschutzrechtliche Rollenverteilung, Anonymisierung und die Risiken von Schatten-KI.

03

Urheberrecht

Text und Data Mining (TDM), urheberrechtliche Schutzfähigkeit von KI-Outputs und rechtskonforme Workflows.



Hinweis: Die Rollenverteilung ist dynamisch. Nach Art. 25 KI-VO können Betreiber durch wesentliche Änderungen oder Markenwechsel rechtlich schnell selbst zum „Anbieter“ mit vollen Pflichten werden.

New Legislative Framework (NLF)

Das KI-Gesetz basiert auf dem New Legislative Framework (NLF) für Produktsicherheit:

01



1. Wesentliche Anforderungen

Das Gesetz legt die Sicherheitsziele fest (z. B. „KI muss vertrauenswürdig und transparent sein“), keine technischen Anweisungen.

02



2. Harmonisierte Normen

Technische Gremien (CEN/CENELEC) entwerfen freiwillige Normen. Die Einhaltung begründet die **Konformitätsvermutung**.

03



3. Konformitätsbewertung

Je nach Risikostufe: Selbstbewertung oder unabhängige Prüfung durch eine **Notifizierte Stelle**.

04



4. CE-Kennzeichnung

Das Anbringen der CE-Kennzeichnung ermöglicht den freien Warenverkehr des Produkts **im gesamten EWR**.



The EU AI Act: A Risk-Based Approach to Regulation

To provide a high-level overview of the EU AI Act's key principles, focusing on its risk-based categories and the corresponding obligations for developers and businesses.

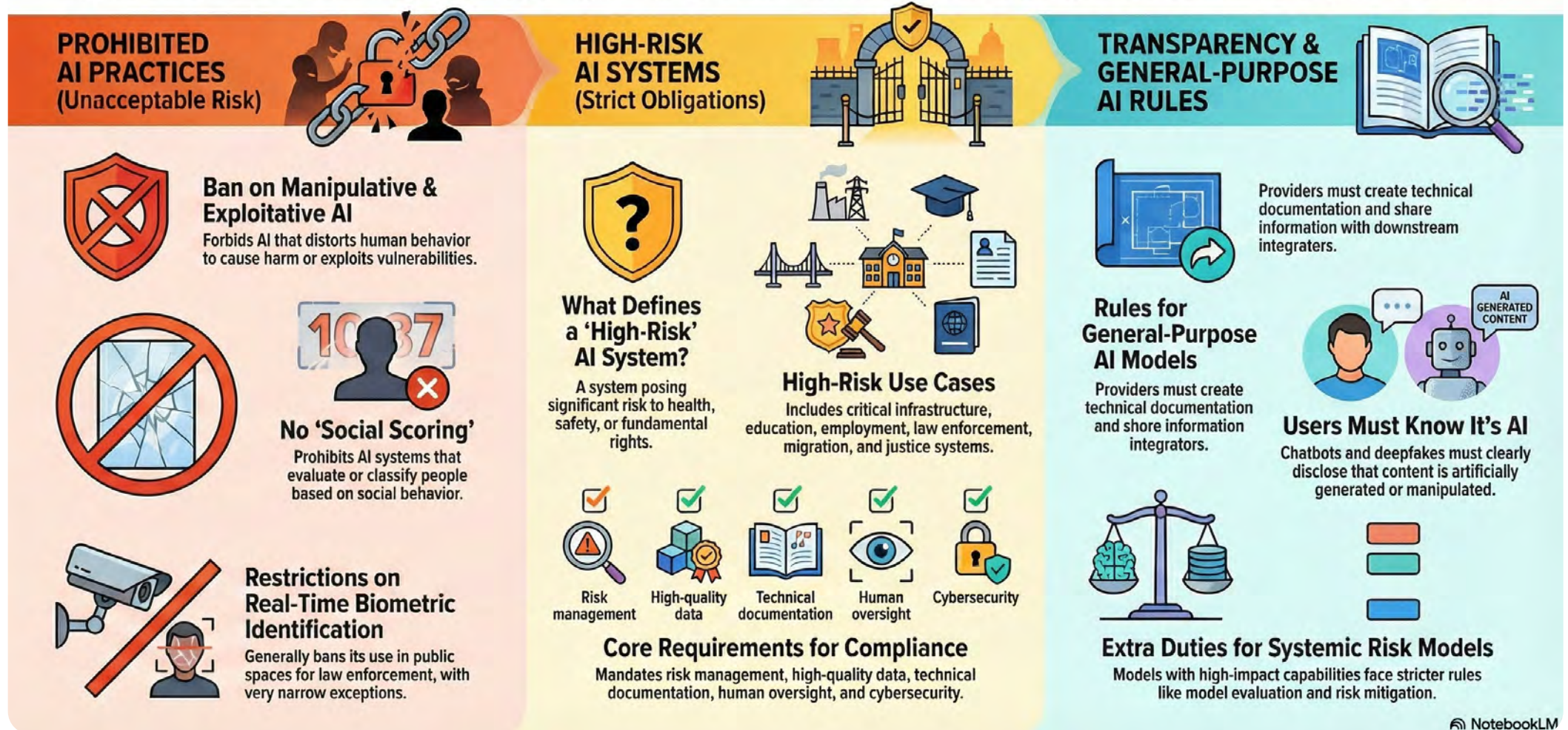


Bild: NotebookLM

NotebookLM



Risikostufen des KI-Gesetzes

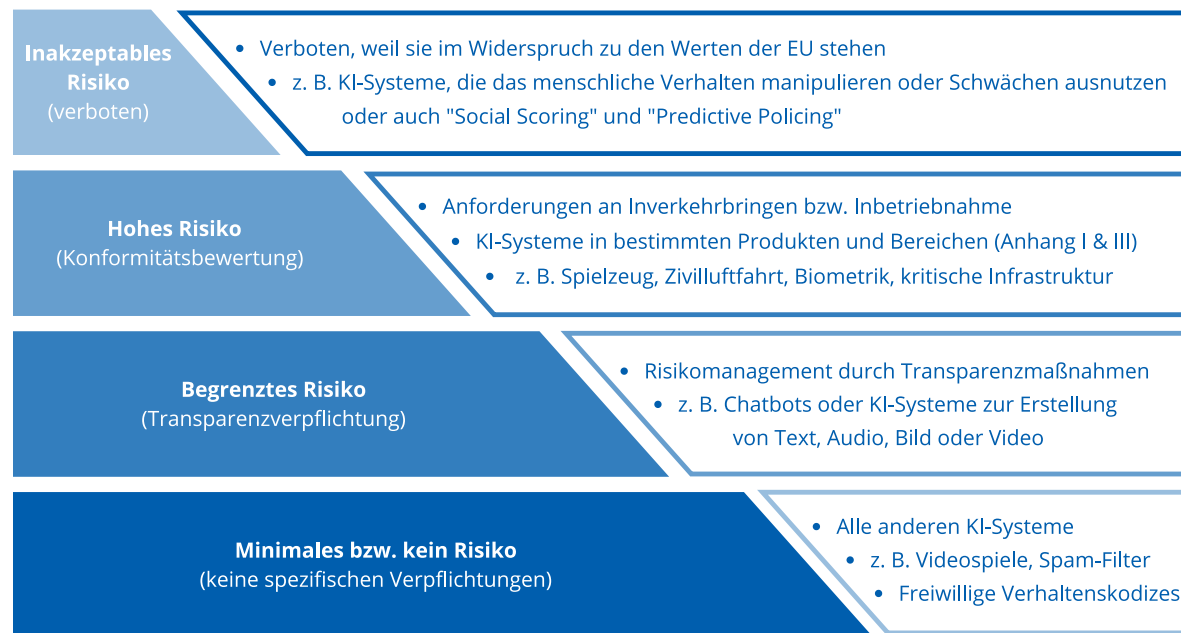
Das KI-Gesetz legt eine **risikobasierte Hierarchie** mit vier Hauptstufen fest:



Risikostufen des KI-Gesetzes

AI Act: Risikostufen für KI-Systeme

Nicht alle KI-Systeme fallen in den regulierten Bereich - je höher das Risiko, desto strikter die Regeln



KI-Servicestelle

ki.rtr.at



Bild: RTR: Risikostufen des KI-Gesetzes¹



AI Act: Verpflichtungen von Anbietern

Der Umfang der Verpflichtungen nimmt entsprechend der Risikoklassifizierung des KI-Systems/KI-Modells ab

	Hochrisiko KI-System	GPAI-Modell system. Risiko	GPAI-Modell	KI-System begrenzt. Risiko	KI-System minimal. Risiko
KI-Kompetenz	Art. 4	Art. 4	Art. 4	Art. 4	Art. 4
Transparenz gegenüber nachgelagerten Akteuren	Art. 13	Art. 55 (1)	Art. 53 (1) b	Art. 50 (1), (2)	
Anforderungen an Daten	Art. 10	Art. 55 (1)	Art. 53 (1) c, d		
Technische Dokumentation	Art. 11	Art. 55 (1)	Art. 53 (1) a		
Zusammenarbeit mit Behörden	Art. 21	Art. 55 (1)	Art. 53 (3)		
Benennung Bevollmächtigter (sofern Drittstaat)	Art. 22	Art. 55 (1)	Art. 54		
Risikomanagement	Art. 9	Art. 55 (1) a, b			
Genauigkeit, Robustheit und Cybersicherheit	Art. 15	Art. 55 (1) d			
Registrierungs- bzw. Mitteilungspflichten	Art. 49	Art. 52 (1)			
Meldepflichten gegenüber Behörden	Art. 73	Art. 55 (1) c			
Aufzeichnung von Ereignissen	Art. 12				
Implementierung menschlicher Überwachungstools	Art. 14				
Kennzeichnungspflichten	Art. 16 b				
Sicherstellung der Barrierefreiheitsanforderungen	Art. 16 l				
Qualitätsmanagement	Art. 17				
Aufbewahrungspflichten	Art. 18, 19				
Korrekturmaßnahmen	Art. 20				
Konformitäts-Bewertungsverf., -Erklärung, -Kennzeichnung	Art. 43, 47, 48				

KI-Servicestelle

ki.rtr.at



Bild: RTR: Anbieterpflichten¹



AI Act: Verpflichtungen von Betreibern

Der Umfang der Verpflichtungen nimmt entsprechend der Risikoklassifizierung des KI-Systems ab

	Hochrisiko KI-System	KI-System begrenzt. Risiko	KI-System minimal. Risiko
KI-Kompetenz	Art. 4	Art. 4	Art. 4
Transparenz gegenüber nachgelagerten Akteuren	Art. 26 (11)	Art. 50 (3), (4)	
Verwendung des KI-Systems laut Betriebsanleitung	Art. 26 (1), (3), (4)		
Menschliche Aufsicht	Art. 26 (2)		
Überwachung des KI-Systems	Art. 26 (5)		
Meldung von schwerwiegenden Vorfällen	Art. 26 (5), 73		
Aufbewahrung von erzeugten Protokollen	Art. 26 (6)		
Sofern relevant, Datenschutz-Folgenabschätzung	Art. 26 (9)		
Zusammenarbeit mit zuständigen nationalen Behörden	Art. 26 (12)		
Recht auf Erläuterung der Entscheidungsfindung im Einzelfall	Art. 86 (1)		
Informationspflichten gegenüber der Arbeitnehmer:innen-Vertretung <i>sofern Arbeitgeber:in Hochrisiko-KI-Systeme am Arbeitsplatz einsetzt</i>	Art. 26 (7)		
Registrierungspflicht <i>sofern EU-Organe, EU-Einrichtungen und sonstige EU-Stellen</i>	Art. 26 (8), 49		
Genehmigungspflicht einer Justiz- oder Verwaltungsbehörde <i>sofern Einsatz zur nachträglichen biometrischen Fernidentifizierung</i>	Art. 26 (10)		
Erstellung einer Grundrechte-Folgenabschätzung <i>sofern u. a. öffentl. oder private Einrichtungen öffentliche Dienste erbringen</i>	Art. 27		

KI-Servicestelle

ki.rtr.at



Bild: RTR: Betreiberpflichtungen¹



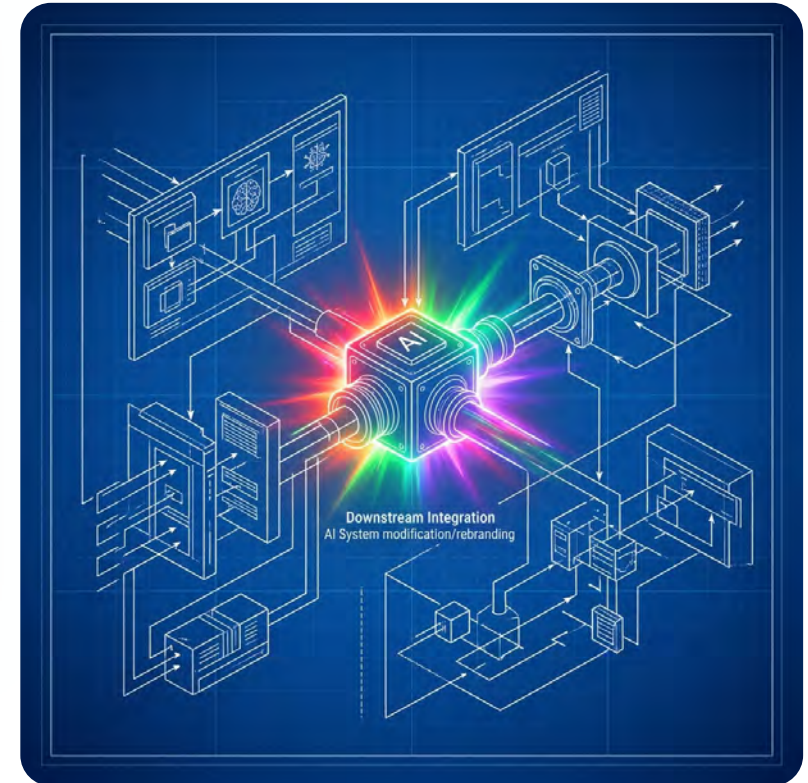
Nachgelagerte Anbieter

Verantwortlichkeiten (Art. 25)

Ketten-Haftung / Pflichtenübertragung

Dritte (Händler, Einführer, Betreiber etc.) gelten als **Anbieter eines Hochrisiko-KI-Systems** und unterliegen den vollen Anbieterpflichten (Art. 16), wenn sie:

- a) das System mit ihrem Namen oder ihrer Handelsmarke versehen.
- b) eine wesentliche Veränderung eines Hochrisiko-KI-Systems vornehmen.
- c) die Zweckbestimmung eines nicht-hochriskanten Systems so verändern, dass es als hochriskant eingestuft wird.



AI-generated

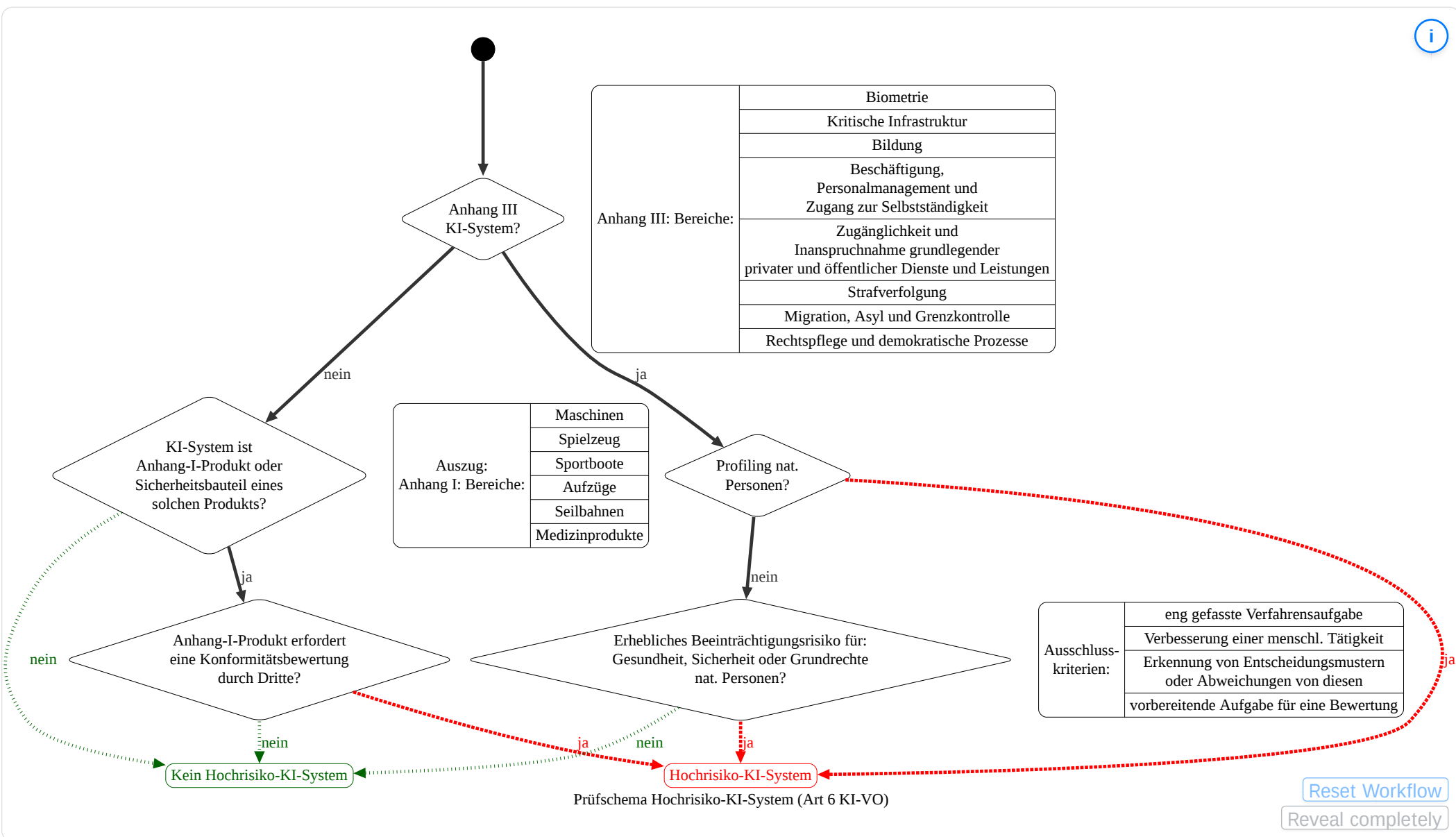


PROHIBITED AI PRACTICES



AI-generated

Was ist hochriskant?



Hochrisiko-KI: „Filter“

Artikel 6(3) befreit Anhang-III-Systeme, wenn sie Entscheidungen **nicht wesentlich beeinflussen**.

RIEGEL: PROFILING

Filter gilt **nie** bei **Profiling** (Bewertung persönlicher Aspekte gemäß DSGVO).

01

Prozedural

Vorgegebene Prozesse.

Z.B. Sortierung, Formatkonvertierung oder Dublettensuche ohne eigene Bewertung.

02

Verbesserung

Ergebnisoptimierung.

Z.B. ex-post Fehlerprüfung oder Rechtschreibprüfung ohne inhaltliche Änderung.

03

Abweichungsprüfung

Mustererkennung.

Z.B. Notenanomalien. Ex-post Vergleich, der eine menschliche Prüfung erfordert.

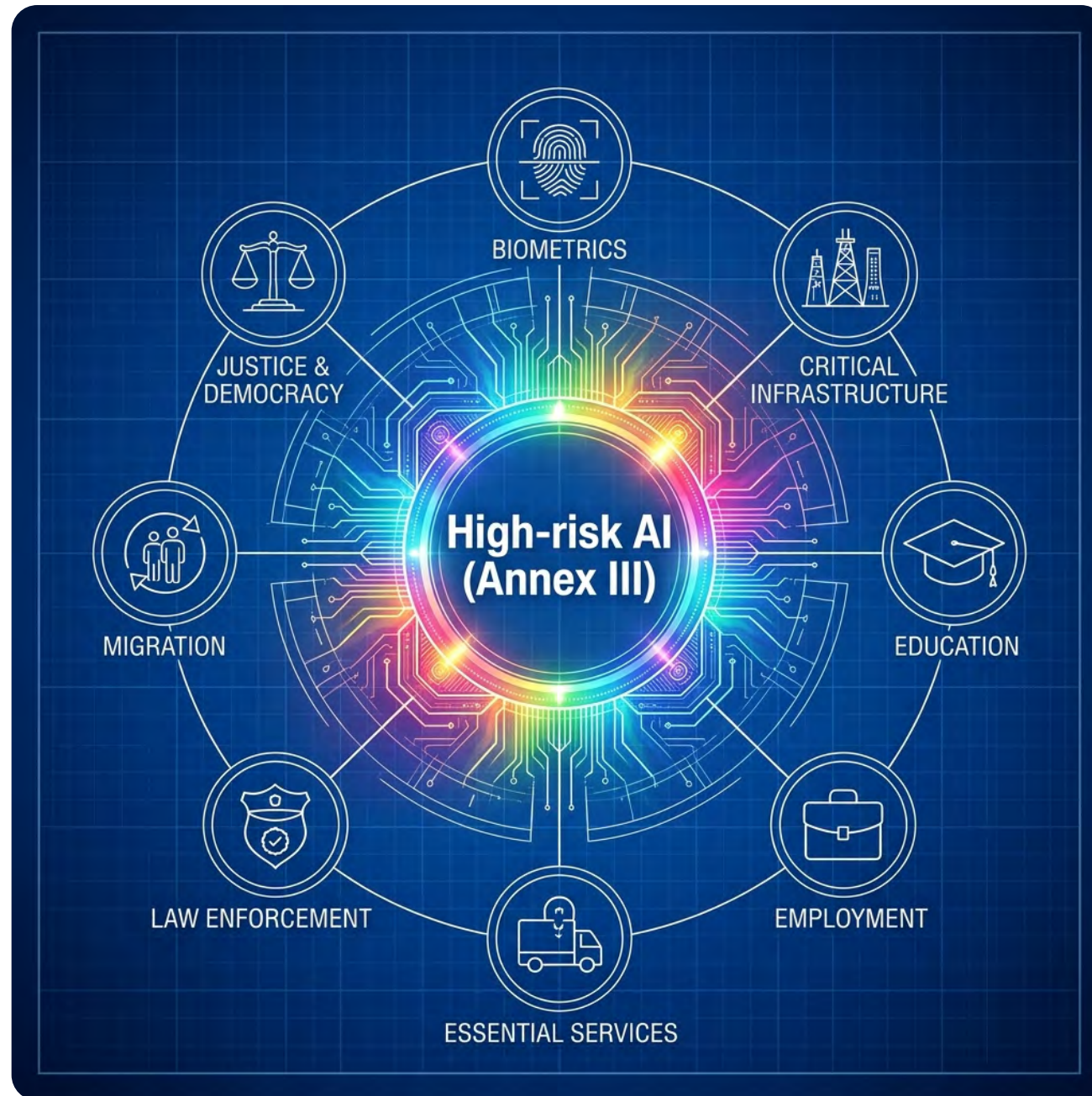
04

Vorbereitung

Zuarbeit vor Prüfung.

Z.B. Indexierung oder Gesetzesrecherche. Nur allgemeine Faktoren, keine Empfehlungen.





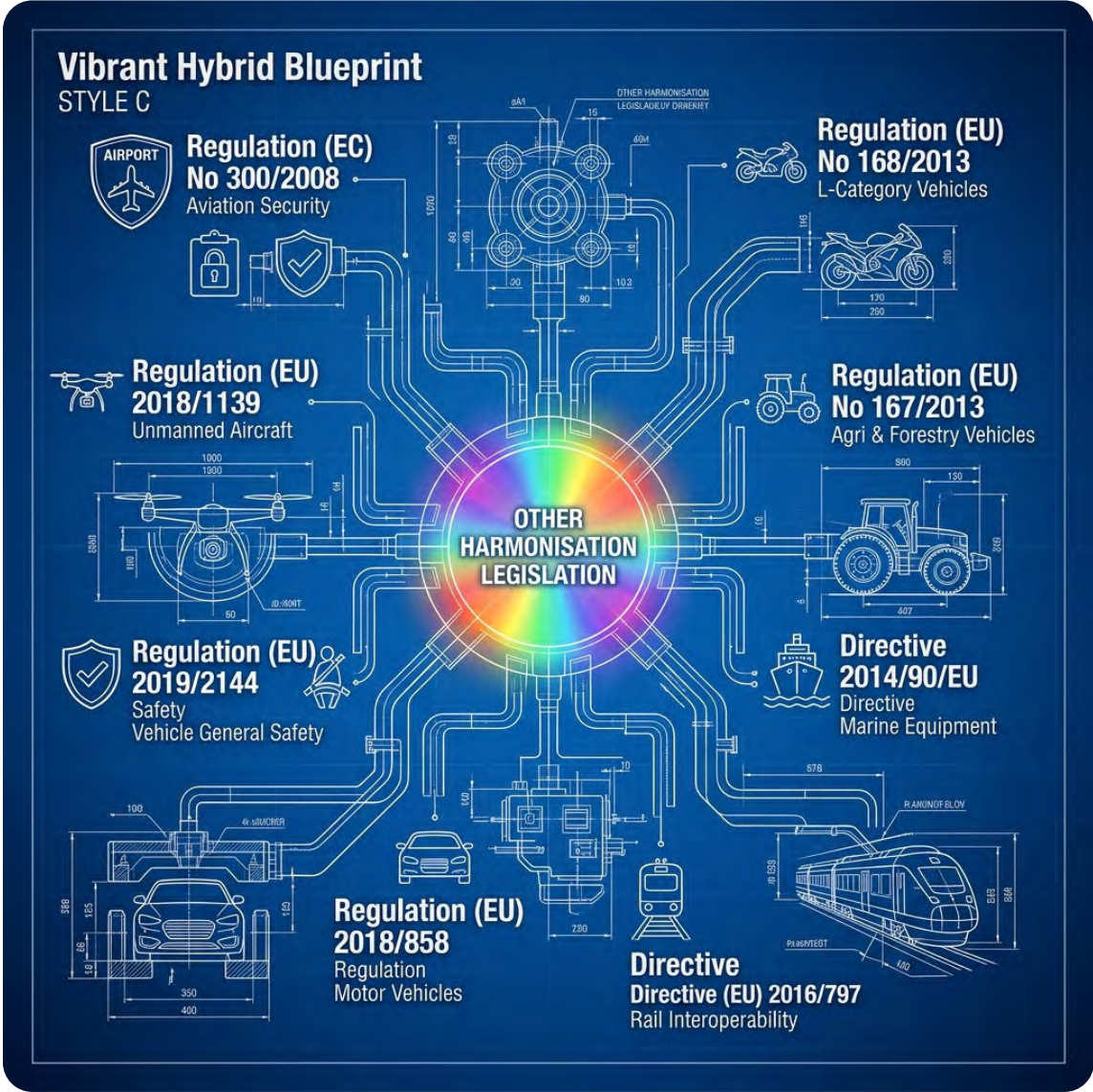
AI-generated

AI Act Annex I



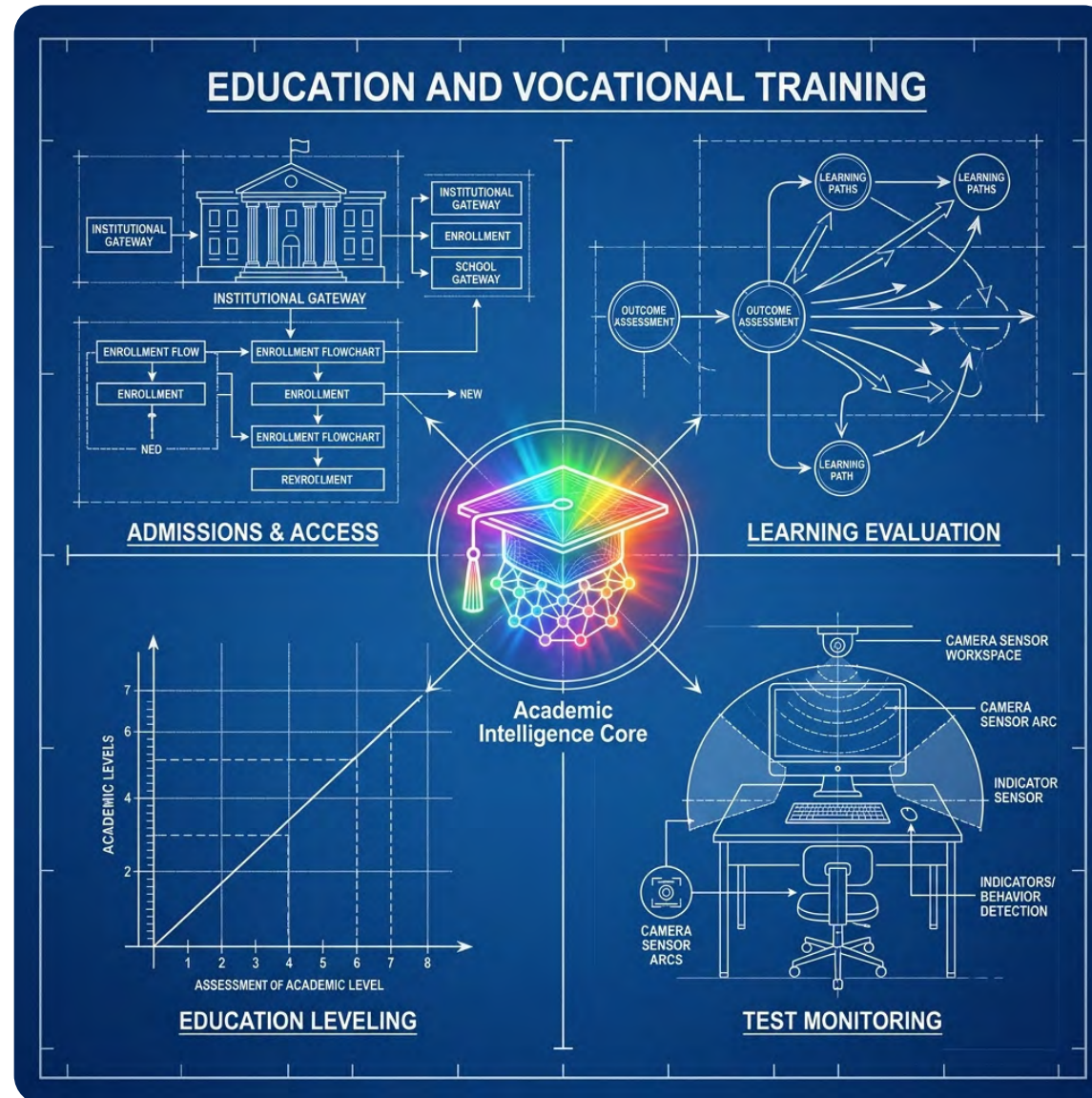
AI-generated

AI Act Annex I



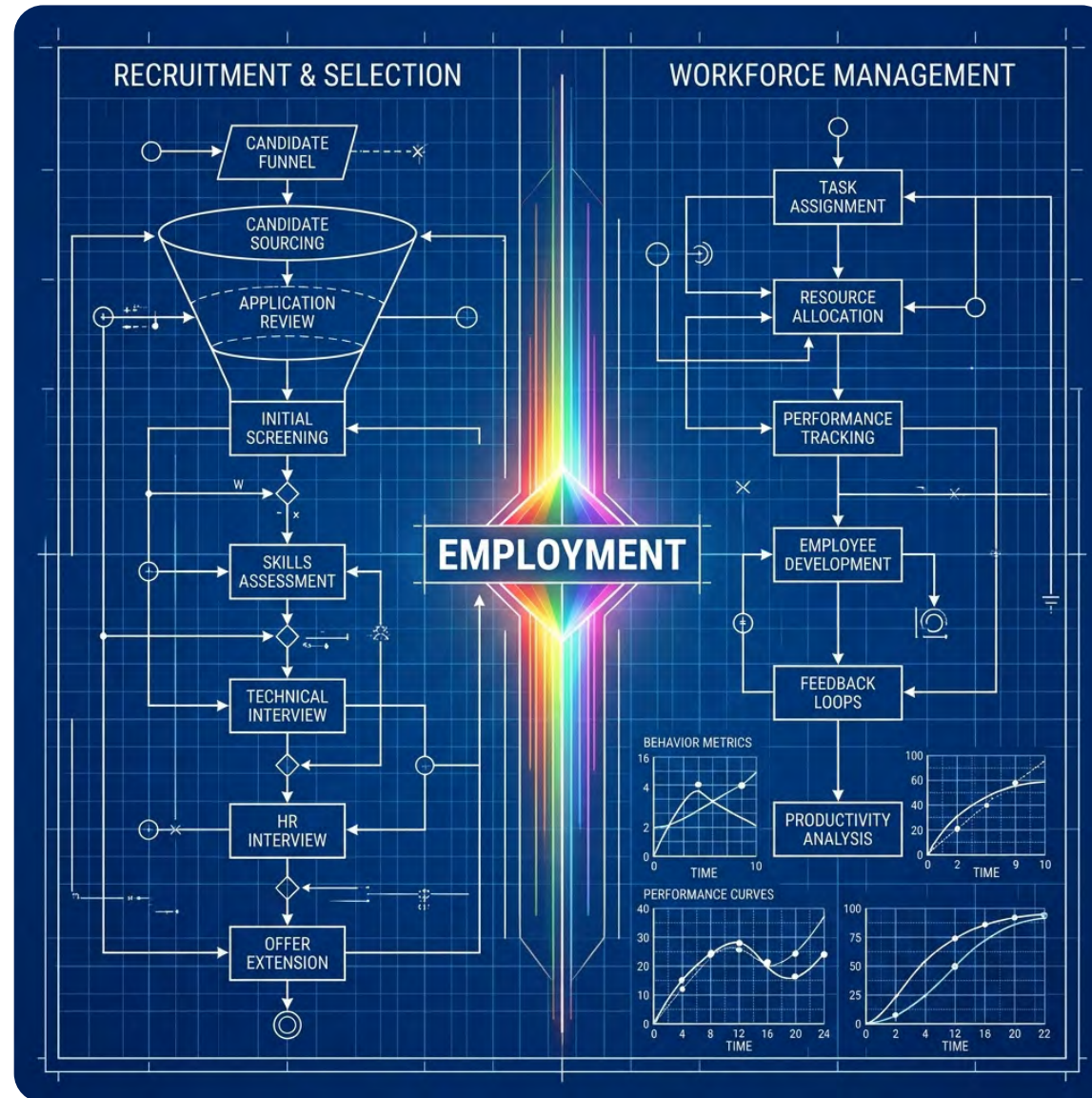
AI-generated

KI im Bildungsbereich = hochriskant



AI-generated

KI im Personalbereich = hochriskant



AI-generated

KI-System

Art 3 Z 1 KI-VO



1. System & Autonomie

Ein **maschinengestütztes System**, das für einen unterschiedlich großen Grad an **Autonomie** konzipiert ist und nach der Inbetriebnahme **anpassungsfähig** sein kann.



2. Ziele & Ableitung

Leitet aus erhaltenen **Eingaben** für explizite oder implizite **Ziele** Ergebnisse ab:

Vorhersagen

Inhalte

Empfehlungen

Entscheidungen



3. Wirkung

Ergebnisse, welche die physische oder virtuelle **Umgebungen beeinflussen können**.

Physisch

Virtuell

KI-System

Art 3 Z 1 KI-VO



1. System & Autonomie

Ein **maschinengestütztes System**, das für einen unterschiedlich großen Grad an Autonomie konzipiert ist und nach der Inbetriebnahme anpassungsfähig sein kann.



2. Ziele & Ableitung

Leitet aus erhaltenen **Eingaben** für explizite oder implizite **Ziele** Ergebnisse ab:

Vorhersagen

Inhalte

Empfehlungen

Entscheidungen



3. Wirkung

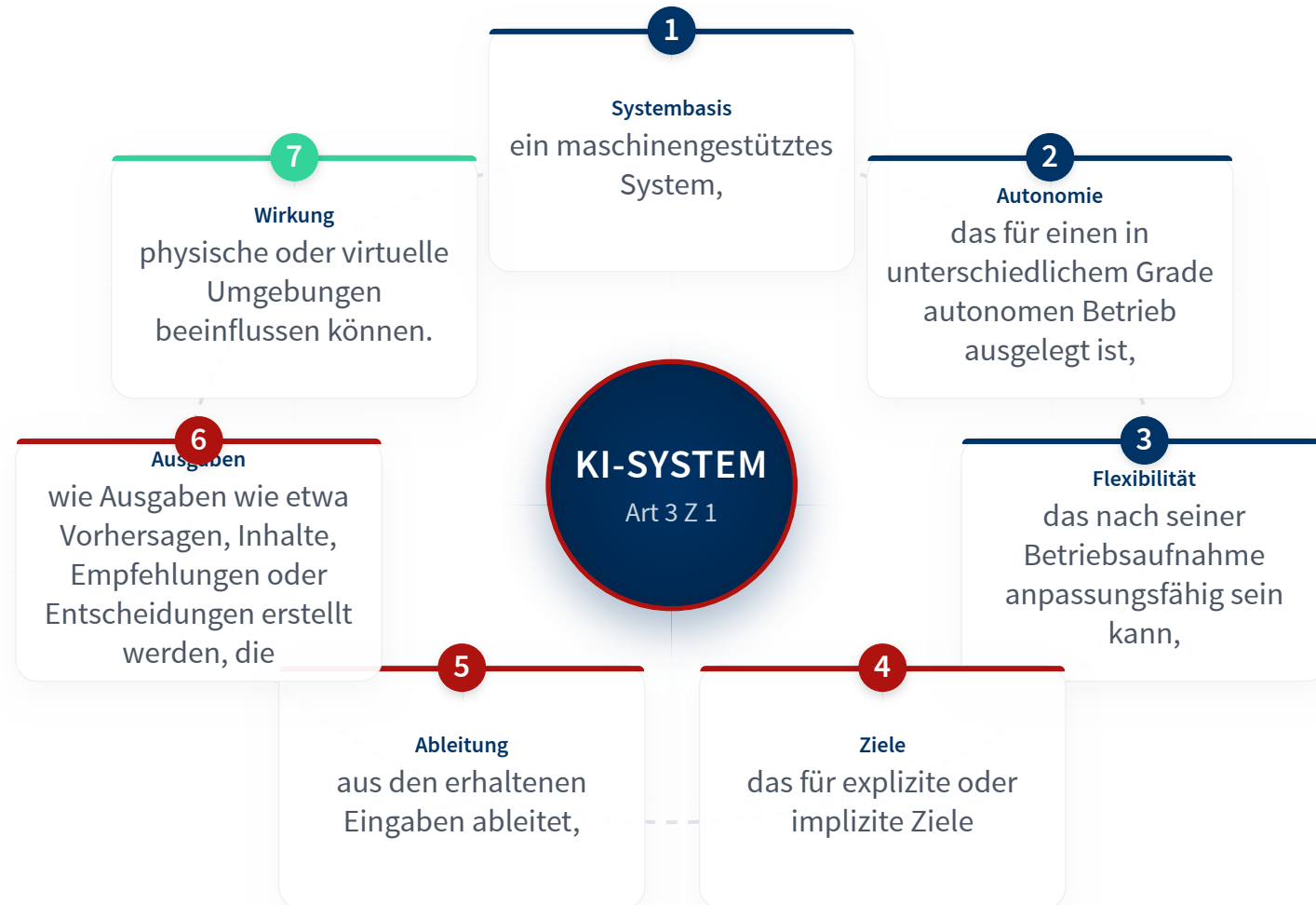
Ergebnisse, welche die physische oder virtuelle **Umgebungen beeinflussen können**.

Physisch

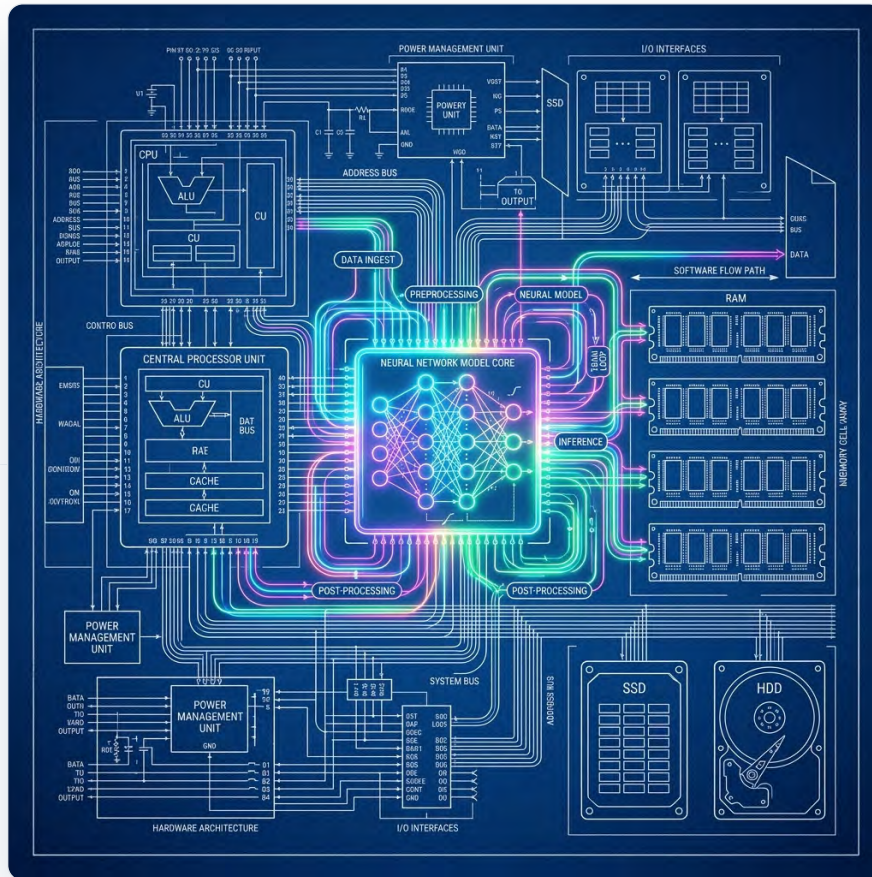
Virtuell

KI-System

Die 7 Elemente der KI-System-Definition



Maschinengestützt



Gemini

1. Hardware & Software

Umfasst sowohl die physische Recheninfrastruktur (Prozessoren, Arbeitsspeicher, Massenspeicher, Netzwerkadapter, Schnittstellen) als auch die steuernde Software (Computercode, Betriebssysteme und Anwendungen).

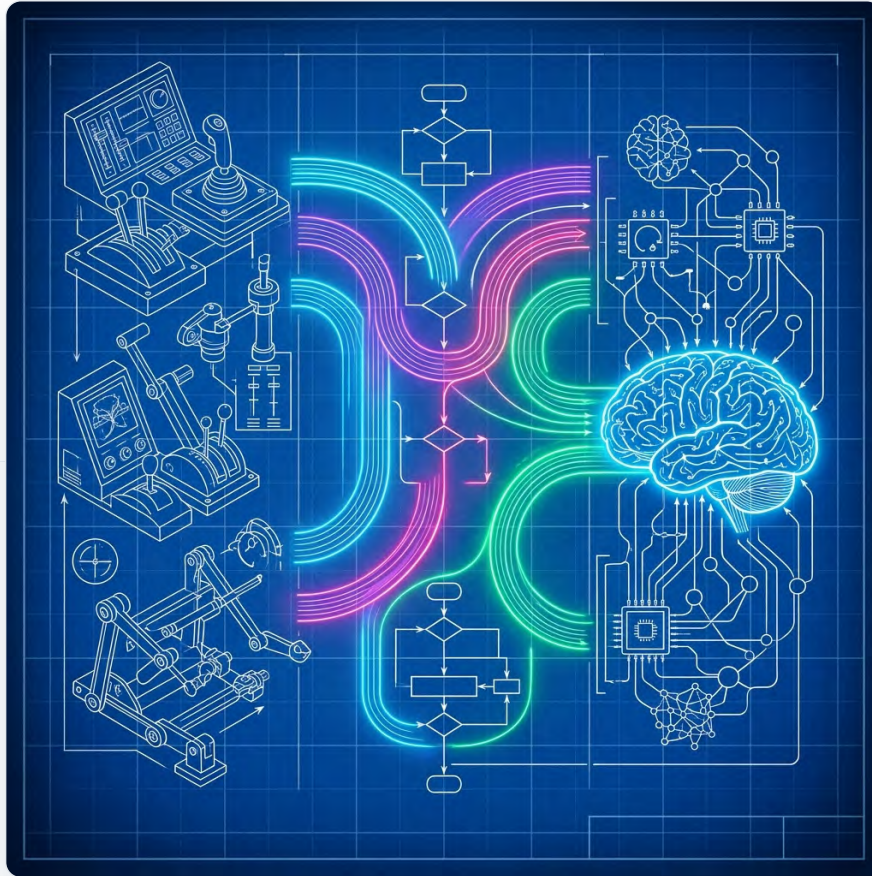
2. Systemischer Lebenszyklus

KI-Systeme basieren zwingend auf maschinellen Vorgängen. Rechnergesteuerte Abläufe steuern den gesamten Lebenszyklus – vom Modelltraining über die Datenverarbeitung bis zur Ausführung von Vorhersagen oder Entscheidungen.

3. Technologieneutralität

Die Definition erfasst eine große Bandbreite von Rechensystemen. Auch neuartige Technologien wie fortschrittliche Quantencomputer sind maschinengestützt, sofern sie klassische oder neuartige Rechenkapazitäten bereitstellen.

Autonomie



Gemini

1. Spektrum der Interaktion

Die Spanne reicht von vollständiger manueller Kontrolle bis zu vollständiger Autonomie. Ausgenommen sind Systeme, die ausschließlich unter permanentem, manuellem menschlichen Zutun operieren.

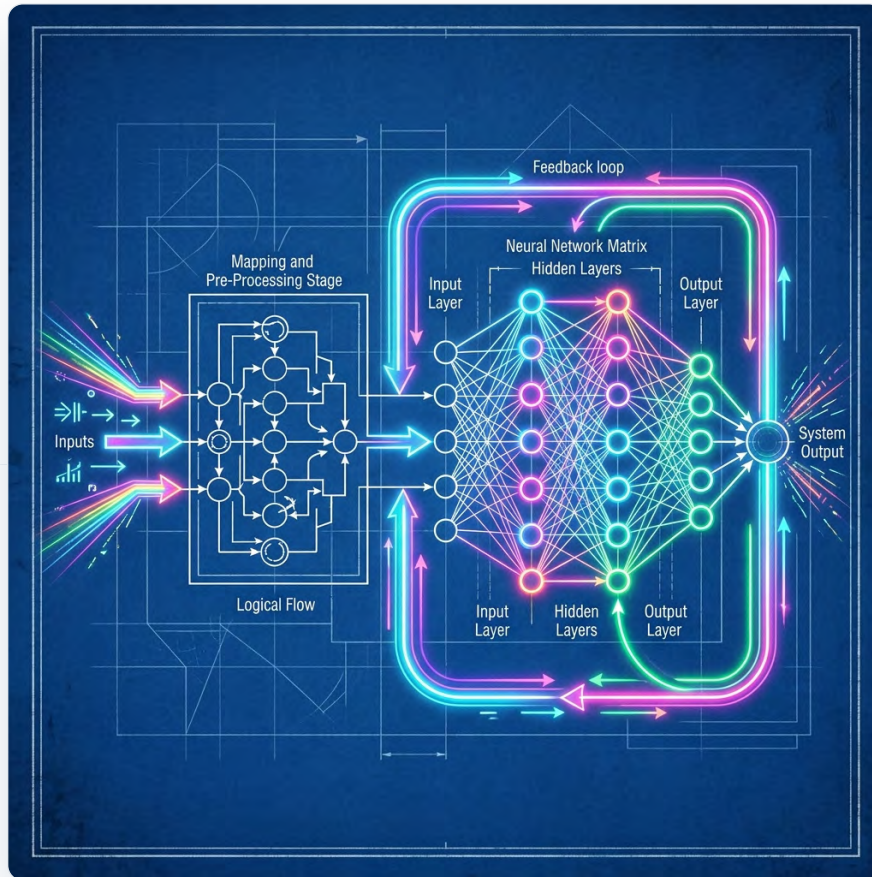
2. Unabhängiges Agieren

Ein System agiert autonom, wenn es nach Erhalt einer Eingabe eigenständig Ausgaben (wie Empfehlungen oder Vorhersagen) erzeugt, ohne dass diese Ausgaben von einem Menschen exakt und im Voraus vordefiniert werden.

3. Externe Interaktion

Entscheidend für die Autonomie ist die Fähigkeit des Systems, mit seinem externen Umfeld zu interagieren und dieses zu beeinflussen, anstatt bloß eine bestimmte mathematische Modelltechnik einzusetzen.

Anpassungsfähigkeit



Gemini

1. Definition & Lernfähigkeit

Bezieht sich auf die Lernfähigkeit des Systems nach der Inbetriebnahme. Das System kann sein Verhalten während der Verwendung so verändern, dass dieselben Eingaben zu anderen Ausgaben führen als zuvor.

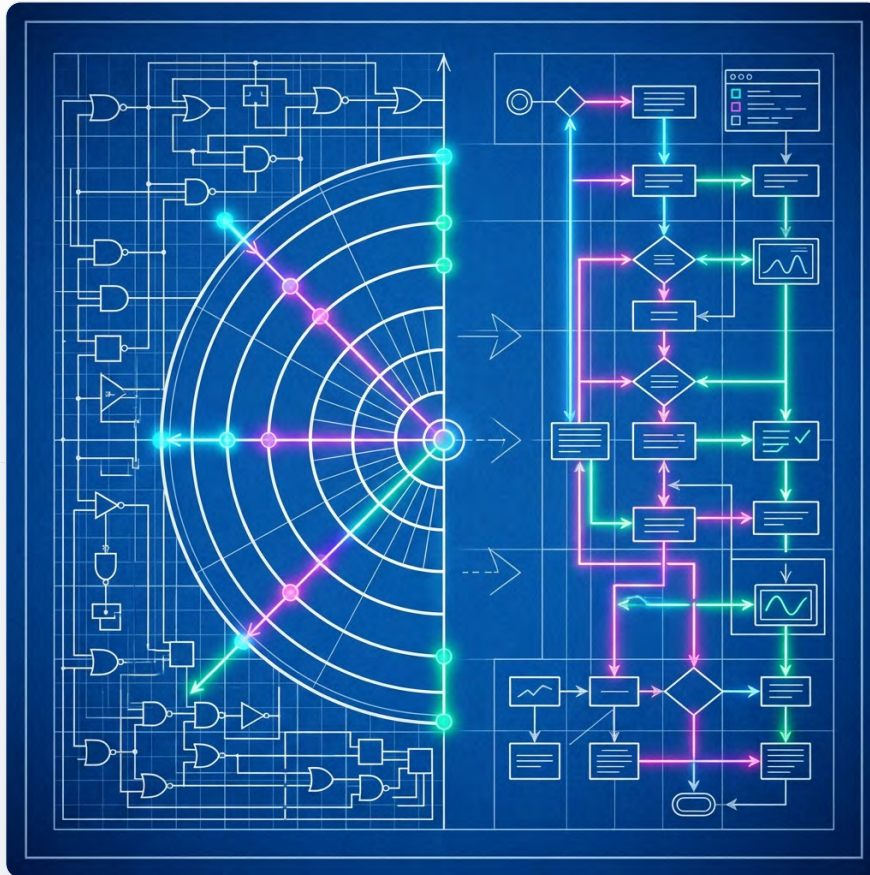
2. Abgrenzung zur Autonomie

Autonomie und Anpassungsfähigkeit sind eng verknüpft, stellen jedoch unterschiedliche funktionale Dimensionen dar. Ein System kann autonom agieren, ohne nach Inbetriebnahme zwingend sein Verhalten anzupassen.

3. Fakultativer Charakter

Die **Anpassungsfähigkeit** nach Betriebsaufnahme ist laut Verordnungstext **optional** („kann anpassungsfähig sein“). Ein automatisches Weiterlernen nach Inbetriebnahme ist somit keine zwingende Voraussetzung für die Einstufung.

Systemziele & Zweck



Gemini

1. Explizite & Implizite Ziele

Ziele können explizit programmiert sein (z. B. Kostenfunktionen, Wahrscheinlichkeiten) oder sich implizit aus Trainingsdaten und Interaktionen mit der Systemumgebung ableiten.

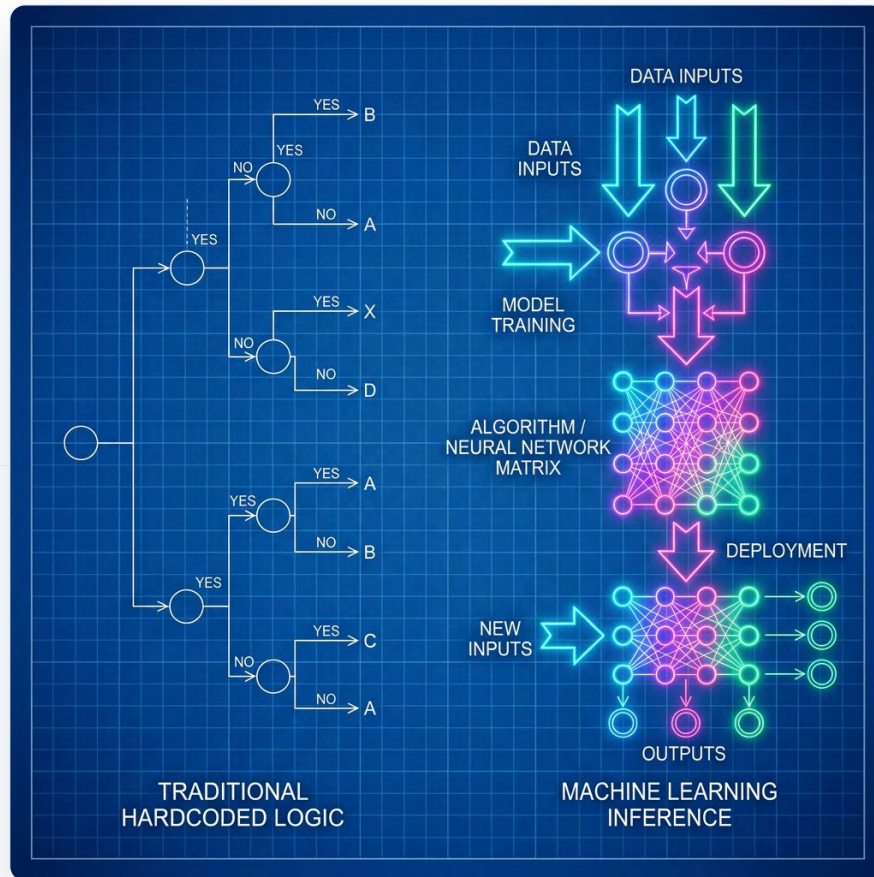
2. Systeminterne Natur

Ziele beziehen sich direkt auf das Verhalten des Systems bei seinen Aufgaben und sind rein systemintern ausgerichtet (z. B. die Optimierung von Antwortgenauigkeiten).

3. Externe Zweckbestimmung

Im Gegensatz dazu ist die Zweckbestimmung nach außen gerichtet. Sie definiert den Kontext, in dem das System eingesetzt werden soll (z. B. Unterstützung einer Abteilung).

Fähigkeit zur Ableitung



Gemini

1. Kernmerkmal der Ableitung

Die Fähigkeit zur Ableitung grenzt KI-Systeme von herkömmlichen Softwaresystemen ab. KI-Systeme basieren nicht auf ausschließlich von Menschen definierten, starren Wenn-Dann-Regeln zur Ausführung von Operationen.

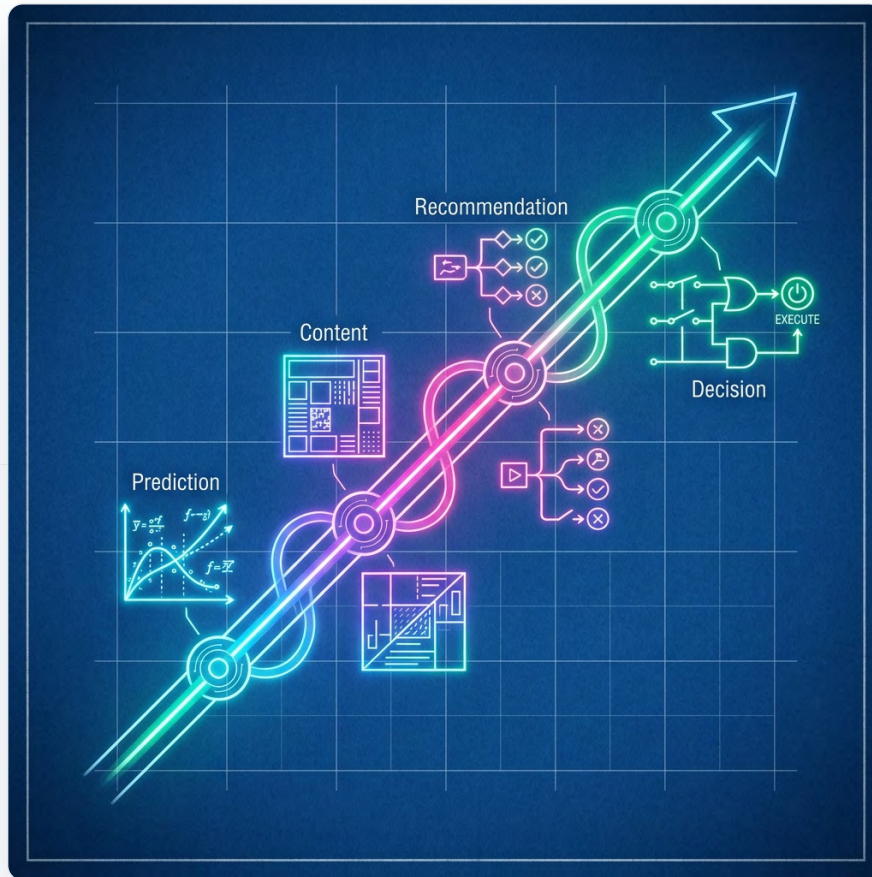
2. Zwei funktionale Phasen

Die Ableitung betrifft zwei Ebenen: Die **Aufbauphase** (selbstständige Ableitung des Algorithmus/Modells aus Daten) und die **Nutzungsphase** (Erzeugung konkreter Ausgaben basierend auf neuen Eingaben).

3. Weites Begriffsverständnis

Das Gesetz versteht Ableitung sehr breit. Es umfasst nicht nur das bloße Errechnen eines Ergebnisses, sondern den gesamten datengetriebenen Prozess, durch den das System lernt, wie Ausgaben erzeugt werden.

Systemausgaben & Einfluss



Gemini

1. Die vier Ausgabenkategorien

Das Gesetz unterscheidet vier Kategorien: **Vorhersagen** (Schätzung unbekannter Werte), **Inhalte** (generativ erzeugte Medien), **Empfehlungen** (Vorschläge) und **Entscheidungen** (automatisierte Auswahlen).

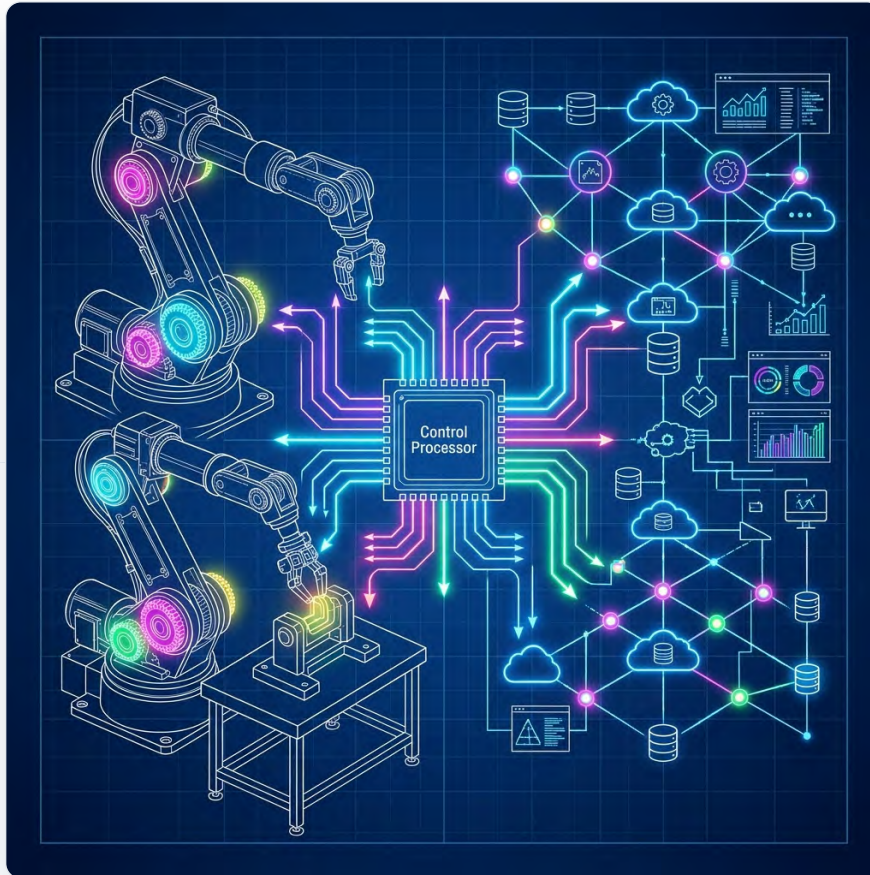
2. Grad des menschlichen Zutuns

Die Klassen unterscheiden sich im Automatisierungsgrad. Empfehlungen (z. B. in HR-Systemen) werden oft von Menschen bewertet. Werden sie direkt umgesetzt, werden sie zu vollautomatisierten Entscheidungen.

3. Beeinflussung von Umgebungen

Die Ausgaben müssen physische oder virtuelle Umgebungen beeinflussen können. KI-Systeme beherrschen hier hochdynamische Szenarien (wie autonomes Fahren), bei denen rein regelbasierte Programme scheitern.

Interaktion mit der Umgebung



Gemini

1. Aktive Beeinflussung

Das Kriterium verlangt, dass Ausgaben Umgebungen beeinflussen können. KI-Systeme agieren aktiv und gestaltend in ihrer jeweiligen Einsatzumgebung; sie verhalten sich nicht passiv.

2. Physische Umgebungen

Die Beeinflussung kann materielle Objekte betreffen. Typische Beispiele sind Roboterarme in der Fertigung, autonome Fahrzeuge oder physische Steuerungssysteme.

3. Virtuelle Umgebungen

Ebenso erfasst sind rein digitale Räume. Hierzu zählen Software-Ökosysteme, automatisierte Datenströme, digitale Plattformen, Social-Media-Feeds und virtuelle Umgebungen.

Quiz

Szenario: Physik-Simulation

Ein System nutzt maschinelles Lernen, um physikalische Simulationen atmosphärischer Prozesse (wie Wolkenmikrophysik oder Turbulenzen) zu beschleunigen und numerisch anzunähern.



Gemini

Stimmen Sie per Handzeichen ab:

* Erhobene Hand: **JA** → Es handelt sich um ein KI-System im Sinne der KI-Verordnung.

Auflösung

! Antwort: NEIN! ✗

Obwohl maschinelles Lernen zum Einsatz kommt, handelt es sich lediglich um die **mathematische Optimierung** bzw. numerische Annäherung physikalischer Modelle. Das System geht nicht über grundlegende Datenverarbeitung hinaus und gilt daher *nicht* als KI-System.¹

Quiz

Szenario: Medizinisches Expertensystem

Ein medizinisches Diagnosesystem stützt sich auf ein komplexes Regelwerk, logische Schlussfolgerungen und strukturiertes Expertenwissen (Expertensystem), das auf Basis von medizinischem Expertenwissen aufgebaut wurde. Es nutzt *kein* maschinelles Lernen.

Stimmen Sie per Handzeichen ab:

* Erhobene Hand: **JA** → Es handelt sich um ein KI-System im Sinne der KI-Verordnung.



Gemini

Auflösung

 Antwort: JA! 

Auch ohne den Einsatz von modernem maschinellen Lernen handelt es sich um ein **logik- und wissensbasiertes System**. Da es unter Verwendung von Expertenregeln autonom Schlussfolgerungen aus Eingaben ableitet, erfüllt es die rechtliche KI-Definition vollständig.¹

Quiz

Szenario: Satelliten-Netzwerkoptimierung

Ein Satelliten-Telekommunikationssystem nutzt Modelle des maschinellen Lernens, um künftigen Netzverkehr vorherzusagen. Darauf aufbauend optimiert es die Zuweisung betrieblicher Hardware-Ressourcen (wie Strom und Bandbreite) für die Satellitentransponder.

Stimmen Sie per Handzeichen ab:

* Erhobene Hand: **JA** → Es handelt sich um ein KI-System im Sinne der KI-Verordnung.



Interaktive Teilnahme

Auflösung

! Antwort: NEIN! ✗

Obwohl maschinelles Lernen zur Verkehrsvorhersage eingesetzt wird, dienen die Selbstanpassungen des Systems ausschließlich dazu, die **Betriebsleistung der Hardware** zu optimieren. Sie ermöglichen keine Anpassung des zugrundeliegenden Entscheidungsmodells. Daher wird das System aus dem Anwendungsbereich ausgeschlossen.¹

Was ist (wahrscheinlich) kein KI-System?¹

- **Einfache Datenverarbeitung:** Fest programmierte Anweisungen ohne Lernprozess (z. B. Excel, Filter).
- **Analysen & Visualisierungen:** Rein beschreibende Statistik (z. B. Diagramme ohne Empfehlungen).
- **Mathematische Optimierung:** Beschleunigung von Modellen (z. B. lineare Regression zur Leistungsumme).
- **Klassische Heuristik:** Regelbasierte Suche oder Trial & Error (z. B. klassische Schach-Engines).
- **Einfache Vorhersagen:** Statische Schätzungen auf Basis historischer Durchschnitte.

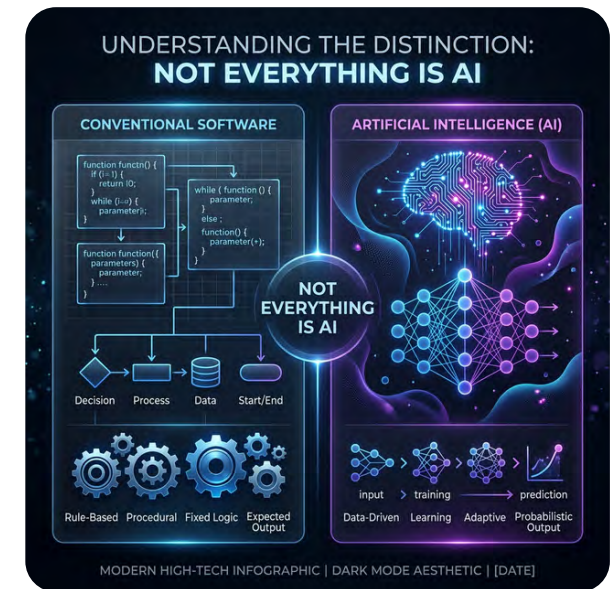
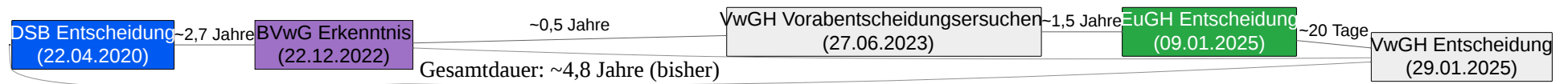
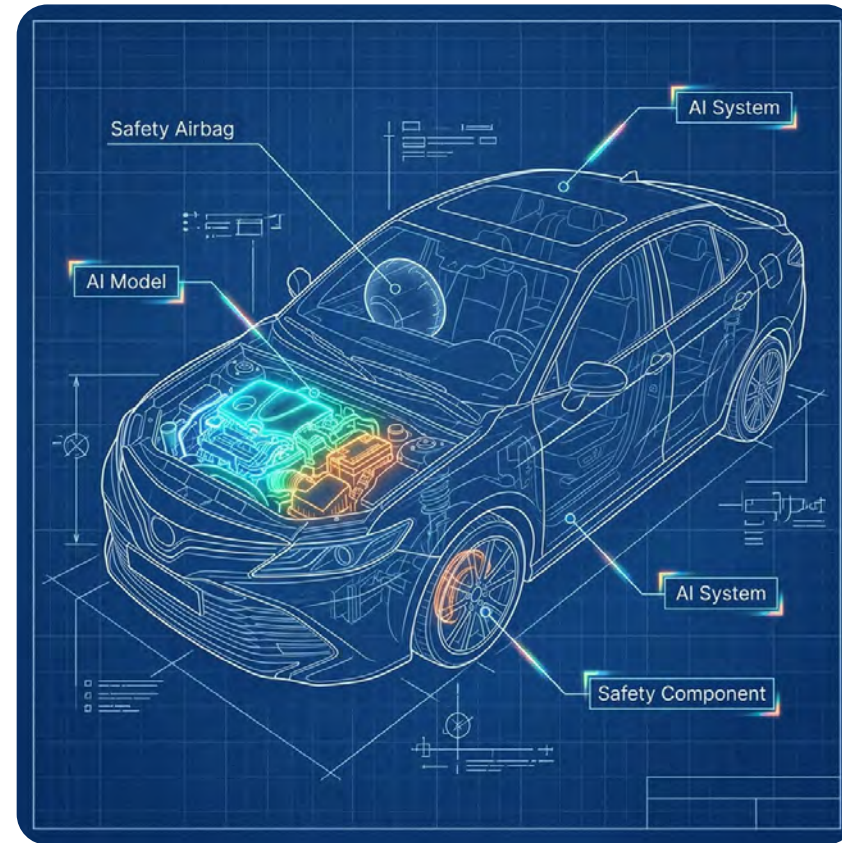


Image: Gemini

Problem rechtlicher Definitionen¹

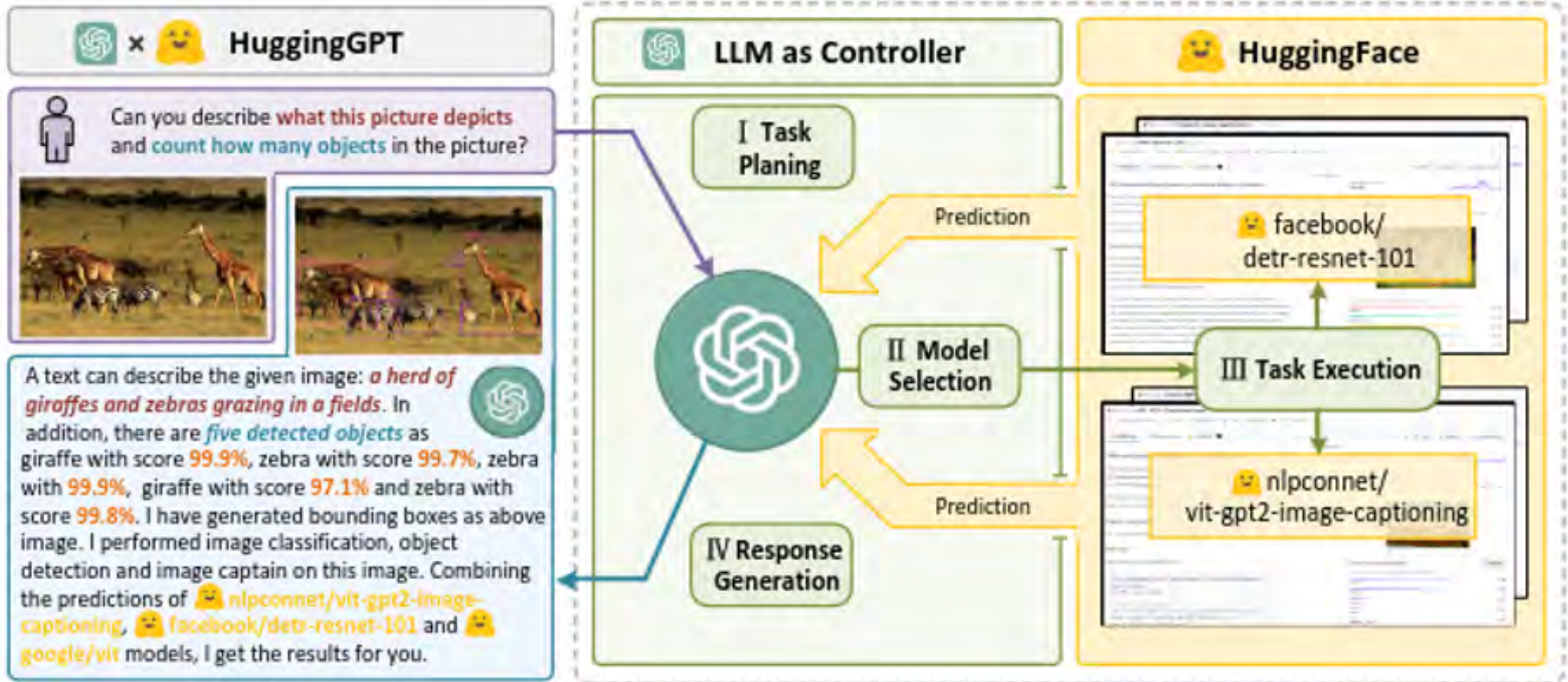


Ein anderer Näherungsversuch



Gemini

Orchestrierung komplexer Aufgaben

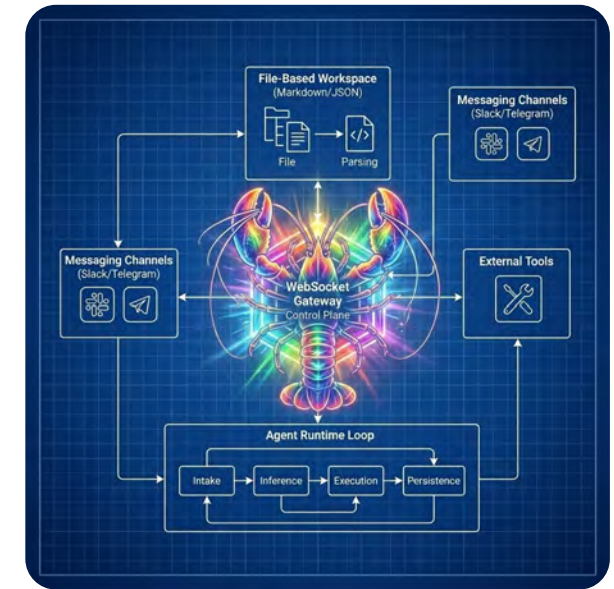


Autonome Agenten-Infrastruktur

Persistent, transparent und lokal-first

OpenClaw ist ein Open-Source-Framework, das LLMs in ausdauernde, autonome KI-Agenten mit eigenem Ausführungskontext verwandelt:

- **Zentraler WebSocket-Gateway (Der “Hummer”)**: Agiert als zentrale Steuerungseinheit (Control Plane), die alle Fäden zieht. Er verwaltet Verbindungen zu Messaging-Plattformen (Slack, Discord, Telegram) und routet Befehle zur Runtime.
- **Agent Runtime (Die Loop-Engine)**: Treibt die kontinuierliche Regelschleife an (Trigger → Kontext → Denkprozess → Tool-Ausführung → Persistenz).
- **File-Based Workspace**: Gedächtnis, Fertigkeiten und System-Prompts liegen transparent als Markdown- und JSON-Dateien auf der Festplatte statt in unlesbaren Datenbanken.
- **Proaktiver “Heartbeat”**: Durch Cron-Jobs kann der Agent eigenständig aufwachen, um proaktiv Mails zu prüfen oder Skripte auszuführen – völlig unabhängig von menschlichem Input.



Gemini

KI-Kompetenz: Gesetzliche Definition

Art. 3 Nr. 56 Basis



Kernkompetenzen

KI-Kompetenz bezeichnet die **Fähigkeiten, Kenntnisse und das Verständnis**, die für einen verantwortungsvollen Umgang mit KI erforderlich sind.

Akteure



Befähigte Akteure

Ermöglicht es **Anbietern, Betreibern und betroffenen Personen**, ihre jeweiligen Rechte und Pflichten im Rahmen der Verordnung wahrzunehmen.

Doppelziel



Zweifacher Zweck

Ermöglicht den **sachkundigen Einsatz** von KI-Systemen und schärft das Bewusstsein für Chancen, Risiken und mögliche Schäden.

AI Literacy: “Ensure” → “Support”

ART 4 AI ACT

Providers and deployers of AI systems shall take measures to ~~ensure, to their best extent, a sufficient level~~ of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

POLITICAL AGREEMENT

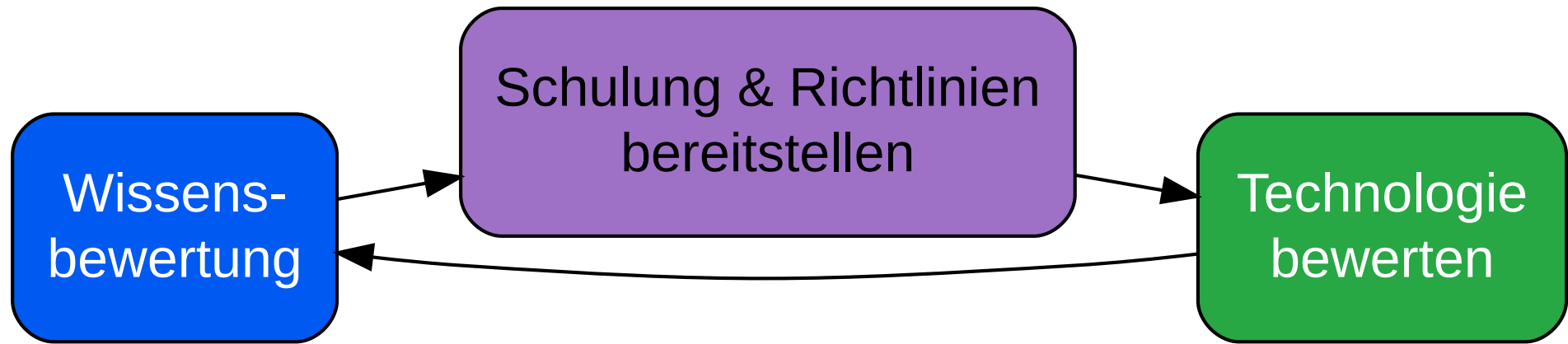
1. Providers and deployers of AI systems shall take measures to support the development of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used. This obligation does not require providers or deployers to guarantee any specific level of AI literacy of any individual.

2. The Commission and the Member States shall support and facilitate the efforts of providers and deployers of AI systems, in particular SMEs, in fulfilling their obligation under paragraph 1 of this Article. For that purpose, the Commission shall publish practical examples of how to comply with that obligation on the single information platform referred to in Article 62(3), point (b).

3. The Board shall adopt recommendations, taking into account European competence frameworks, to support the Commission and Member States in the promotion of AI literacy required under paragraph 1, including by setting out common objectives.

KI-Kompetenz

...ist notwendig, damit Menschen KI-Tools bestmöglich und sicher nutzen können.



KI-Kompetenz: Komponenten

Ein erfolgreiches Schulungsprogramm sollte diese Kerndimensionen abdecken:

Dimension 1



Technisches Wissen

Praktische Anwendung von Tools, Prompt Engineering und Verständnis der Modellfähigkeiten.

Dimension 2



Richtlinien & Regeln

Klare organisatorische **Do's and Don'ts** bezüglich Datenfreigabe und zugelassener Anwendungsfälle.

Dimension 3



Ethisches Bewusstsein

Verständnis von Bias (Verzerrung), Halluzinationsrisiken, potenziellen gesellschaftlichen Schäden und menschlicher Aufsicht.



Transparenz

Systeme ohne hohes Risiko -> oft nur Transparenzpflichten (Art 50 KI-VO):

Anbieter (Providers)



Pflichten der Anbieter

- **Offenlegung der Interaktion:** Nutzer darüber informieren, dass sie mit einer KI interagieren.
- **Wasserzeichen:** Kennzeichnung von KI-generierten Audio-, Bild-, Video- oder Textdateien in einem maschinenlesbaren Format.

Betreiber (Deployers)



Pflichten der Betreiber

- **Biometrische Systeme:** Nutzer informieren, wenn Emotionserkennung oder biometrische Kategorisierung aktiv ist.
- **Deepfakes / Text:** Offenlegung von Deepfakes und KI-generierten Texten von öffentlichem Interesse.



Praktische Transparenzbeispiele

Audio



Audio-Offenlegung

- **Kurz (<30s):** Spoken Warning oder akustisches Signal direkt zu Beginn.
- **Länger:** Wiederholter Hinweis zu Beginn, in der Mitte und am Ende.
- **UI-Sync:** Visuelles „KI“-Symbol auf dem Gerätebildschirm, falls vorhanden.

Video & Streams



Video & Streams

- **Echtzeit:** Dauerhaftes Symbol oder regelmäßige Warnhinweise.
- **Kurzvideo:** Statisches Visual-Label dauerhaft eingeblendet.
- **Langvideo:** Wiederholt zu Beginn, nach Pausen und im Abspann.

Text



Text & Provenienz

- **Publikationen:** Label oben, nahe der Überschrift oder im Impressum.
- **Kurztexte:** UI-Indikatoren oder Hinweis auf Sitzungsebene.
- **Freitext:** Vom Anbieter signiertes, exportierbares Herkunftsmanifest.

Kunst



Ausnahmen & Kunst

- **Kunst/Satire:** Offenlegung darf die Rezeption nicht stören.
- **Kreativ-Video:** 5s Ecksymbol zu Beginn oder Hinweis im Abspann.
- **Physisch:** Aushang am Eingang, Broschüren oder beim Ticketkauf.



KI-Kennzeichnungsvorschlag¹



Figure 1: Sample icon developed by the European Commission (left) with variations against a background (right).



Figure 2: Sample icon developed by the European Commission (left) with variations against a background (right).

Bontcheva et al.²

Der zweite Entwurf des Verhaltenskodex definiert standardisierte visuelle Symbole zur Kennzeichnung von KI-Inhalten:

- **Kontrast & Anpassbarkeit:** Vorgabe von Hell-auf-Dunkel- und Dunkel-auf-Hell-Varianten für optimale Lesbarkeit auf unterschiedlichen Hintergründen (z. B. Farbverläufen).
- **Platzierung:** Dauerhaftes Overlay bei kurzen Videos/Bildern oder periodische Einblendung bei langen Beiträgen.

Note

Einheitliche Symbole sollen eine plattformübergreifende und intuitive Erkennbarkeit von KI-generierten Medien in der gesamten EU gewährleisten.



AI-Office Leitlinien¹

ART. 50(1)



Interaktive KI

- **Pflicht:** Nutzer informieren, dass sie mit KI interagieren (z. B. Chatbots, Sprachassistenten).
- **Zeitpunkt:** Spätestens zum Zeitpunkt der ersten Interaktion.
- **Ausnahme:** Offensichtliche Interaktion für einen vernünftigen, aufmerksamen Nutzer.

ART. 50(2)



Kennzeichnung

- **Pflicht:** Ausgaben maschinenlesbar markieren und Erkennbarkeit gewährleisten.
- **Qualität:** Lösungen müssen effektiv, robust, zuverlässig & interoperabel sein.
- **Ausnahme:** Hilfs-/ Editierwerkzeuge; keine semantische Änderung der Eingabedaten.

ART. 50(3)



Biometrie & Emotionen

- **Pflicht:** Betreiber müssen Personen über den Einsatz der Systeme informieren.
- **Bereich:** Gilt unabhängig von Echtzeit- oder Ex-post-Betrieb.
- **Ausnahme:** Gesetzlich zugelassen für Strafverfolgungszwecke.

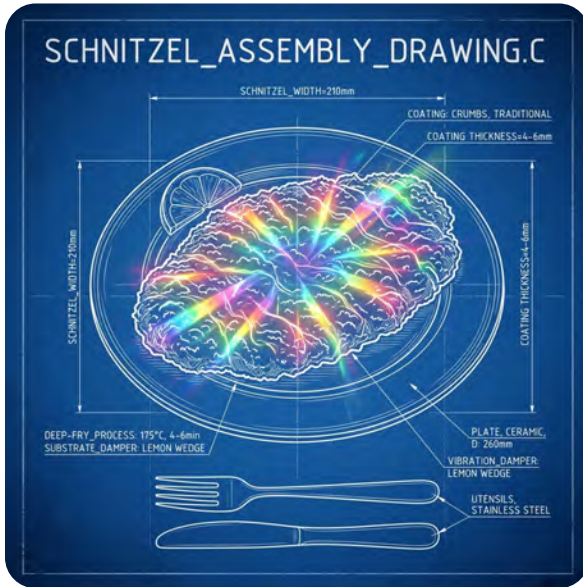
ART. 50(4)



Deep Fakes & Text

- **Deep Fakes:** Offenlegung der Manipulation; abgeschwächte Pflicht bei Kunst/Satire.
- **Öffentlicher Text:** Offenlegung bei Veröffentlichungen im öffentlichen Interesse.
- **Ausnahme:** Text unter menschlicher Überprüfung & redaktioneller Verantwortung.

„Schnitzel-Briefe“



AI-generated

Der Rechtsstreit um gefälschte FPÖ-Briefe des Satiremagazins *Die Tagespresse* ist rechtskräftig abgeschlossen.

Hintergrund

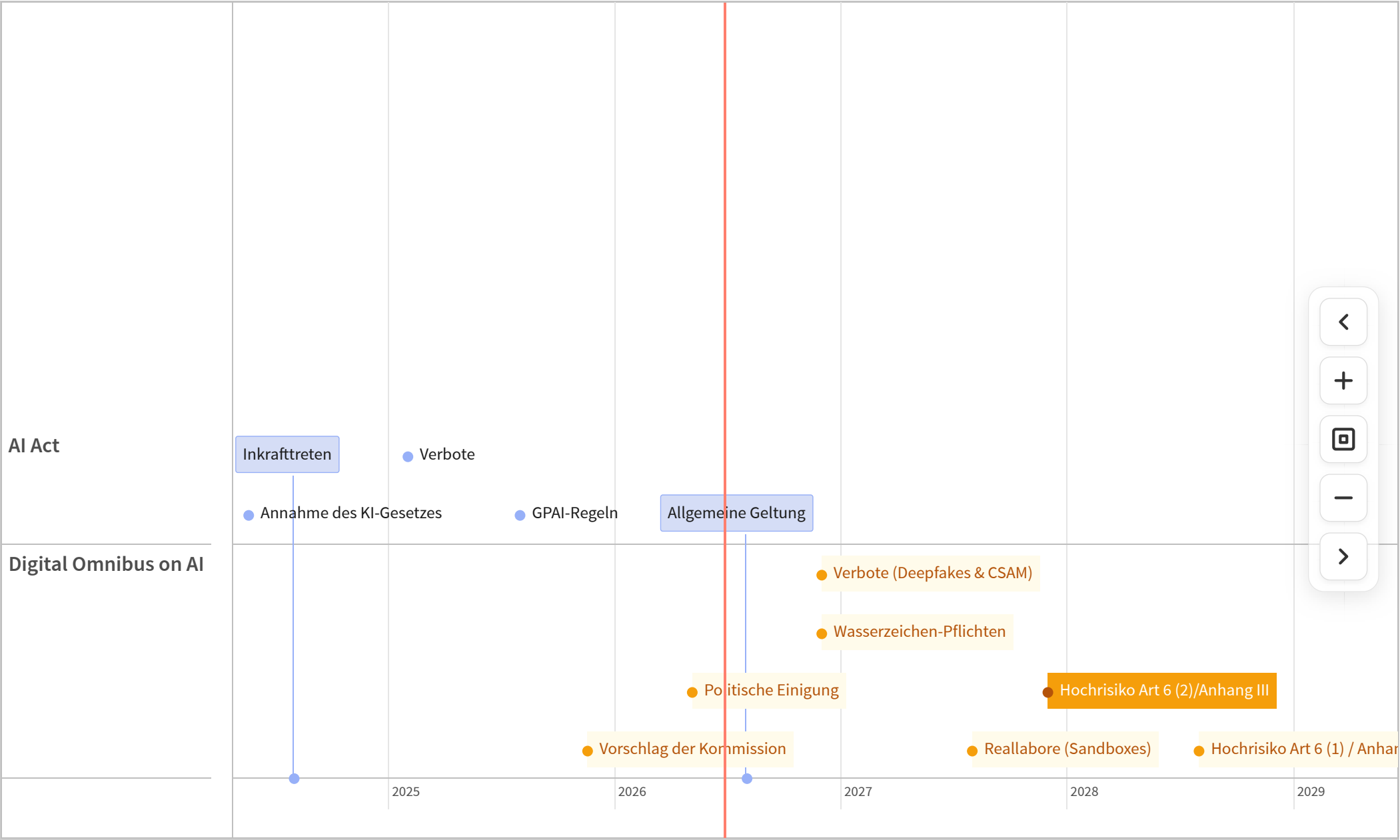
Die Satire-Aktion

- **April 2023:** Versand von 500 gefälschten Briefen im Namen der FPÖ NÖ an Gastwirte („Wirtshausprämie“).
- **Inhalt:** Satirische Forderungen wie eine „Panierquote“ oder „Andreas-Hofer-Schnitzel“.

Urteil & Begründung

Namensrecht überwiegt

- **OGH-Entscheidung:** Abänderung der Vorinstanzen zu Gunsten der FPÖ NÖ¹.
- **Täuschungsgefahr:** Logo-Nutzung suggerierte offiziellen Absender -> unzulässige Namensanmaßung (§ 43 ABGB).



Verbot von “Nudifier”-Apps

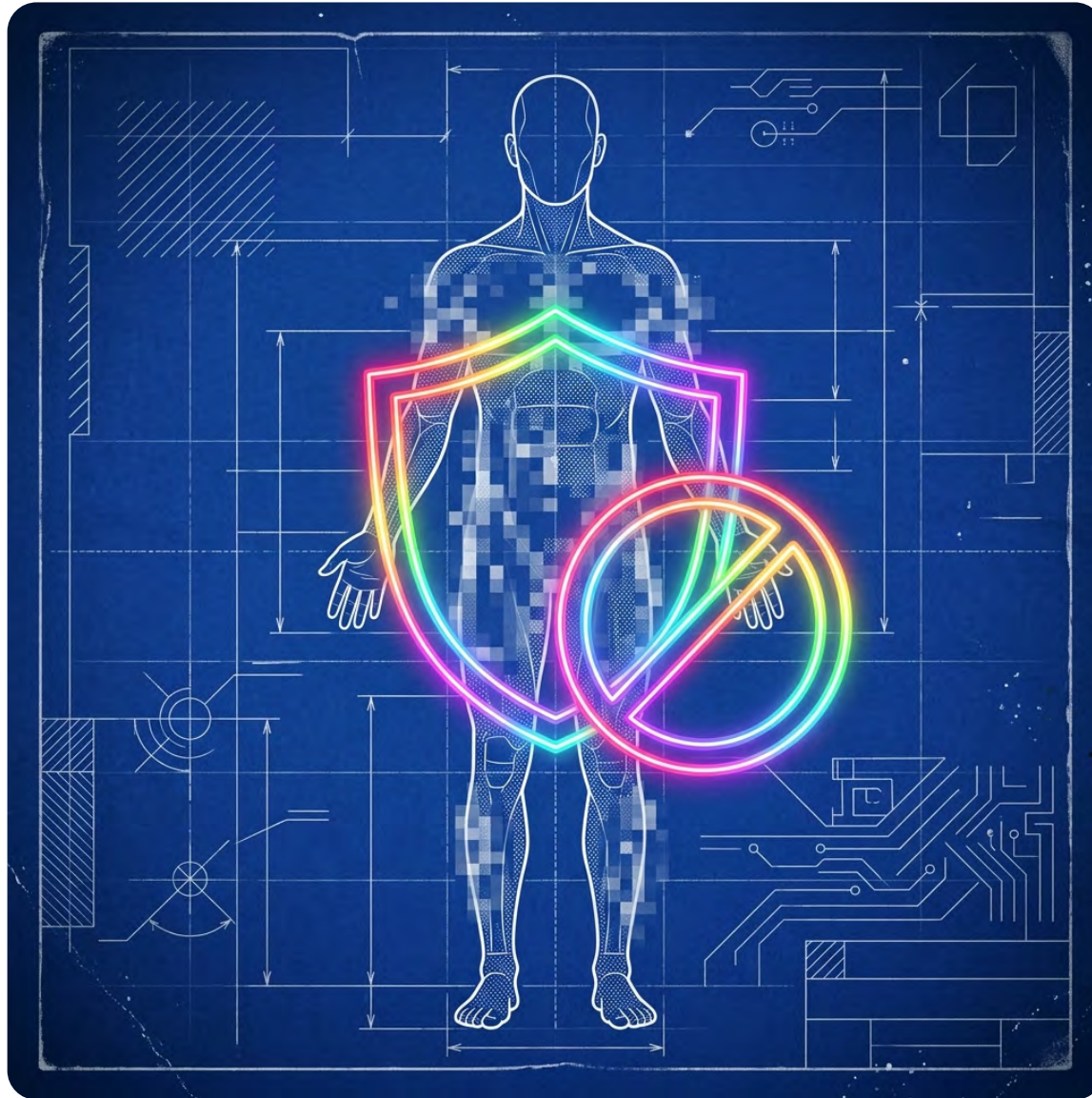


Bild: Gemini

NO CHILD PORNOGRAPHY

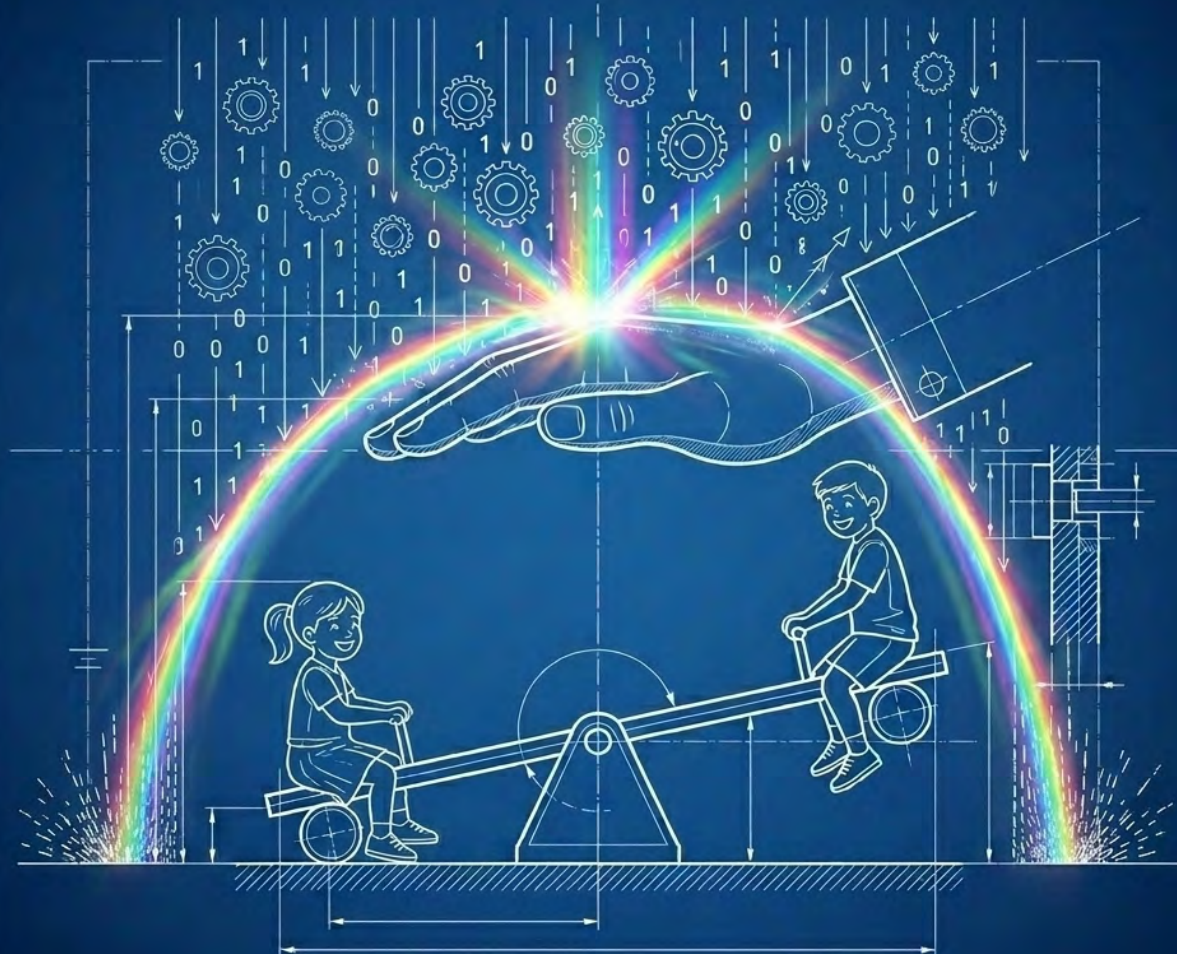
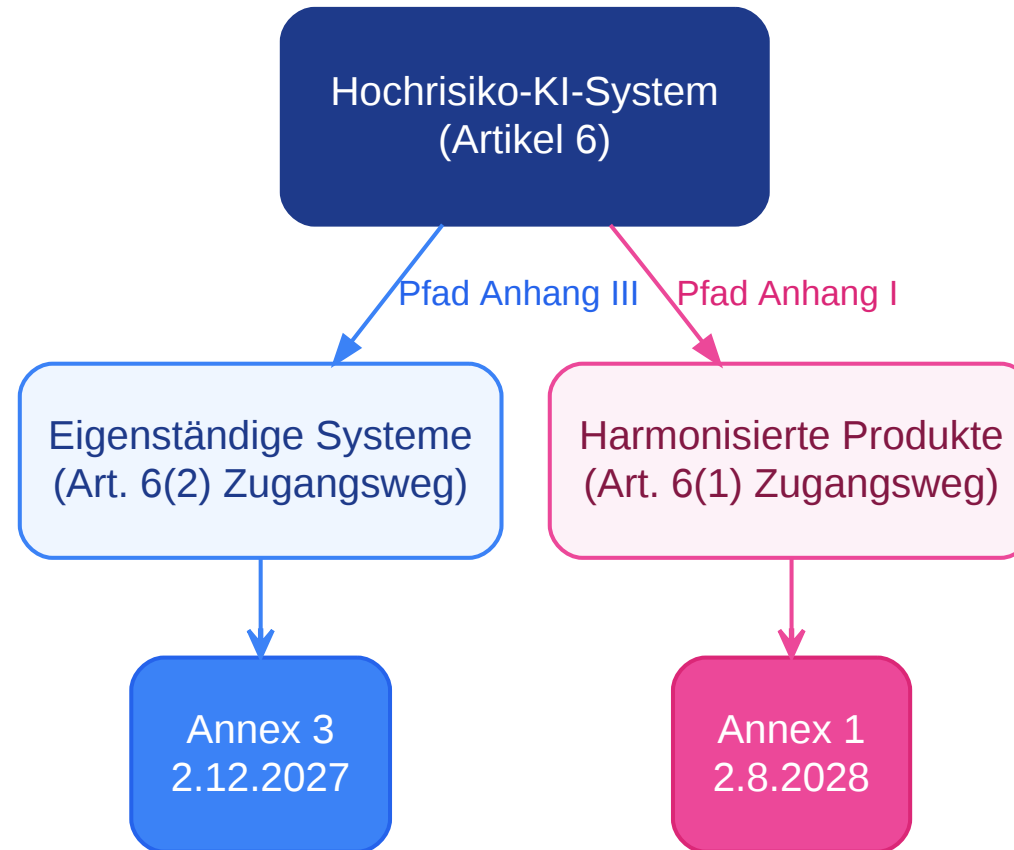


Image: AI-generated

Hochrisiko-KI Fristen



Leitlinien & Ressourcen

Nutzen Sie offizielle Leitlinien zur Unterstützung Ihres Compliance-Prozesses:

Jetzt Verfügbar



Vorhandene Ressourcen

- **Leitlinien der EU-Kommission:** Definition des Anwendungsbereichs und Ausnahmen für KI-Systeme.
- **RTR / AI-Servicestelle:** Nationale Check-Tools, Vorlagen und Informationen zur Sandbox.
- **Normenentwürfe:** Frühzeitiger Zugriff auf die CEN/CENELEC-Standardisierung.

In Kürze



Zukünftige Unterstützung

- **EU-KI-Amt (AI Office):** Veröffentlichung offizieller Leitlinien für Allzweck-KI (GPAI) und verbotene Praktiken bis Ende 2025.
- **Verhaltensregeln (Codes of Practice):** Von Akteuren gemeinsam ausgearbeitete Regeln zur Erleichterung der praktischen Compliance.



Agenda: Datenschutz

01

Künstliche Intelligenz

Definitionen, Risikoklassen des AI Acts, Rollen & Pflichten für Anbieter und Betreiber.

02

Datenschutz

DSGVO-Grundlagen, datenschutzrechtliche Rollenverteilung, Anonymisierung und die Risiken von Schatten-KI.

03

Urheberrecht

Text und Data Mining (TDM), urheberrechtliche Schutzfähigkeit von KI-Outputs und rechtskonforme Workflows.



Hinweis: Datenschutz endet nicht beim Vertrag. Die unkontrollierte Nutzung von Public-LLMs durch Mitarbeiter („Schatten-KI“) und das Risiko der De-Anonymisierung stellen erhebliche DSGVO-Haftungsrisiken dar.

Worauf muss bei KI geachtet werden?

1st

 DER AI ACT ALS WEGWEISER

Der AI Act ist die erste
horizontale Regulierung für
Software!



Understanding GDPR: Core Principles & Your Rights

A high-level overview of data processing principles organizations must follow and the fundamental rights individuals have over their personal data under the General Data Protection Regulation (GDPR).

How Organizations Must Handle Your Data



How You Can Control Your Data



NotebookLM

AI-generated

“

Data can be either *useful* or *perfectly anonymous*, but
NEVER both.

— PAUL OHM ¹

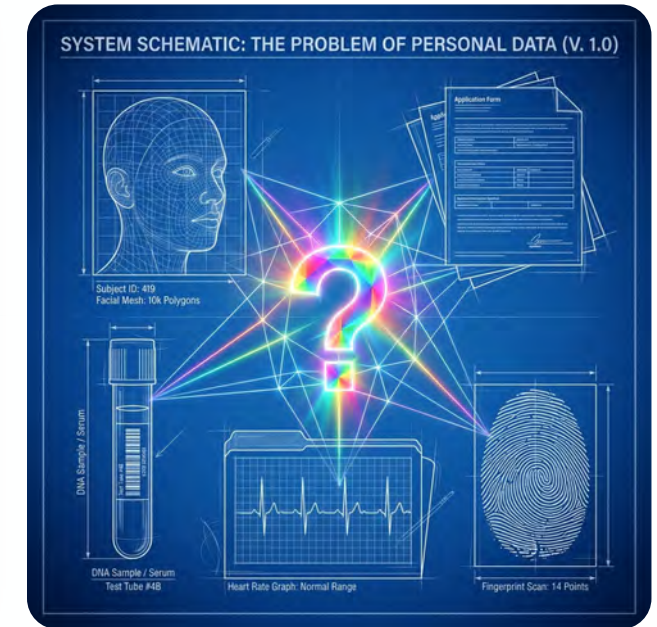
”



Was sind personenbezogene Daten?

ARTIKEL 4 NR. 1 DSGVO OFFIZIELLE DEFINITION

„**personenbezogene Daten**“ alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;“



💡 Kontext moderner KI-Umgebungen

Die Bestimmung, ob Daten in modernen KI-Umgebungen „personenbezogen“ sind, ist ein komplexes Puzzle. Abgeleitete Metadaten, Nutzungsmuster und Verhaltensfragmente stellen in Kombination oft personenbezogene Daten dar.

Gemini

LLM Deanonimization

LARGE-SCALE ONLINE DEANONYMIZATION WITH LLMS

“The practical obscurity protecting pseudonymous users online **no longer holds** [...] Large language models can perform at-scale deanonymization directly on raw, unstructured user content across arbitrary platforms, matching what would take hours for a dedicated human investigator.”¹

The Three-Stage LLM Pipeline

Unlike classical methods that rely on structured databases, the LLM attack works directly on unstructured text. It automatically **(1) extracts identity-defining features, (2) searches for matches** via semantic embeddings, and **(3) reasons over top candidates** using an LLM to verify and eliminate false positives.

Shattering GDPR Pseudonymization

LLMs shift the legal threshold of “**means reasonably likely to be used**”. Unstructured pseudonymous datasets must now be legally treated as **personal data** due to cheap, scalable re-identification.



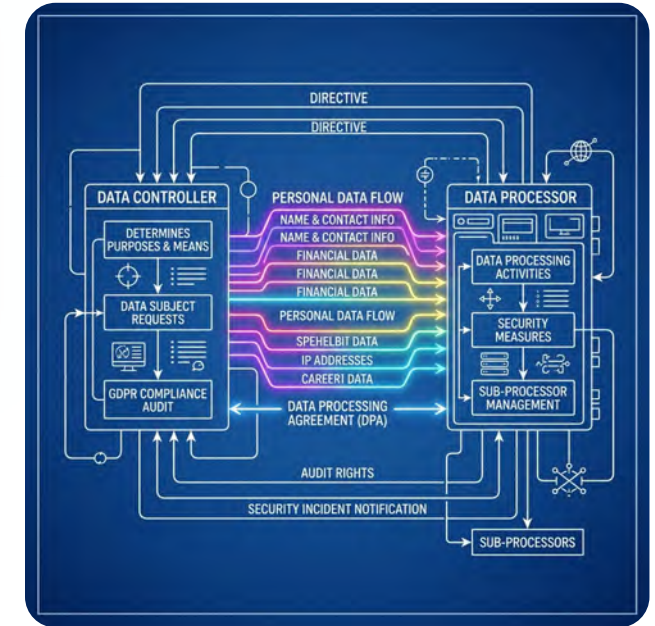
Was ist ein Auftragsverarbeiter?

ARTIKEL 4 NR. 8 DSGVO OFFIZIELLE DEFINITION

„„Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“¹

💡 Kontext moderner KI-Auftragsverarbeitung

In modernen KI-Ökosystemen agieren Betreiber von Hochleistungs-GPU-Infrastrukturen, Machine-Learning-as-a-Service-Plattformen und externe Fine-Tuning-Dienste als Auftragsverarbeiter.



KI-generiert

Auftragsverarbeitungsvertrag (AVV)

ART. 28 ABS. 3 DSGVO • VERTRAGLICHE GRUNDLAGE VERPFLICHTEND

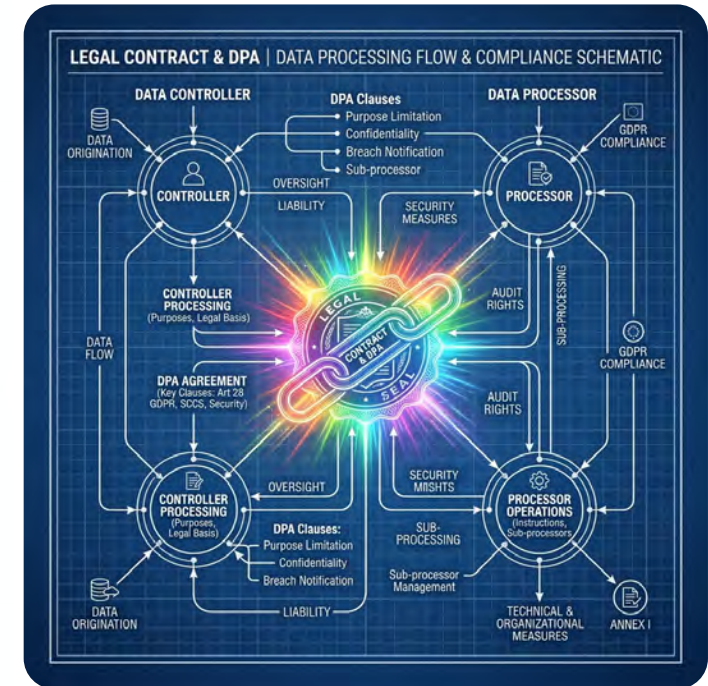
„Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines **Vertrags oder eines anderen Rechtsinstruments** nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet [...]"

ART. 28 ABS. 7 DSGVO • STANDARDKLAUSELN OPTION

Die Kommission kann
Standardvertragsklauseln festlegen [...]

ART. 28 ABS. 9 DSGVO • FORMVORSCHRIFT STRIKT

Der Vertrag oder das andere
Rechtsinstrument im Sinne der Absätze 3
und 4 muss **schriftlich abgefasst sein, was
auch in einem elektronischen Format
erfolgen kann**.



KI-generiert

Auftragsverarbeitungsverträge (AVV - Art. 28 DSGVO)



1. Weisungsbindung

Der Auftragsverarbeiter darf Daten **ausschließlich** auf dokumentierte Weisung des Verantwortlichen verarbeiten, auch bezüglich Drittlandübermittlungen.



2. Vertraulichkeitspflicht

Es ist sicherzustellen, dass sich die zur Verarbeitung berechtigten Personen zur **Verschwiegenheit** verpflichtet haben oder einer gesetzlichen Pflicht unterliegen.



3. Sicherheit der Verarbeitung

Implementierung von technischen und organisatorischen Maßnahmen (TOMs) nach dem Stand der Technik, um ein angemessenes Sicherheitsniveau zu gewährleisten.



4. Subunternehmer-Kontrolle

Einhaltung der strengen Bedingungen für die Hinzuziehung weiterer Auftragsverarbeiter; erfordert eine **vorherige schriftliche Genehmigung** und gleichwertige Verträge.



5. Unterstützung & Rechte

Unterstützung des Verantwortlichen bei der Beantwortung von Betroffenenanfragen und bei der Einhaltung von Compliance-Pflichten wie **DSFAs**.



6. Überprüfungen & Audits

Bereitstellung aller Informationen zum Nachweis der Einhaltung der Pflichten sowie **Ermöglichung und Unterstützung von Überprüfungen**, einschließlich Inspektionen.

Internationaler Datenverkehr

Drittlandstransfer im Vergleich

Dienst	Anbieter	Konzernsitz
ChatGPT	OpenAI	USA
Gemini	Google	USA
Mistral	Mistral AI	EU
AI Factory	AI:AT	EU

⚠ Risiko des Behördenzugriffs

Bei Anbietern mit US-Konzernsitz besteht das grundlegende Risiko des Datenzugriffs durch ausländische Sicherheitsbehörden – dies gilt im Regelfall auch dann, wenn die Daten auf europäischen Servern gehostet werden.



AI-generated

Action-Items: Data Transfer Impact Assessment (DTIA)

- ☐ **Datenflüsse analysieren:** Verarbeiten LLMs personenbezogene Daten in Drittstaaten?
- ☐ **Rechtsgrundlage & DPF prüfen:** Ist der Anbieter DPF-zertifiziert? Liegen SCCs vor?
- ☐ **Sicherheitsmaßnahmen:** Pseudonymisierung vor API-Versand, Opt-Out für Training.
- ☐ **Dokumentation:** DTIA schriftlich festhalten zur Erfüllung der Rechenschaftspflicht.



Top Risiken bei KI

- 01** Unklare Ziele & Anforderungen
- Software wird ohne konkrete Definition des Nutzens oder klarer Anforderungen eingeführt.

Art 5 Abs 1 lit b, Art 25 DSGVO (Zweckbindung & Privacy by Design)

- 02** Schatten-KI (Shadow AI)
- Mitarbeiter nutzen unautorisierte KI-Tools im Arbeitsalltag, wodurch sensible Daten abfließen.

Art 28, Art 32 DSGVO (Fehlende Auftragsverarbeitung & Datensicherheit)

- 03** Mangelnde Benutzerakzeptanz
- Die beste Software scheitert, wenn Anwender im Change-Prozess nicht ausreichend geschult und mitgenommen werden.

Art 32 Abs 4 DSGVO (Mangelnde Anweisung und Schulung von Mitarbeitern)

- 04** Prompt Injection
- Sicherheitslücken entstehen, wenn manipulative Eingaben KI-Systeme korrumpieren.

Art 32 DSGVO (Verletzung der technischen Sicherheit & Systemintegrität)

- 05** Fehlende Compliance
- Datenschutz- und Regulierungsrisiken werden vorab unzureichend geprüft.

Art 35, Kapitel V DSGVO (Pflichtverletzung DSFA & Internationaler Datenverkehr)

Schatten-KI (Shadow AI)

Das Problem: Beschäftigte speisen eigenmächtig Dokumente, Quellcodes oder personenbezogene Daten in frei zugängliche Online-KI-Systeme ein.

- **Rechtswidriger Drittstaatstransfer:** Viele Standard-LLMs werden in den USA gehostet. Ohne SCCs oder Data Privacy Framework liegt ein Verstoß gegen Kap. V DSGVO vor.
- **Fehlender AVV (Art 28 DSGVO):** Mit jedem Dienstleister, der personenbezogene Daten verarbeitet, muss ein AVV geschlossen werden. Kostenlose Tools bieten dies meist nicht.
- **Verlust von Geschäftsgeheimnissen:** Eingaben in kostenlose Versionen werden oft zum Modell-Training genutzt – sensible Geschäftsdaten können in Ausgaben Dritter auftauchen.

Praktische Gegenmaßnahmen

1. **Klare Richtlinien:** Offizielle Betriebsvereinbarungen und Nutzungsverbote für unautorisierte Tools.
2. **Sichere Alternativen:** Bereitstellung von Enterprise-Lizenzen mit Trainings-Opt-Out und AVV.
3. **Technische Sperren:** Blockieren nicht freigegebener KI-Domains im Firmennetzwerk.

Prompt Injection

Sicherheitsmängel bei KI-Systemen führen direkt zu Datenschutzverletzungen. Eine Bedrohung für LLMs sind Prompt Injections:

- **Direct Prompt Injection (Jailbreaking):** Ein Angreifer manipuliert das System über den Chat direkt, um Sicherheitsfilter zu umgehen.
- **Indirect Prompt Injection (Sehr kritisch!):** Schädliche Instruktionen sind in externen Daten versteckt, die das LLM liest (z. B. versteckte Anweisungen in einer PDF-Bewerbung, um die HR-Entscheidung zu manipulieren).
- **Datenschutz-Folge:** Verletzung des Richtigkeitsprinzips (Art 5 Abs 1 lit d DSGVO) durch manipulierte oder halluzinierte Ausgaben.

BSI Defence-in-Depth Konzept

Das **BSI** empfiehlt eine mehrschichtige Sicherheitsstrategie:

1. **Strikte Datentrennung:** Externe Daten dürfen niemals direkt als Steuerungscode (System-Prompt) interpretiert werden.
2. **Zero-Trust:** Alle Eingaben aus externen Dateien als potenziell bösartig behandeln.
3. **Sandboxing:** KI-Agenten in isolierten Umgebungen ausführen.
4. **Human-in-the-Loop:** Keine vollautomatischen Aktionen bei kritischen Prozessen.

Agenda: Urheberrecht

01

Künstliche Intelligenz

Definitionen, Risikoklassen des AI Acts, Rollen & Pflichten für Anbieter und Betreiber.

02

Datenschutz

DSGVO-Grundlagen, datenschutzrechtliche Rollenverteilung, Anonymisierung und die Risiken von Schatten-KI.

03

Urheberrecht

Text und Data Mining (TDM), urheberrechtliche Schutzfähigkeit von KI-Outputs und rechtskonforme Workflows.



Hinweis: Reine KI-Generates sind urheberrechtlich gemeinfrei, da sie keine menschliche Schöpfung darstellen. Für das Training von KI müssen jedoch die strengen TDM-Ausnahmen (Opt-Outs) beachtet werden.

A QUICK GUIDE TO AUSTRIAN COPYRIGHT LAW

WHAT IS A PROTECTED 'WORK'?



Literature (incl.
Software) &
Unique Creations



Music



Visual Arts
(Photography,
Architecture)



Film



Translations & Adaptations are also Protected

If original, they are protected like
new works without harming the
original's copyright.

THE CREATOR'S EXCLUSIVE RIGHTS



Right of Reproduction

The exclusive right to
make copies of the work
in any form.



Right of Distribution

The exclusive right to
offer physical copies of
the work to the public.



Right of Public Performance

The right to publicly recite,
perform, or display the work.



Right of Making Available Online

The right to make the
work available on-demand
(e.g., via the internet).

HOW LONG DOES COPYRIGHT LAST?



70 Years After the Author's Death

For most literary, musical, and
artistic works, protection
lasts for 70 years.



Special Rule for Films

Protection ends 70 years after the
death of the last key contributor.

NotebookLM

AI-generated

“

Urheber haben das

AUSSCHLIESSLICHE

Recht, Werke in den gesetzlich geregelten Fällen zu *verwerten*.

— § 14 ABS. 1 URHG • VERWERTUNGSRECHTE

”



Leitfaden: AI-Input¹

Vervielfältigung



1. Kopierintensiver Prozess

- **Jeder technische Schritt** (Scraping, Caching, Speicherung) ist eine Vervielfältigung im Sinne des EU-Rechts.
- **Selbst temporäre Kopien** oder Fragmente während des Trainings greifen in das exklusive Recht der Urheber ein.
- **Keine bloße Inspiration:** KI-Training unterscheidet sich rechtlich fundamental vom menschlichen Lernen.

TDM-Schranken



2. Rechtliche Ausnahmen

- **Wissenschaft (Art. 3):** Erlaubt TDM für Hochschulen und gemeinnützige Forschung bei **rechtmäßigem** Zugang.
- **Kommerziell (Art. 4):** Erlaubt TDM für alle Akteure, steht aber unter dem Vorbehalt eines erklärten **Opt-Outs**.
- **Enger Anwendungsbereich:** TDM-Ausnahmen decken die reine Analyse ab, nicht zwingend den gesamten GenAI-Trainings- und Verteilungsprozess.

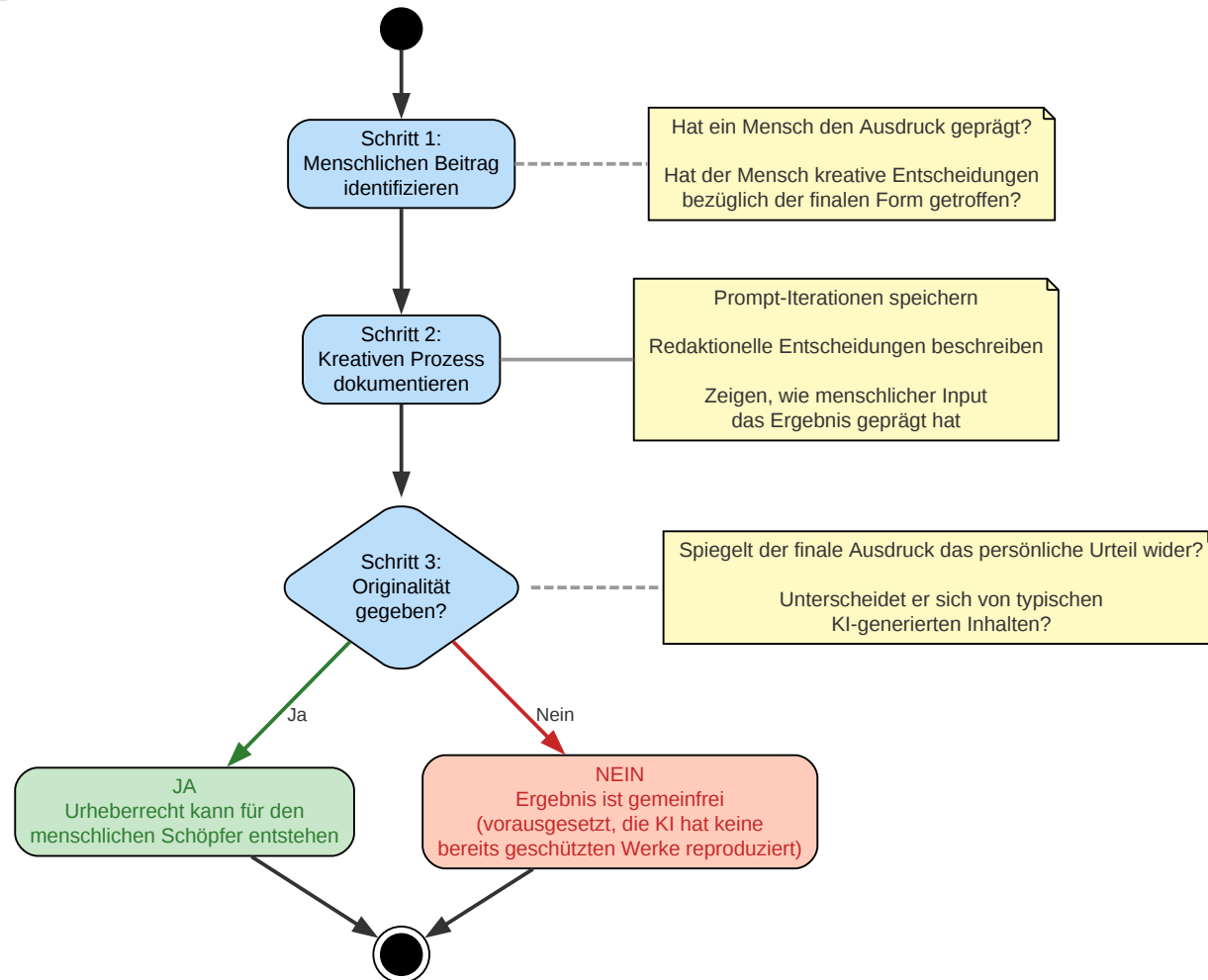
AI Act & Standard



3. Pflichten & Opt-Outs

- **Beachtungspflicht:** GPAI-Entwickler müssen eine Strategie zur Einhaltung des Urheberrechts pflegen und Opt-Outs beachten.
- **Harmonisierung:** Die EU erarbeitet standardisierte Protokolle (robots.txt, C2PA, TDMRep) zur maschinenlesbaren Rechteerklärung.
- **Transparenzbericht:** Pflicht zur Veröffentlichung einer detaillierten Zusammenfassung der Trainingsdaten.

Urheberrecht bei KI-Erzeugnissen¹



Klicke auf die Pfade, um die Schritte nacheinander freizuschalten.

Leitfaden: AI-Outputs¹

Urheberschaft

Schutzfähigkeit

- **Reine KI-Outputs:** Sind **gemeinfrei** (*public domain*), da nur menschliche Schöpfungen urheberrechtlich geschützt sind.
- **KI-gestützte Werke:** Schutz möglich, wenn ein Mensch gestalterischen Einfluss ausübt (Kuration, Editierung, komplexe Prompt-Iterationen).
- **Nachweis:** Dokumentation des kreativen Prozesses und der Prompt-Entwicklung zwingend erforderlich.

Haftung & Risiko

Verletzungsrisiken

- **Plagiate & Memorierung:** Risiko von wortgetreuen Reproduktionen (Verbatim) geschützter Trainingsdaten.
- **Ketten-Haftung:**
 - **Nutzer:** Haftet bei kommerzieller Verbreitung oder Umgehung von Filtern.
 - **Deployer:** Haftet bei fehlenden Output-Filtern und Massenverbreitung.
 - **Entwickler:** Haftet bei systematischen Urheberrechtsverletzungen.

AI Act

Compliance-Pflichten

- **Kennzeichnungspflicht:** KI-generierte Inhalte und Deepfakes müssen klar als solche markiert werden (Art. 50 AI Act).
- **GPAI-Modelle:** Entwickler müssen Urheberrechts-Policies einhalten und technische Maßnahmen zur Plagiatsvermeidung etablieren (Art. 53).
- **Praxis:** Einsatz von Ähnlichkeitsprüfung, Provenienz-Tracking und Wasserzeichen.



Transparenz bei Nutzung von GenAI in der Forschung

EU-LEITLINIEN



EU-Kommission

- **Forschungsleitlinien:** Grundsätzliche Offenlegung von GenAI im Forschungsprozess empfohlen.
- **Verbot vs. Transparenz:** Manche Fachverlage verbieten GenAI komplett.
- **Regulierung:** Andere Verlage verweisen auf spezifische Offenlegungsrichtlinien (z. B. Elsevier).

ELSEVIER POLICY



Elsevier Richtlinien

- **Volle Verantwortung:** Autoren haften uneingeschränkt für die Inhalte ihrer Arbeit.
- **Offenlegungspflicht:** Einreichung erfordert ein separates *AI declaration statement*.
- **Rechtswahrung:** Bedingungen des KI-Tools prüfen (Datenschutz, geistiges Eigentum, Rechte Dritter).
- **Inhalt der Erklärung:** Name des Tools, Zweck der Nutzung und Grad der menschlichen Überwachung.

TU WIEN



TU Wien (Gute Praxis)

- **Zitierpflicht:** Unveränderte GenAI-Texte sind wie *Zitate aus anderen Quellen* zu behandeln.
- **Eindeutige Kennzeichnung:** Passagen müssen klar als synthetisch markiert sein.
- **Quellenangabe:** Angabe von Prompt, Generierungsdatum, System und Version zwingend erforderlich.
- **Format:** „Promptbeispiel, 12.09.2023, ChatGPT, Version [X]“

1. The use of generative artificial intelligence in research. (2025). ↩

2. Generative AI policies for journals, 2025 <<https://www.elsevier.com/about/policies-and-standards/generative-ai-policies-for-journals>>. ↩

3. Empfehlung zur guten Praxis im Umgang mit generativer KI an der Technischen Universität Wien, 10/15/2023 <<https://www.tuwien.at/studium/lehren-an-der-tuw/digital-gestuetzte-lehre/kuenstliche-intelligenz-in-der-lehre>>. ↩

Compliance-Zusammenfassung

Regulierung



Risikoklassen & AI Act

- **Risiko-basierter Ansatz:** Verbotene Praktiken vs. Hochrisiko-Systeme.
- **Anhang III:** Strikte Regulierung für sensible Bereiche (Bildung, Beschäftigung, Justiz).
- **NLF-Prinzipien:** CE-Kennzeichnung und Konformitätsbewertungen.

Akteure



Pflichten & Rollen

- **Anbieter (Provider):** Tragen die Hauptlast (Qualitätsmanagement, technische Doku).
- **Betreiber (Deployer):** Pflicht zur Überwachung, Nutzungskontrolle & AI Literacy.
- **Haftungsübergang (Art. 25):** Nachgelagerte Akteure haften bei wesentlichen Änderungen.

Praxis



Literacy & Transparenz

- **KI-Kompetenz:** Schulungen für Mitarbeiter im KI-Kontakt.
- **Kennzeichnung:** Pflicht zur Offenlegung von KI-generiertem Content (Audio, Video, Text).
- **Ausnahmen:** Erleichterungen für Kunst/Satire sowie reine Forschung & Entwicklung.

Recht



DSGVO & Urheberrecht

- **Datenschutz:** Notwendigkeit klarer Verträge zur Auftragsverarbeitung (Art. 28 DSGVO).
- **Schatten-KI:** Risiken durch unkontrollierten Einsatz externer Cloud-Systeme minimieren.
- **IP / TDM:** Berücksichtigung von Urheberrecht & Text-and-Data-Mining-Ausnahmen.



Contact



michael-loeffler

Michael Löffler

Lead Legal, Regulatory and Ethics
AI Factory Austria AI:AT

+43 664 883 906 92

michael.loeffler@ai-at.eu

Karl-Farkas-Gasse 22, 1030 Wien

References

Ahmed/Cooper/Koyejo/Liang, Extracting books from production language models, 01/06/2026 <<http://arxiv.org/abs/2601.02671>>, aufgerufen am 01/16/2026

Almada, [Law & Compliance in AI Security & Data Protection](#), 12/2024

Artificial Intelligence Office, [Draft Guidelines on the implementation of the transparency obligations for certain AI systems under Article 50](#), 05/08/2026

Bontcheva/Bechmann/Pedreschi/Gregorio/Riess/Botan, [Second Draft Code of Practice on Transparency of AI-Generated Content](#), 03/05/2026

Bundesamt für Sicherheit in der Informationstechnik, Indirect Prompt Injections - Intrinsische Schwachstelle in anwendungsintegrierten KI- Sprachmodellen, 07/18/2023

—, Schwächen von LLMs, <<https://medien.bsi.bund.de/lagebericht/de/schwachstellen-von-llms/>>, aufgerufen am 06/02/2026

and of the Council as regards the simplification of the implementation of harmonised rules on artificial intelligence, Letter sent to the European Parliament, 05/13/2026

Elsevier, Generative AI policies for journals, 2025 <<https://www.elsevier.com/about/policies-and-standards/generative-ai-policies-for-journals>>, aufgerufen am 10/30/2025

Europäische Kommission, Leitlinien der Kommission zur Definition eines Systems der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung), 07/29/2025

European Commission, Draft Commission guidelines on the classification of high-risk AI systems under Article 6 of Regulation (EU) 2024/1689 (AI Act) for stakeholder consultation

European Commission. Directorate General for Research and Innovation., [The use of generative artificial intelligence in research.](#), Publications Office, LU 2025

European Parliament (Hrsg), [Generative AI and copyright: Training, creation, regulation](#), European Parliament, Brussels 2025

Kercz, Vom Prompt zum Code: Urheberrechtliche Risiken, Open-Source-Fallstricke und Transaktionsrelevanz, ailex 2026/10

Lermen/Paleka/Swanson/Aerni/Carlini/Tramèr, Large-scale online deanonymization with LLMs, 02/25/2026 <<http://arxiv.org/abs/2602.16800>>, aufgerufen am 03/04/2026

Ohm, [Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization](#), UCLA Law Review 2010, 1701

Rozgonyi/Löffler, [AI OUTPUT & COPYRIGHT: A primer for the AI:AT Factory \(Austria\)](#), 03/23/2026

—, [AI INPUT & COPYRIGHT: A primer for the AI:AT Factory \(Austria\)](#), 03/23/2026

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), Provider obligations in the AI Act, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Provider_obligations.en.html>, aufgerufen am 10/20/2025

—, AI Act: Deployer Obligations, <https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Deployer_obligations.en.html>, aufgerufen am 10/20/2025

Schippel, "Urheberrecht first!" - Die Pflicht zur KI-Policy nach Art. 53 KI-VO, KuR 2025, 547

Telekom Regulierungs-GmbH, [Text und Data Mining: Welche Botschaft senden österreichische Webseiten an KI-Anbieter?](#), 01/29/2026

Wendehorst/Nessler/Aufreiter/Aichinger, Der Begriff des „KI-Systems“ unter der neuen KI-VO, MMR 2024, 605

Wien, Empfehlung zur guten Praxis im Umgang mit generativer KI an der Technischen Universität Wien, 10/15/2023 <<https://www.tuwien.at/studium/lehren-an-der-tuw/digital-gestuetzte-lehre/kuenstliche-intelligenz-in-der-lehre>>, aufgerufen am 10/30/2025

Zankl/Madner, Art 4 KI-VO: Was bedeutet KI-Kompetenz "nach besten Kräften" und was folgt daraus straf- und schadenersatzrechtlich?, ailex 2025/12