

Künstliche Intelligenz in der Verwaltung von Forschungseinrichtungen

Rechtliche Grundlagen für die Anwendung von KI

Michael Löffler

07.10.2026



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

Definition & Ausnahmen, Risikostufen, Hochrisiko (Bildung/Personal), Rollen, Fristen, KI-Kompetenz und Transparenz.

02

Datenschutz

Personenbezogene Daten, Anonymisierung, LLM-Deanonymisierung, Drittlandtransfer und Schatten-KI in der Verwaltung.

03

Urheberrecht

Input- und Output-Seite, rechtskonforme Workflows sowie Transparenz bei GenAI in der Forschung.



Hinweis: In Forschungseinrichtungen greifen Hochrisiko-Regeln oft über Anhang III (Bildung, Personal). Nach Art. 25 KI-VO können Betreiber durch wesentliche Änderungen selbst zum Anbieter mit vollen Pflichten werden.



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

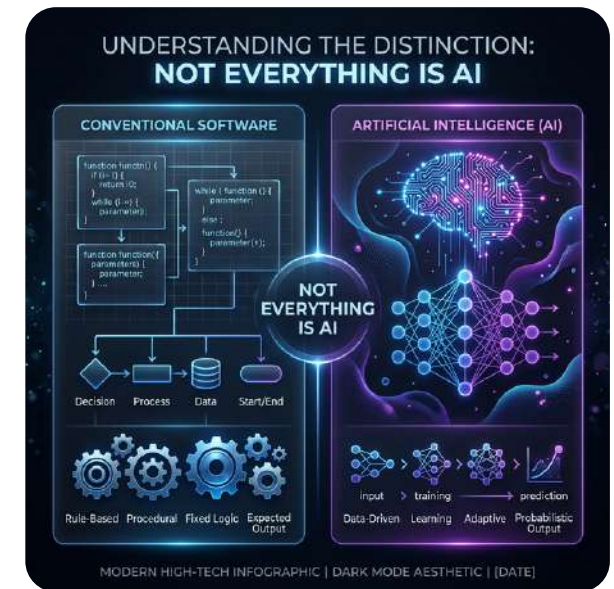
Ergebnisse, welche die physische oder virtuelle **Umgebungen beeinflussen können**.

Physisch

Virtuell

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.



AI GENERATED

New Legislative Framework (NLF)

Die KI-VO 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**.

CE

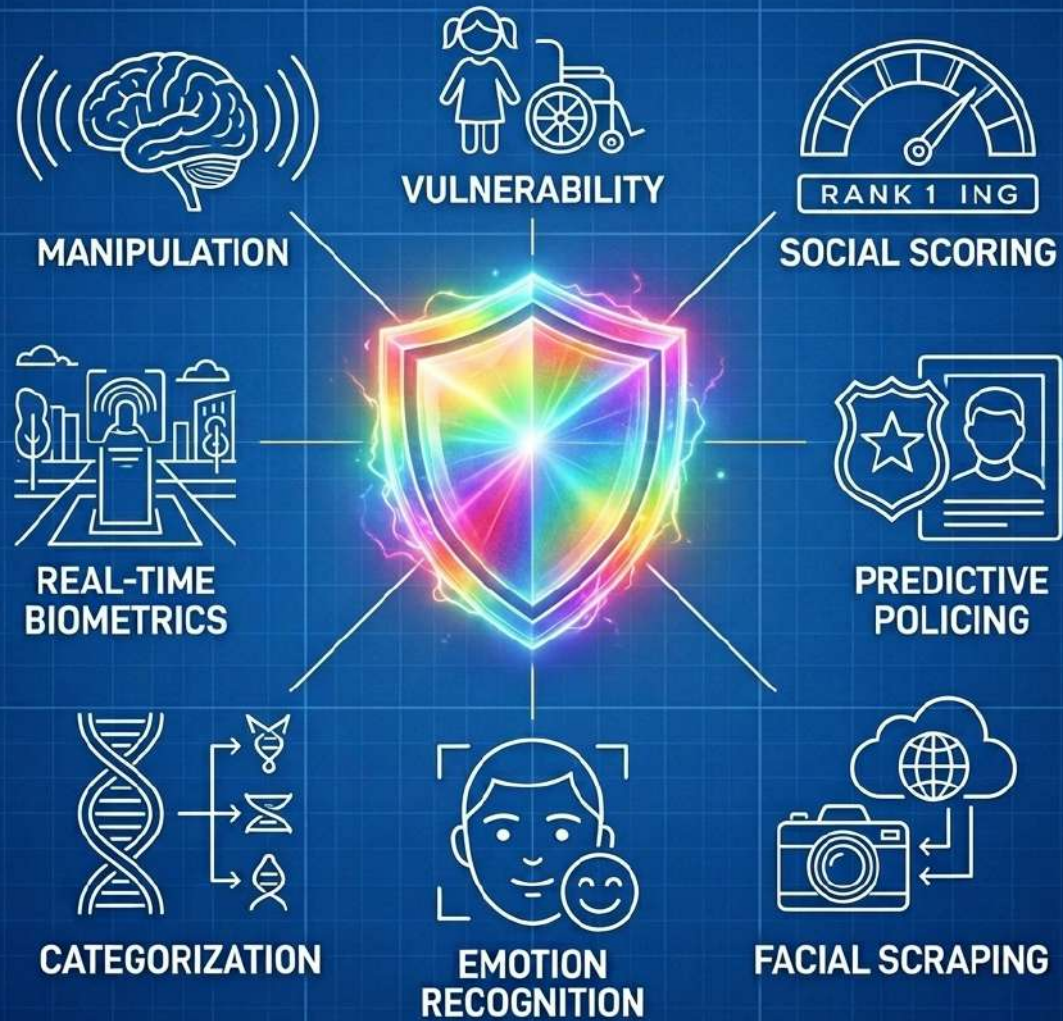


Risikostufen des KI-Gesetzes

Die KI-VO legt eine **risikobasierte Hierarchie** mit vier Hauptstufen fest:

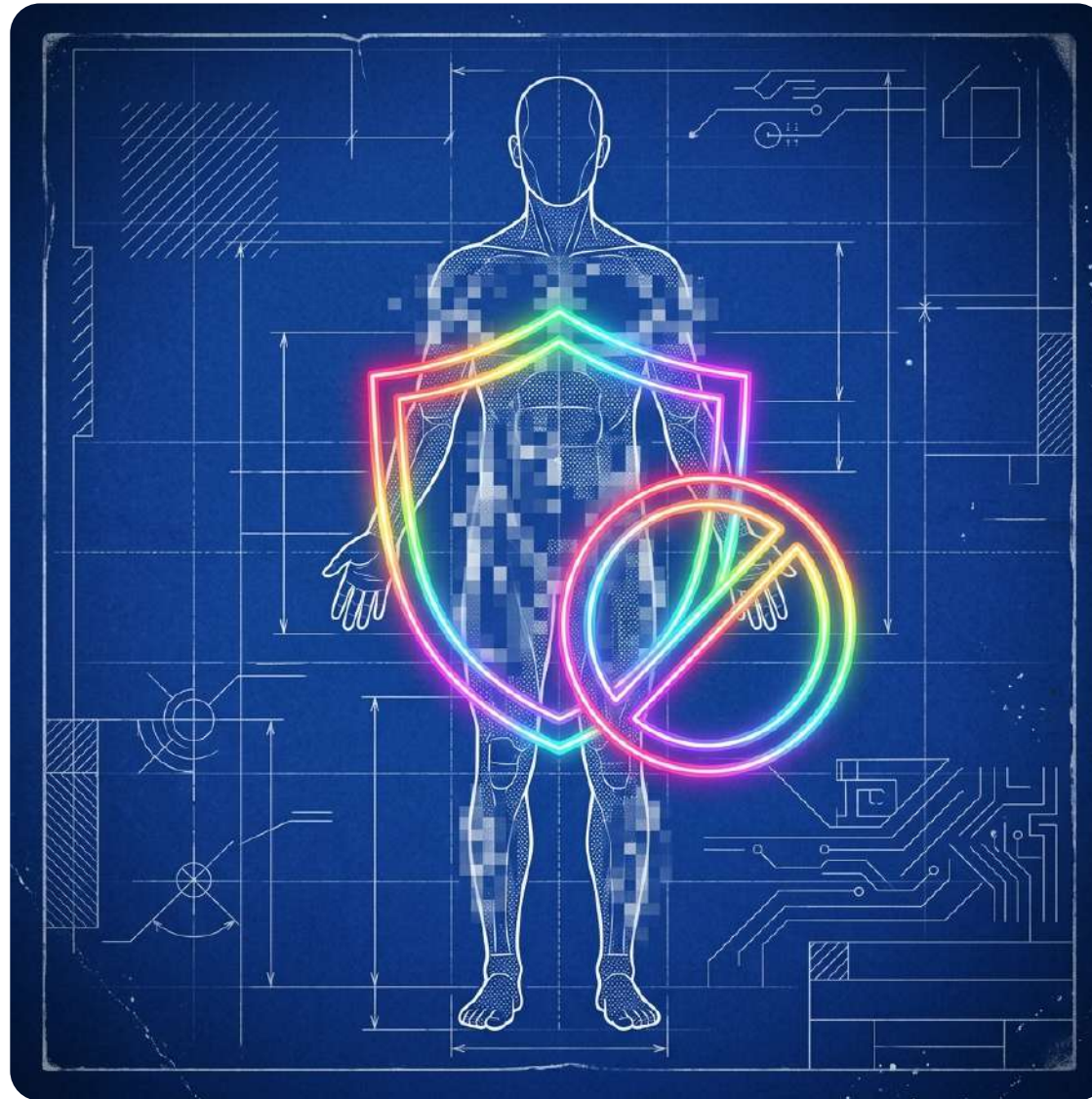


PROHIBITED AI PRACTICES



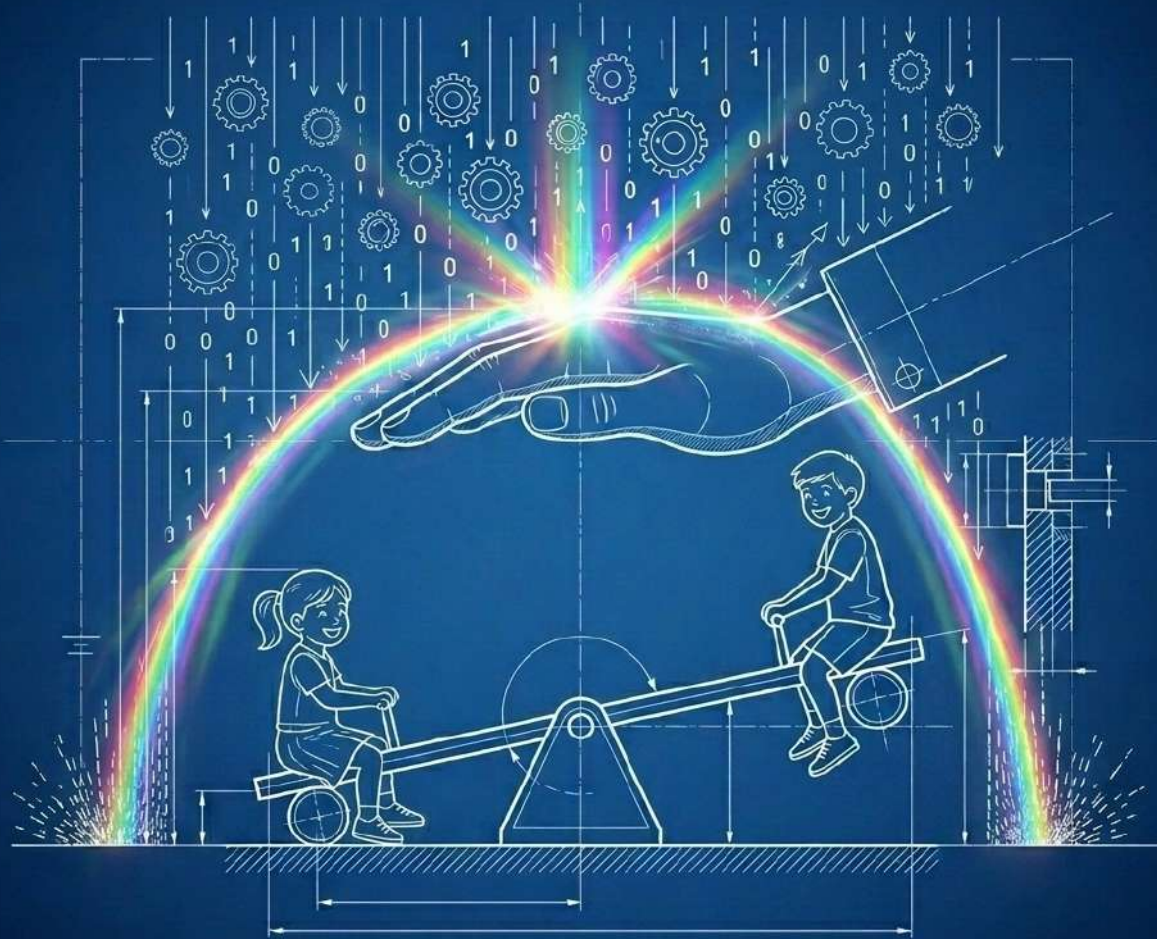
AI GENERATED

Verbot von “Nudifier”-Apps



AI GENERATED

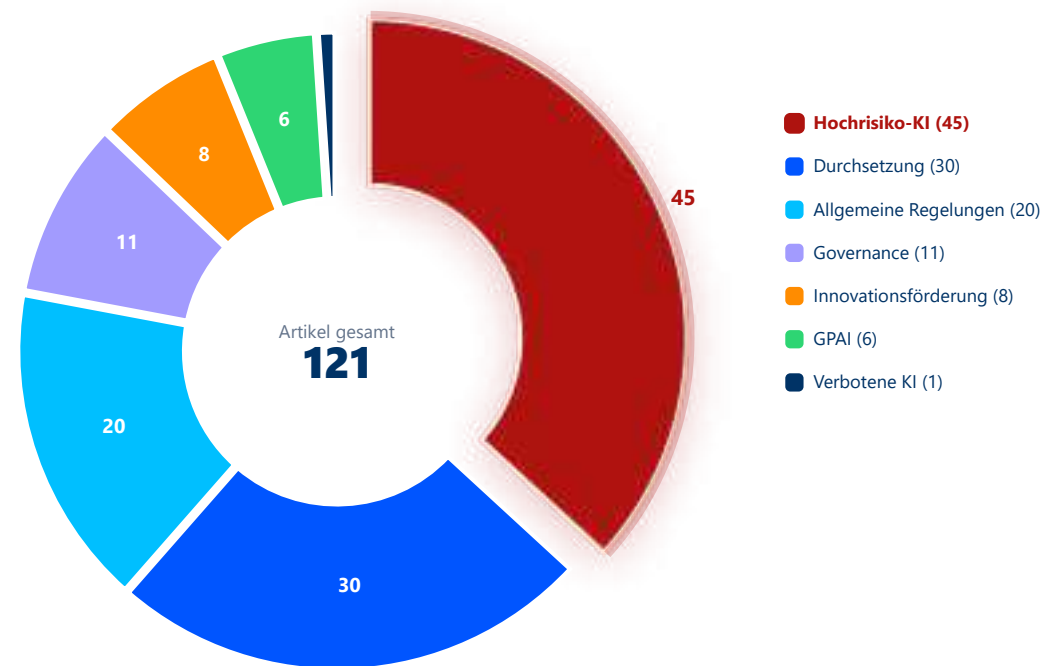
NO CHILD PORNOGRAPHY



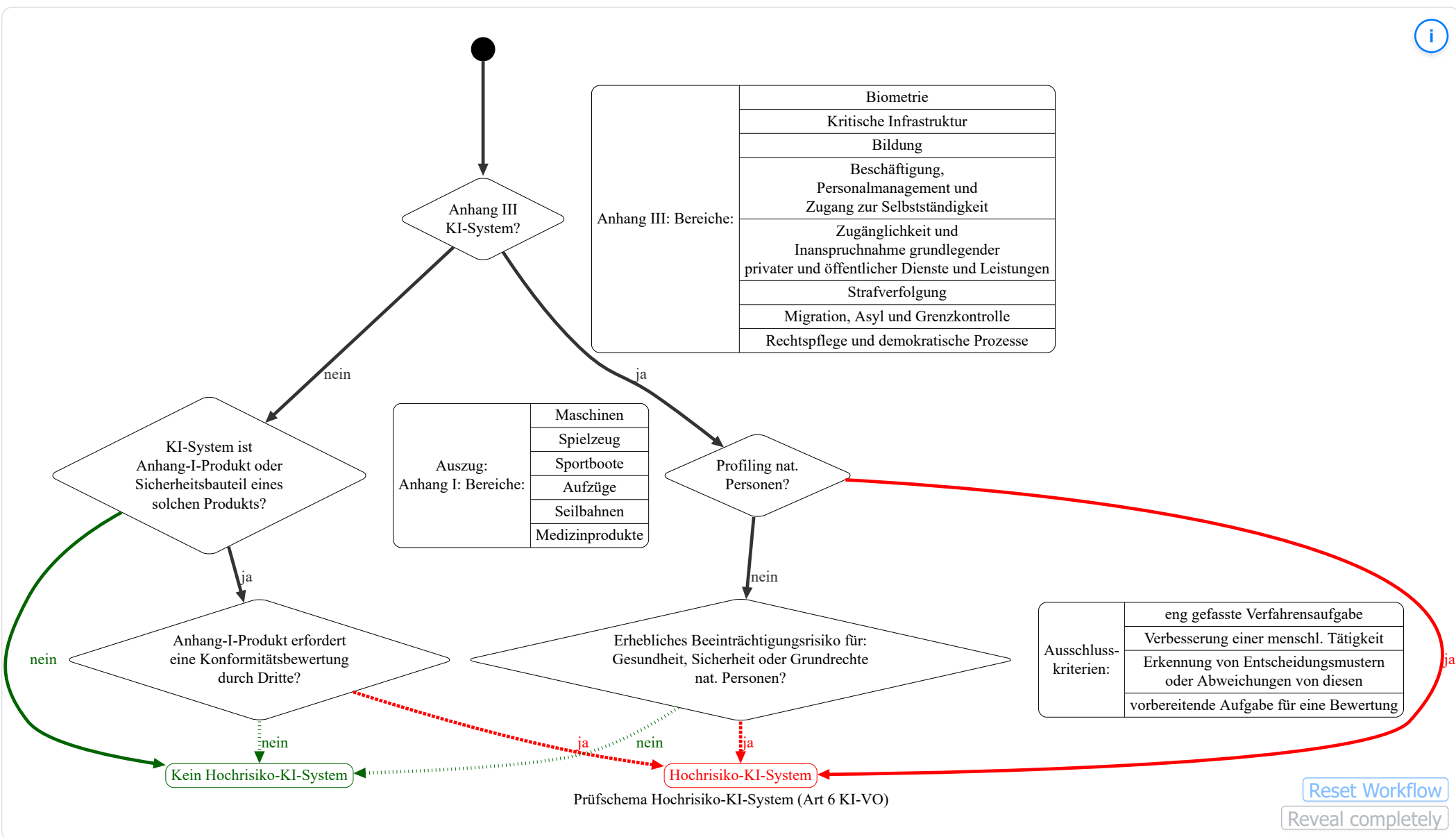
AI GENERATED

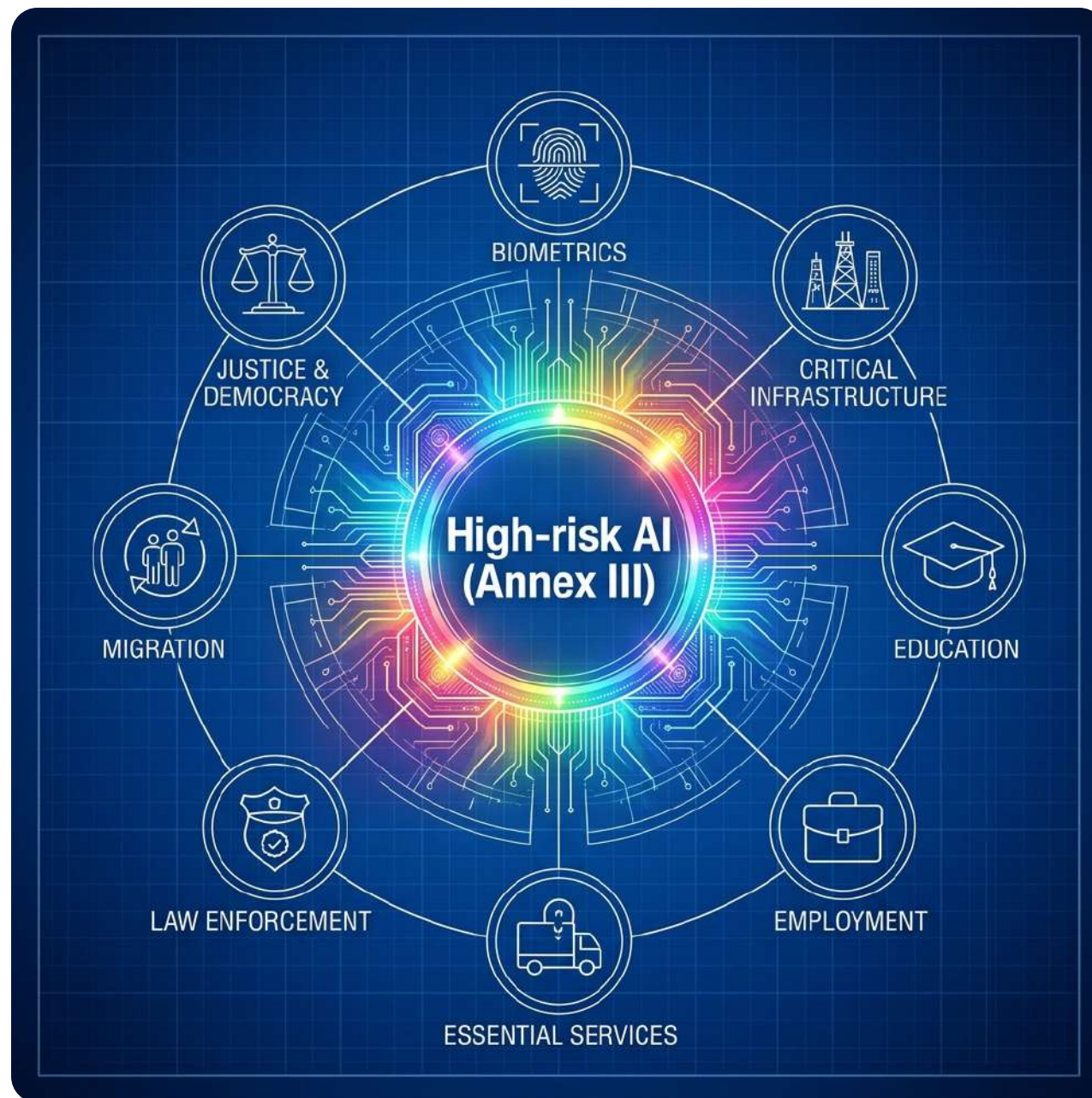
Die meisten Regeln gelten nur für Hochrisiko-KI

KI-V0 Artikelverteilung



Was ist hochriskant?





AI GENERATED



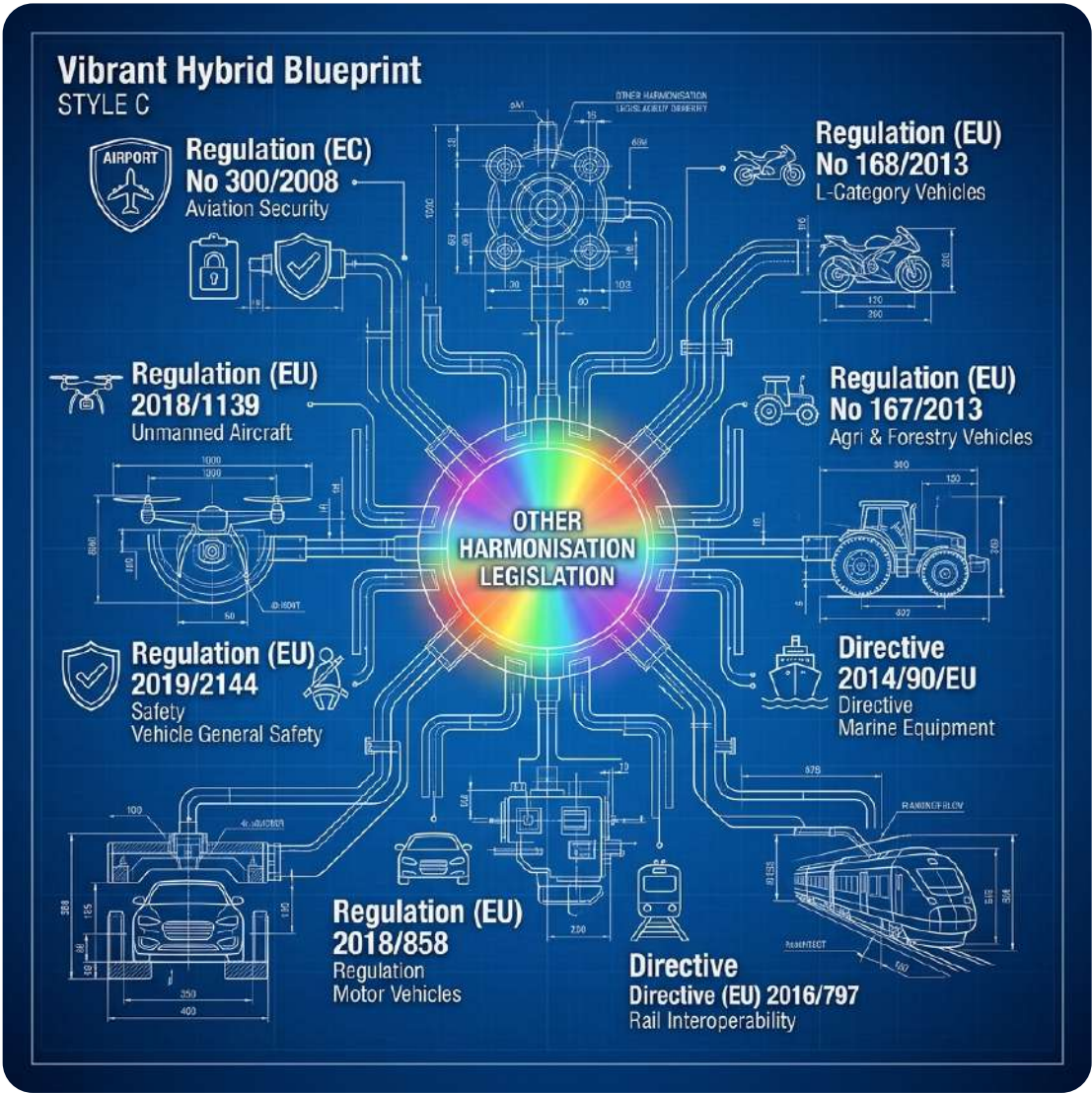
AI Act Annex I



AI GENERATED



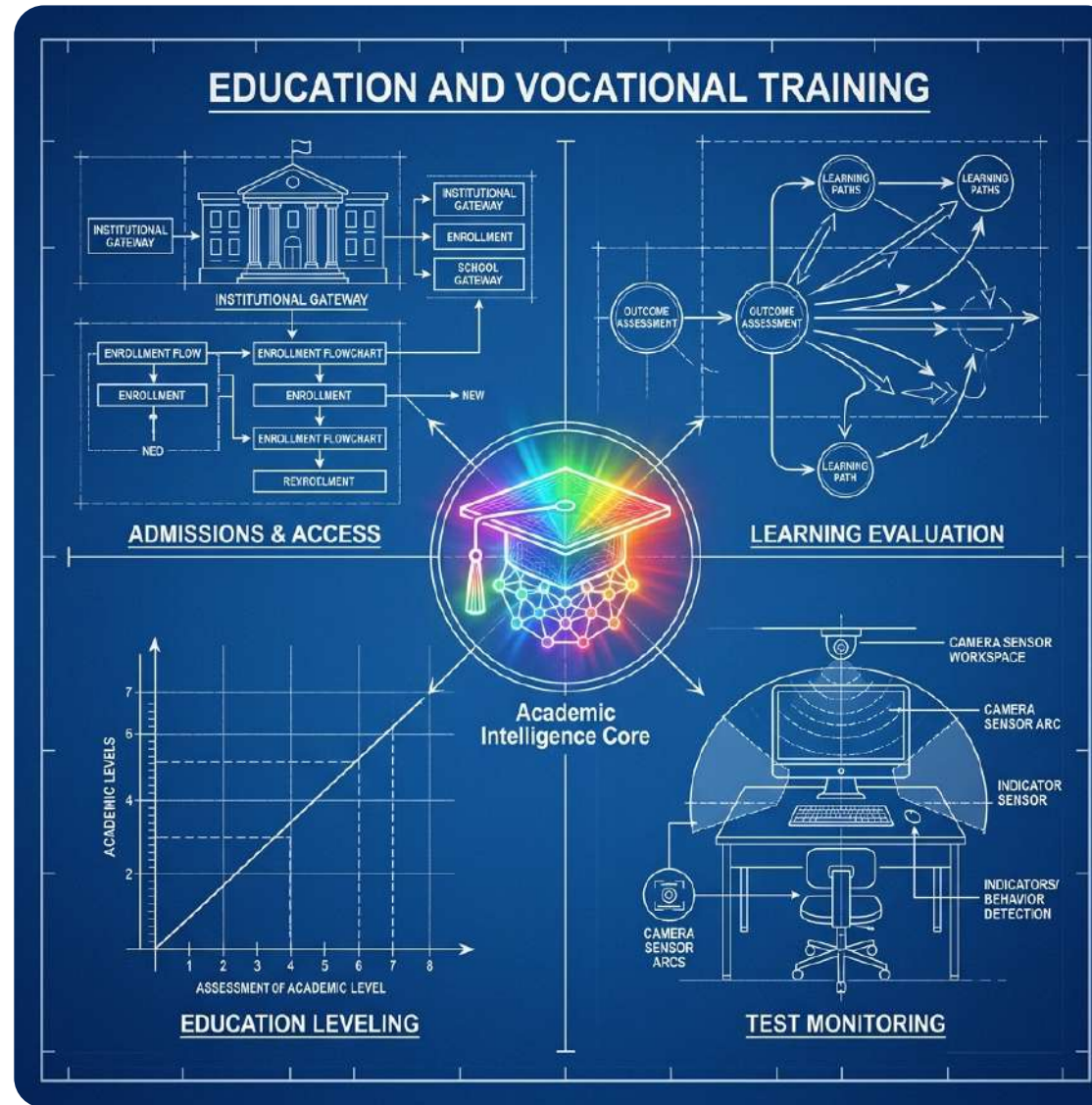
AI Act Annex I



AI GENERATED



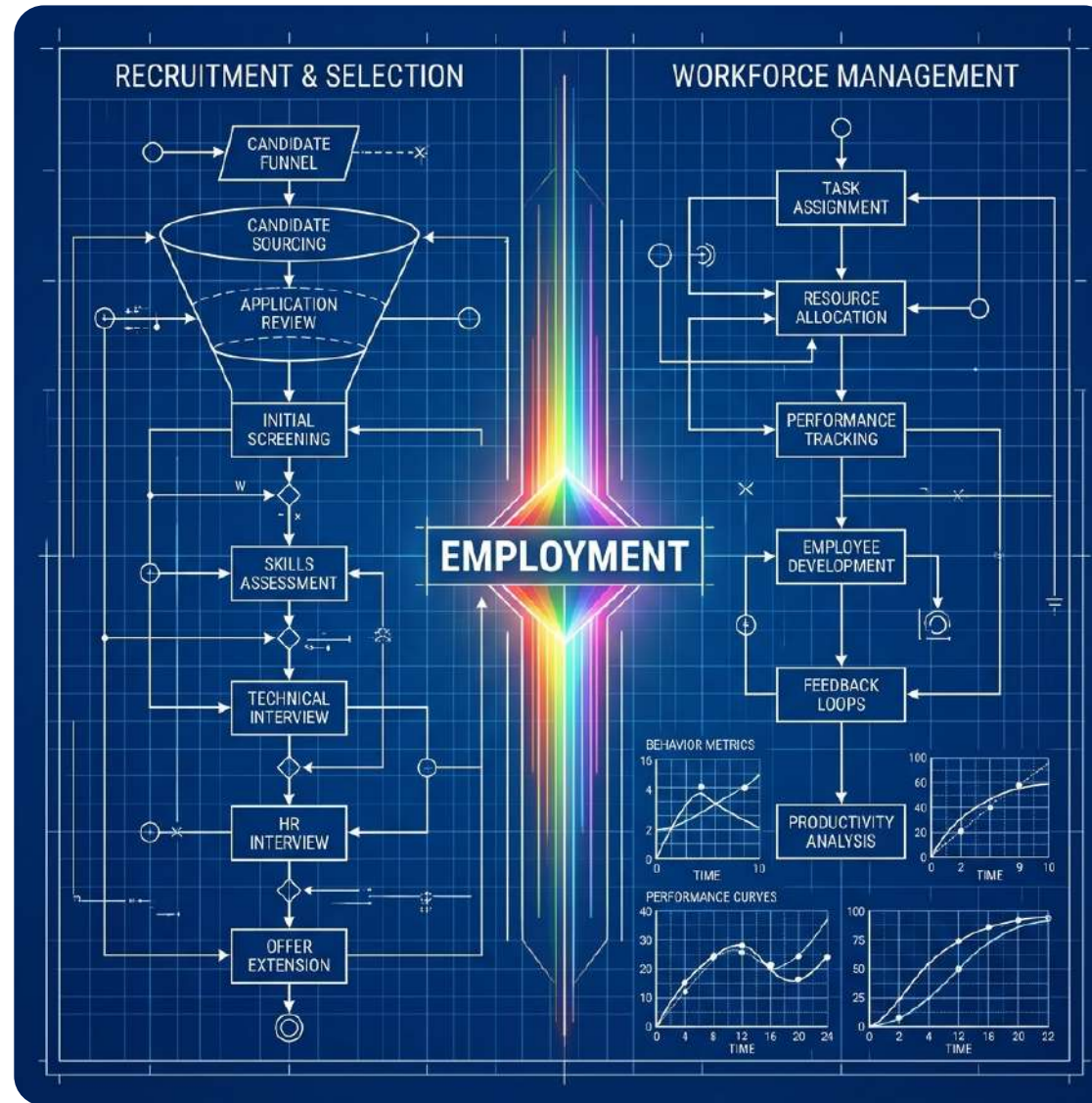
KI im Bildungsbereich = hochriskant



AI GENERATED



KI im Personalbereich = hochriskant



AI GENERATED



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



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



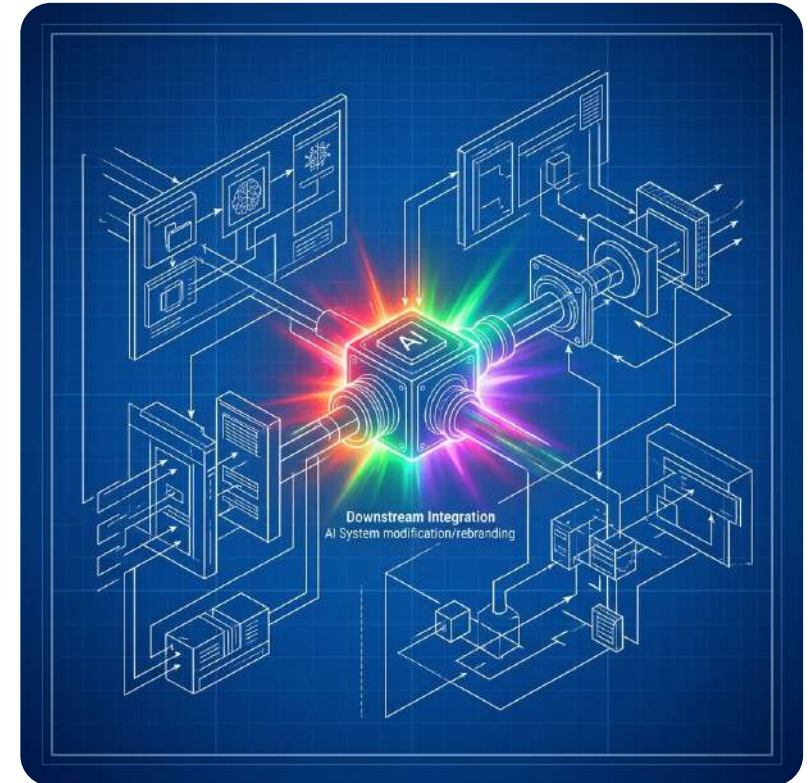
Nachgelagerte Anbieter

Verantwortlichkeiten (Art. 25)

Ketten-Haftung / Pflichtenübertragung

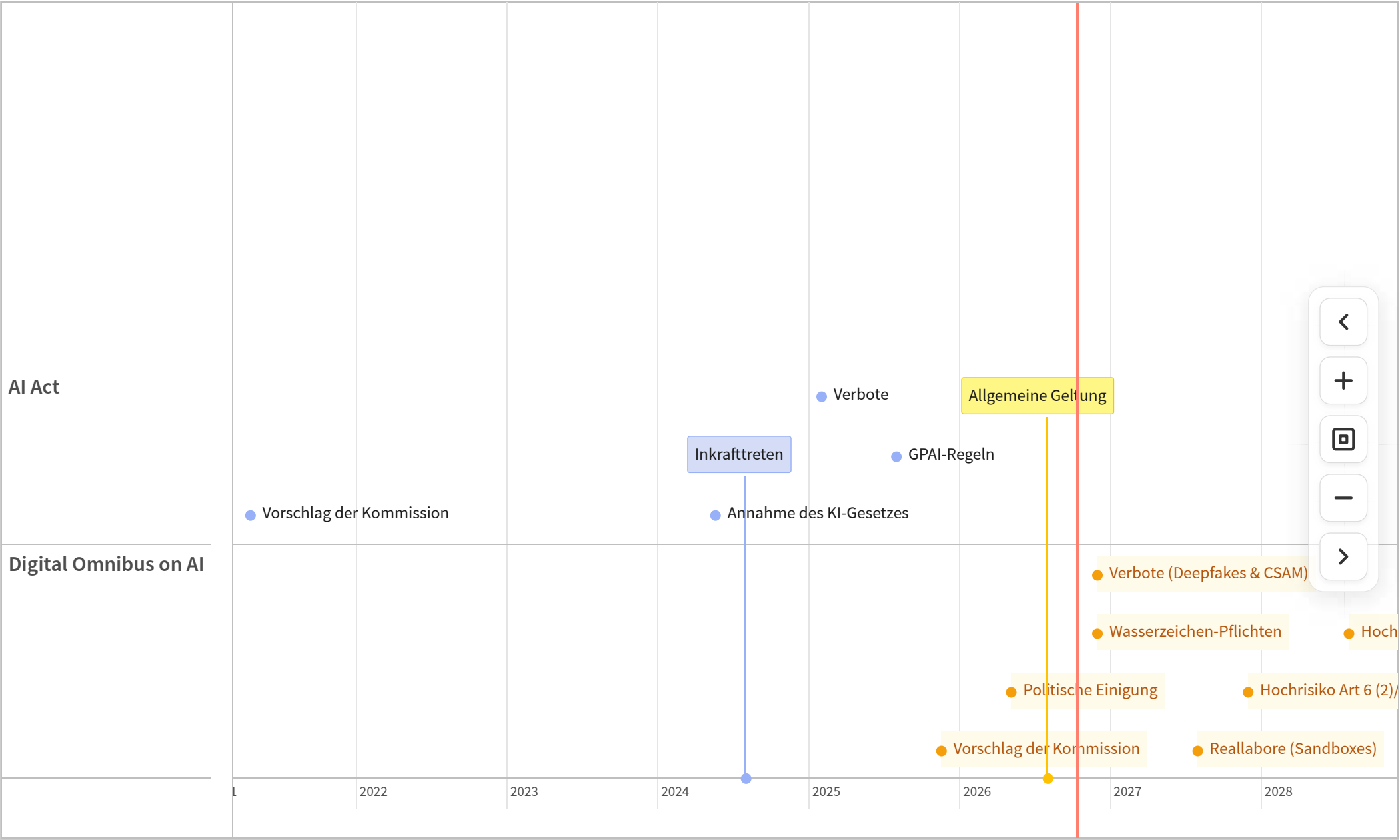
Dritte (Händler, Einführer, Betreiber etc.) gelten als **Anbieter eines Hochrisiko-KI-Systems** und unterliegen den vollen Anbieterpflichten (Art. 16), wenn sie:

- 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.



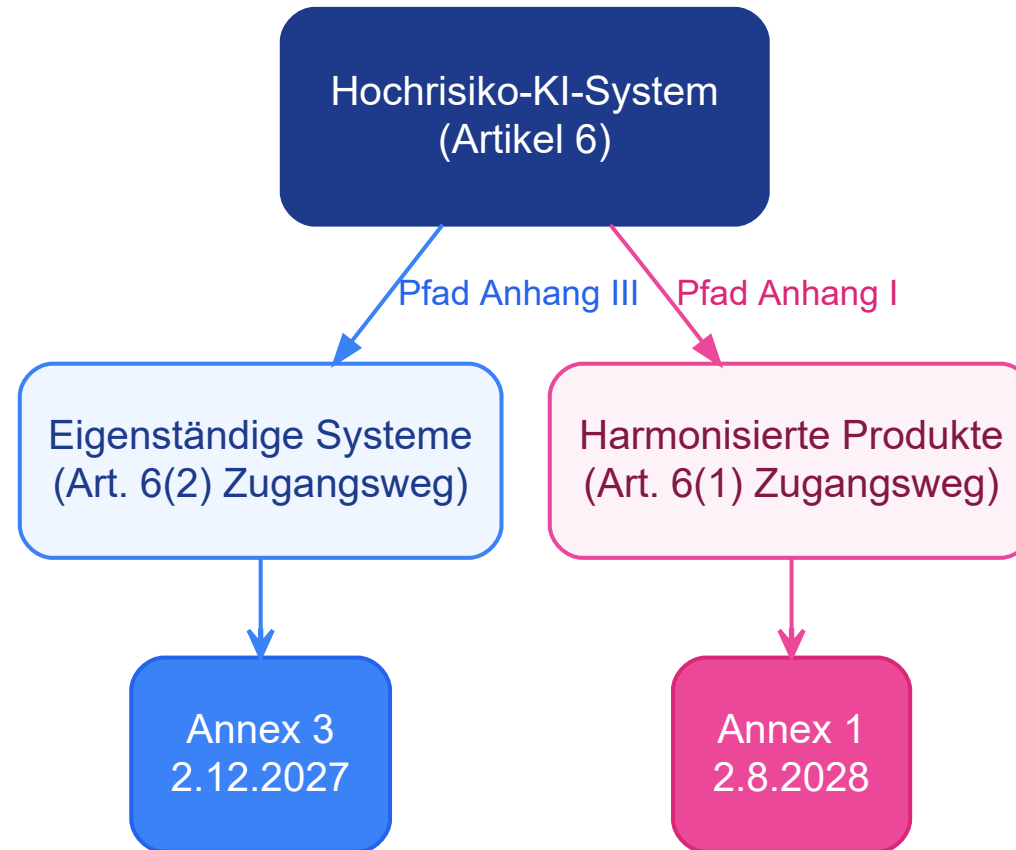
AI GENERATED





2. Aug. 2026: Die meisten Bestimmungen des KI-Gesetzes treten in Kraft.

Hochrisiko-KI Fristen



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

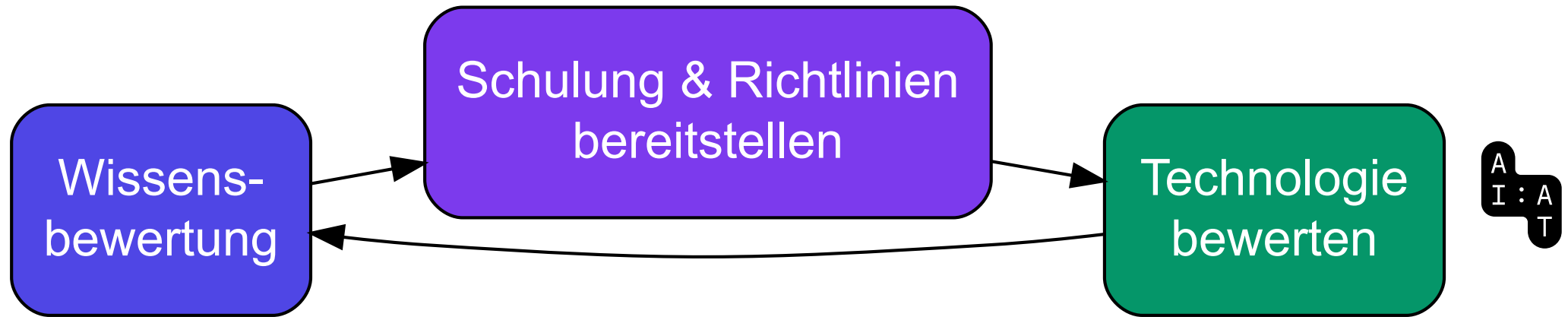


Zweifacher Zweck

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

KI-Kompetenz fördert Compliance und Wettbewerbsvorteil

Der eigentliche Treiber ist der Nutzen: Menschen müssen KI verstehen, um sie sicher und effektiv zu nutzen.



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.



Trainings & Webinars



[News](#) [Events](#) [Trainings](#) [Services](#) [Ecosystem](#) [Über uns](#) [FAQ](#) [in](#) [EN](#) [DE](#)

AI Factory Austria AI:AT

Trainings & Webinars

Die Trainings und Webinare der AI Factory Austria AI:AT machen KI nicht nur verständlich, sondern wirklich nutzbar. Von grundlegenden Konzepten über aktuelle Research-Breakthroughs bis zu realen Unternehmens-Use-Cases: Wir verbinden Theory, Code und Deployment. So entwickeln Fachkräfte, Führungsteams und Entwickler:innen die Skills, um KI zuverlässig in Produkte, Prozesse und Wertschöpfung zu integrieren und das von der Idee bis zum produktiven Stack.



AI:AT Selbstlernplattform

Lerne in deinem eigenen Tempo mit Videos, Infoblättern, Präsentationen, Quizen und mehr.

[Registrieren und mit dem Lernen beginnen →](#)



Live-Trainings

Lerne live mit unseren Expert:innen – in interaktiven Kursen, Webinaren und Workshops mit persönlichem Austausch und praxisnahen Inhalten.

[Trainings entdecken →](#)



Menschen müssen wissen, wann KI im Spiel ist¹

ART. 50 ABS. 1-2



Pflichten der Anbieter

- **Interaktion** — Nutzer darüber informieren, dass sie mit KI sprechen
- **Wasserzeichen** — KI-Ausgaben maschinenlesbar kennzeichnen

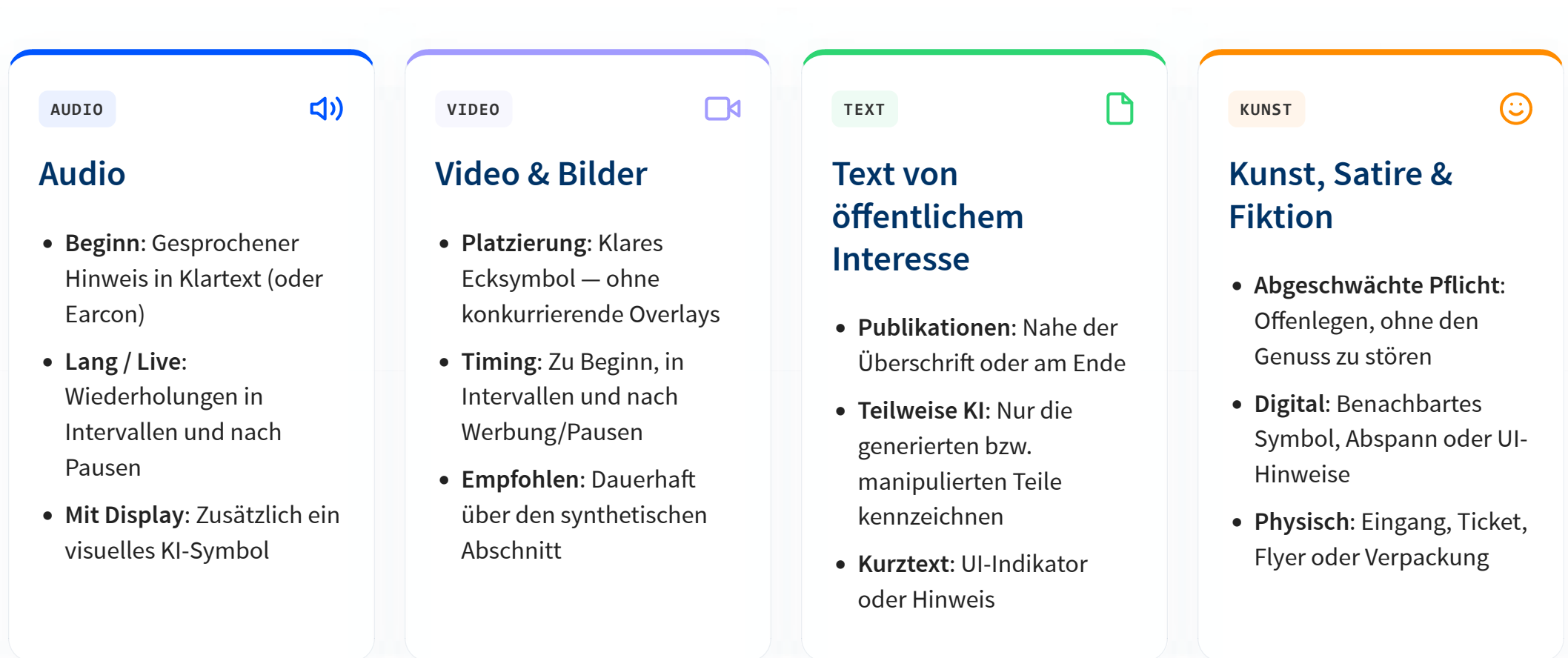
ART. 50 ABS. 3-4



Pflichten der Betreiber

- **Biometrie** — informieren, wenn Emotions- oder Kategorisierungssysteme laufen
- **Deepfakes & generierte Inhalte** — Deepfakes und synthetische Inhalte von **öffentlichem Interesse** offenlegen

Der Code of Practice regelt KI-Kennzeichnung nach Modalität¹



Offizielle EU-Icons zur Kennzeichnung¹

BASIS



Basissymbol

- KI war an Deepfake oder veröffentlichtem Text beteiligt
- Mit eigenem Textlabel oder interaktiver zweiter Ebene kombinieren

GENERIERT

AI GENERATED

Vollständig KI-generiert

- Gesamter Deepfake oder Text stammt von KI
- Keine menschlich geschaffenen Elemente außer Prompting

MODIFIZIERT

AI MODIFIED

Teilweise KI-modifiziert

- Vorgegebener menschlicher Inhalt teilweise mit KI verändert
- Ergebnis ist Deepfake oder Text von öffentlichem Interesse

Icons sind optional — die Erfüllung von Artikel 50 ist es nicht¹

CAVEAT



Icons ≠ Compliance

Icons sind optional. Die Kennzeichnung nach Art. 50 ist **verpflichtend**. Icons allein begründen **keine** Rechtskonformität.

PLATZIERUNG



Erste Exposition

Klar wahrnehmbar bei der **ersten Exposition**; keine störenden Overlays; in den Inhalt einbetten (oder gleichwertige UI), sodass die Marke bei Teilen und Download erhalten bleibt.

ZUGANG



Barrierefreiheit

Sichtbare Größe; klare Sprache; Alt-Text / ARIA; zeitlich begrenzte Hinweise lange genug lesbar; zweite Ebenen mit Assistenztechnik navigierbar.

Leitlinien & Ressourcen

👁️ Transparenz & Support

- [Verhaltenskodex zur Transparenz](#) KI-generierter Inhalte.
- [Art.-50-Transparenzleitlinien](#) — Scope & Auslegung.
- [EU-Icons zur Kennzeichnung](#) — optionales Icon-Set (Art. 50 Abs. 4).
- [Art.-50-FAQ](#) — Praxishilfe zu den Transparenzpflichten.
- [KI-Kompetenz-Repositorium](#) & [FAQ](#) (Art. 4).

❓ Anwendungsbereich & Definition

- [Leitlinien KI-System-Definition](#) — Anwendungsbereich.
- [Entwurf Hochrisiko-Klassifizierung](#) (Art. 6).
- [Leitlinien verbotene Praktiken](#) (Art. 5).
- [EDSA 28/2024](#) — Datenverarbeitung in KI-Modellen.
- [MDCG 2025-6](#) — MDR/IVDR ↔ KI-VO (AI Board/MDCG).

📄 Offizielle Vorlagen

- [Model Documentation Form](#) — GPAI-CoP Transparenz (Art. 53).
- [Zusammenfassung Trainingsdaten](#) — Art. 53 Abs. 1 lit. d.
- [GPAI-Schwerstvorfälle](#) — systemisches Risiko (Art. 55).
- [Entwurf Vorfallsmeldung](#) — Art. 73 (Hochrisiko).

AI Factory Austria AI:AT - PUBLIC – Michael Löffler

🛡️ GPAI-Rahmenwerk

- [GPAI-Verhaltenskodex](#) — Transparenz, Urheberrecht, Sicherheit.
- [Kommissionsstellungnahme](#) zur Angemessenheit des GPAI-Kodex.
- [Leitlinien Scope & Pflichten](#) für GPAI-Anbieter.
- [GPAI-FAQ](#) & [Kodex-FAQ](#).



Anwendungsfall aus der Forschungsverwaltung

Einsatz von KI zur Erstellung von Berichten und Ablegung in den jeweiligen Systemen

01 • ERSTELLEN



Berichte generieren

- KI entwirft Text, Tabellen oder Zusammenfassungen
- Typisch: Fortschritts-, Finanz- oder Compliance-Berichte

02 • ABLEGEN



In Fachsysteme einbringen

- Ablage in DMS, ERP, Förder- oder Forschungsportalen
- Dokument wird Teil der institutionellen Akte



Agenda: Datenschutz

01

Künstliche Intelligenz

Definition & Ausnahmen, Risikostufen, Hochrisiko (Bildung/Personal), Rollen, Fristen, KI-Kompetenz und Transparenz.

02

Datenschutz

Personenbezogene Daten, Anonymisierung, LLM-Deanonymisierung, Drittlandtransfer und Schatten-KI in der Verwaltung.

03

Urheberrecht

Input- und Output-Seite, rechtskonforme Workflows sowie Transparenz bei GenAI in der Forschung.



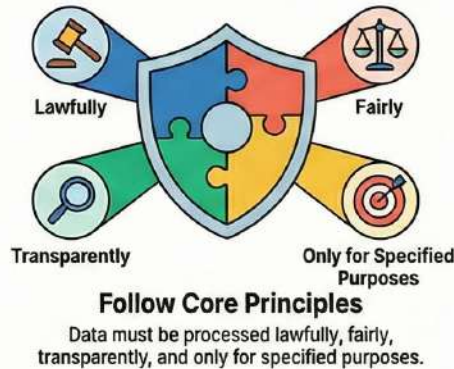
Hinweis: Schatten-KI und LLM-gestützte Deanonymisierung sind zentrale Risiken in der Forschungsverwaltung: Ohne AV-Vertrag, Transferprüfung und Freigabeprozesse drohen DSGVO-Verstöße und Datenabfluss.



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

AI:AT

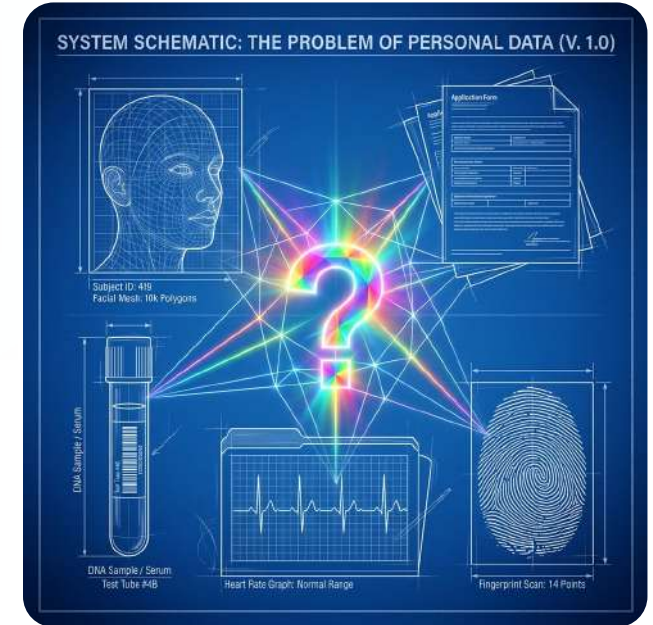
Was sind personenbezogene Daten?

ARTIKEL 4 NR. 1 DSGVO OFFIZIELLE DEFINITION

„**personenbezogene Daten**“ alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** beziehen [...]

💡 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.



AI GENERATED

“

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

— PAUL OHM ¹

”



LLM Deanonymization

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.



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.



Quelle: Art. 44 ff. DSGVO, EuGH (Schrems II), EU-US Data Privacy Framework (2023).

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.

Anwendungsfall aus der Forschungsverwaltung

Einsatz von KI zur Internetrecherche und Erstellung forschungsbezogener Dokumente

01 • RECHERCHIEREN



Forschungsdaten sammeln

- KI durchsucht und verdichtet Quellen aus dem Internet
- Typisch: Literatur, Fakten, Marktdaten, Hintergrundwissen

02 • GENERIEREN



Deliverables & Publikationen

- Entwürfe für Berichte, Deliverables oder Veröffentlichungen
- Menschliche Prüfung bleibt für Qualität und Quellenpflicht



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

AI:AT

Agenda: Urheberrecht

01 Künstliche Intelligenz

Definition & Ausnahmen, Risikostufen, Hochrisiko (Bildung/Personal), Rollen, Fristen, KI-Kompetenz und Transparenz.

02 Datenschutz

Personenbezogene Daten, Anonymisierung, LLM-Deanonymisierung, Drittlandtransfer und Schatten-KI in der Verwaltung.

03 Urheberrecht

Input- und Output-Seite, rechtskonforme Workflows sowie Transparenz bei GenAI in der Forschung.



Hinweis: Reine KI-Generate sind oft nicht urheberrechtlich geschützt; zugleich verlangen Fördergeber und Verlage zunehmend Offenlegung von GenAI in Researchoutputs – inklusive klarer Input-/Output-Workflows.

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

A
I
:
A
T

“

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

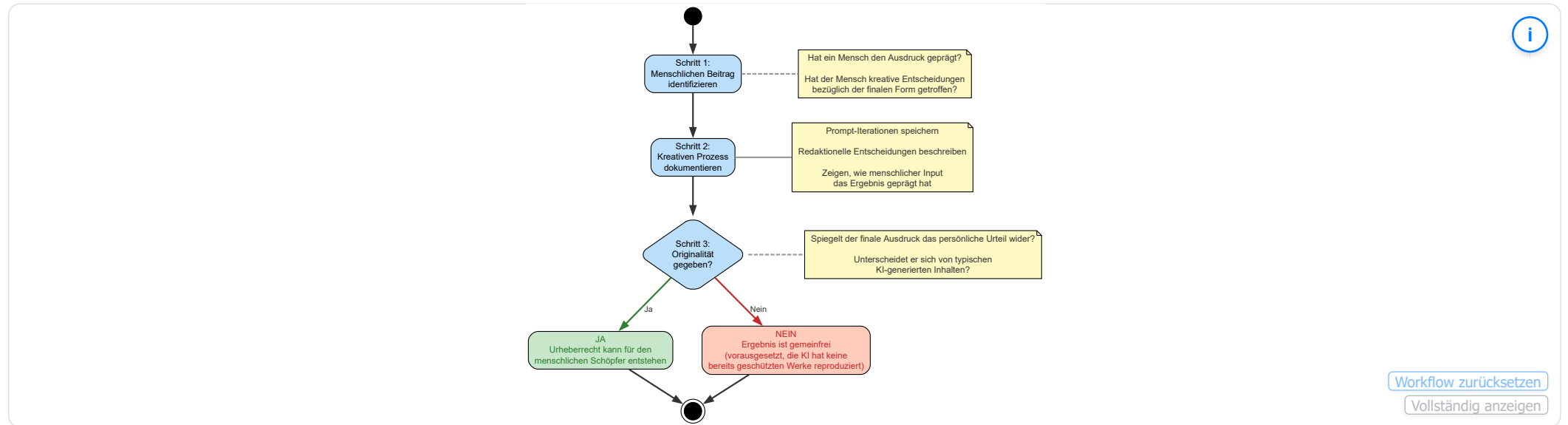


3. Pflichten & Opt-Outs

- **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-Kommission¹

- **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 Richtlinien²

- **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 WIEN³



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. European Commission. Directorate General for Research and Innovation., The use of generative artificial intelligence in research. (2025). ↩

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

3. Technische Universität 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>>. ↩

Anwendungsfall aus der Forschungsverwaltung

Einsatz von KI für E-Mail-Entwürfe, um die E-Mail-Flut zu bewältigen — KI bereitet Antwortvorschläge vor

01 • SICHTEN



Posteingang bewältigen

- KI fasst Anfragen zusammen und priorisiert
- Typisch: Förderfragen, Partneranfragen, interne Abstimmungen

02 • ENTWERFEN



Antwortvorschläge vorbereiten

- KI liefert Entwürfe in Ton und Kontext der Anfrage
- Mensch prüft, passt an und versendet bewusst



Compliance-Zusammenfassung

Regulierung



Risikoklassen & AI Act

- **Risiko-basiert:** Verbote (Art. 5), Hochrisiko, Transparenz, minimale Risiken.
- **Anhang III:** Bildung & Personal sind für Forschungseinrichtungen besonders relevant.
- **Fristen:** Omnibus-Timeline – Anhang III (Dez. 2027) vs. Anhang I (Aug. 2028).

Akteure



Pflichten & Rollen

- **Anbieter:** Qualitätsmanagement, technische Dokumentation, Konformität.
- **Betreiber:** Überwachung, Logging, Information & KI-Kompetenz (Art. 4).
- **Art. 25:** Wesentliche Änderungen → nachgelagerte Akteure werden selbst Anbieter.

Praxis



Literacy & Transparenz

- **KI-Kompetenz:** Schulungen für alle mit KI-Kontakt in der Verwaltung.
- **Art. 50:** Kennzeichnung KI-generierter Inhalte (Text, Audio, Bild, Video).
- **Forschung:** Offenlegung von GenAI in Outputs; Anwendungsfälle Berichte, Recherche, E-Mail.

Recht



DSGVO & Urheberrecht

- **Datenschutz:** Personenbezug, Anonymisierung, Deanonymisierung, Drittlandtransfer.
- **Schatten-KI:** Unkontrollierte Public-LLMs ohne AV-Vertrag und Freigabe vermeiden.
- **Urheberrecht:** Input-/Output-Workflows; reine KI-Generate oft nicht schutzfähig.



Compliance in drei Schritten

✓ KI-VO Risiko ermitteln

✓ Datenschutzcompliance herstellen

✓ Einhaltung des Urheberrechts sicherstellen



It's that simple

Contact



michael-löffler

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



This presentation was created with the help of agentic AI.

References

Ahmed/Cooper/Koyejo/Liang, [Extracting books from production language models](#),
01/06/2026

Bontcheva/Bechmann/Pedreschi/Gregorio/Riess/Botan, Code of Practice on
Transparency of AI-Generated Content,

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

—, Leitlinien der Kommission zum Umfang der Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung), 11/19/2025

European Commission, EU Icons for labelling AI-generated content | Shaping Europe's digital future, 06/10/2026 <<https://digital-strategy.ec.europa.eu/en/policies/eu-icons-labelling-ai-generated-content>>, aufgerufen am 06/18/2026

—, [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

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

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

Technische Universität 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