BIS§ET

digiCAFÉ
KI-Werkstatt

17.09.2025

BI§ET

RA Mag. Katharina Bisset, MSc

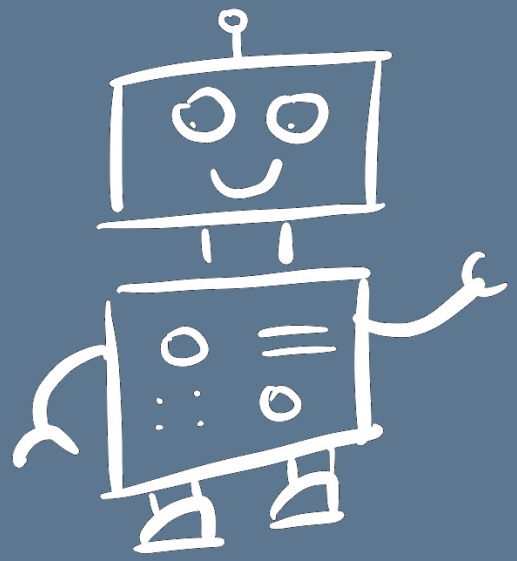
- Selbstständige Rechtsanwältin (IT/IP)
- Disziplinarrätin in der RAK Niederösterreich
- Co-Founderin Nerds of Law & NetzBeweis
- Lektorin FH Wr Neustadt

- Rechtswissenschaften (Mag.iur.)
- Business Process Engineering & Management (MSc)
- CIPP/E
- Creativity & Design Thinking (Stanford)
- Scrum Master PSM I, PMA Level D, Legal PM Associate, ISTQB Foundation Level, CPRE Foundation Level

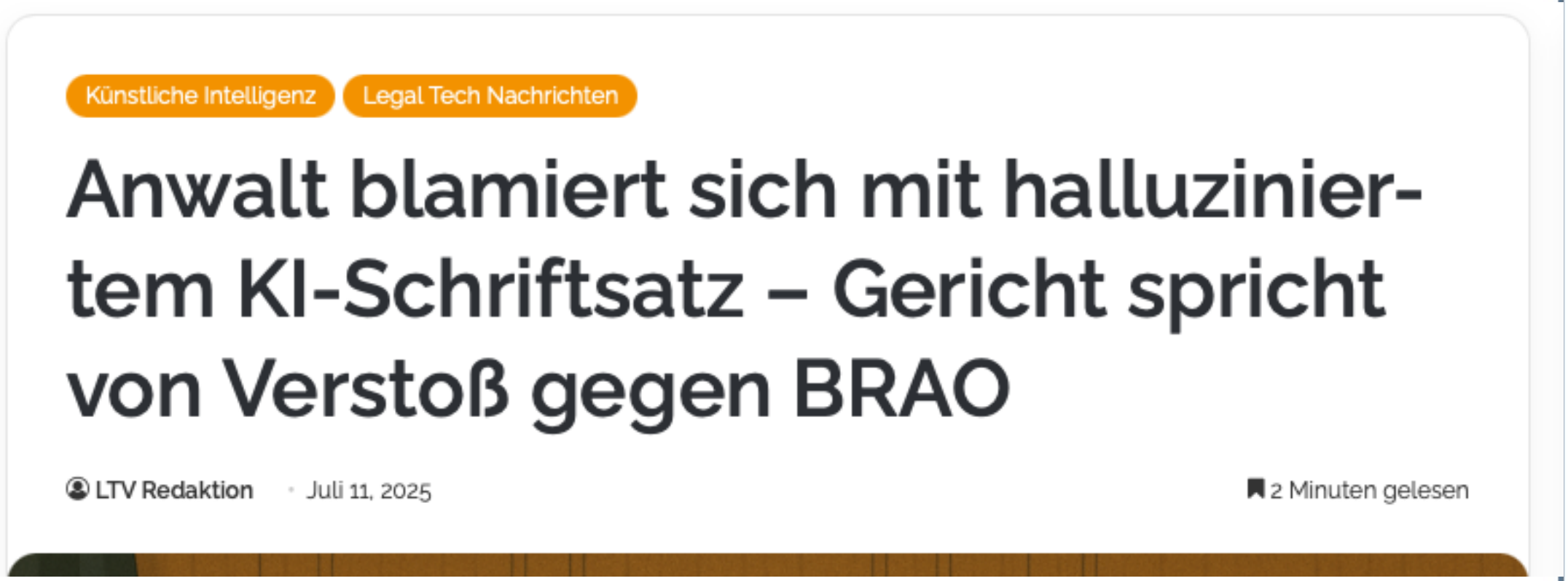
BI§ET

Recht

- Der AI Act
- KI und Datenschutz
- KI und Geschäftsgeheimnisse
- KI und Urheberrecht / IP
- KI und Haftung



BI§ET



Künstliche Intelligenz | Legal Tech Nachrichten

Anwalt blamiert sich mit halluzinier-tem KI-Schriftsatz – Gericht spricht von Verstoß gegen BRAO

LTV Redaktion · Juli 11, 2025 · 2 Minuten gelesen

https://legal-tech-verzeichnis.de/legal-tech-nachrichten/anwalt-blamiert-sich-mit-halluziniertem-ki-schriftsatz-gericht-spricht-von-verstoss-gegen-brao/

BI§ET

AI Act
Verordnung (EU) 2024/1689

ab 02.02.2025

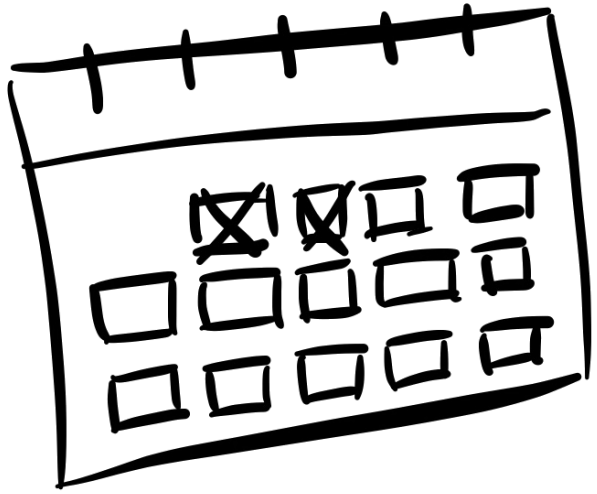
- Verbotene KI Praktiken
- **KI-Kompetenz (Art 4 AIA)**

ab 02.08.2025

- General Purpose AI
- Governance
- Strafen

ab 02.08.2026

- Restliche Verpflichtungen



BI§ET

Rollen im AI Act

BETREIBER [ist, wer] […] ein KI-System in eigener Verantwortung verwendet

Importeur, Händler, Representative,…

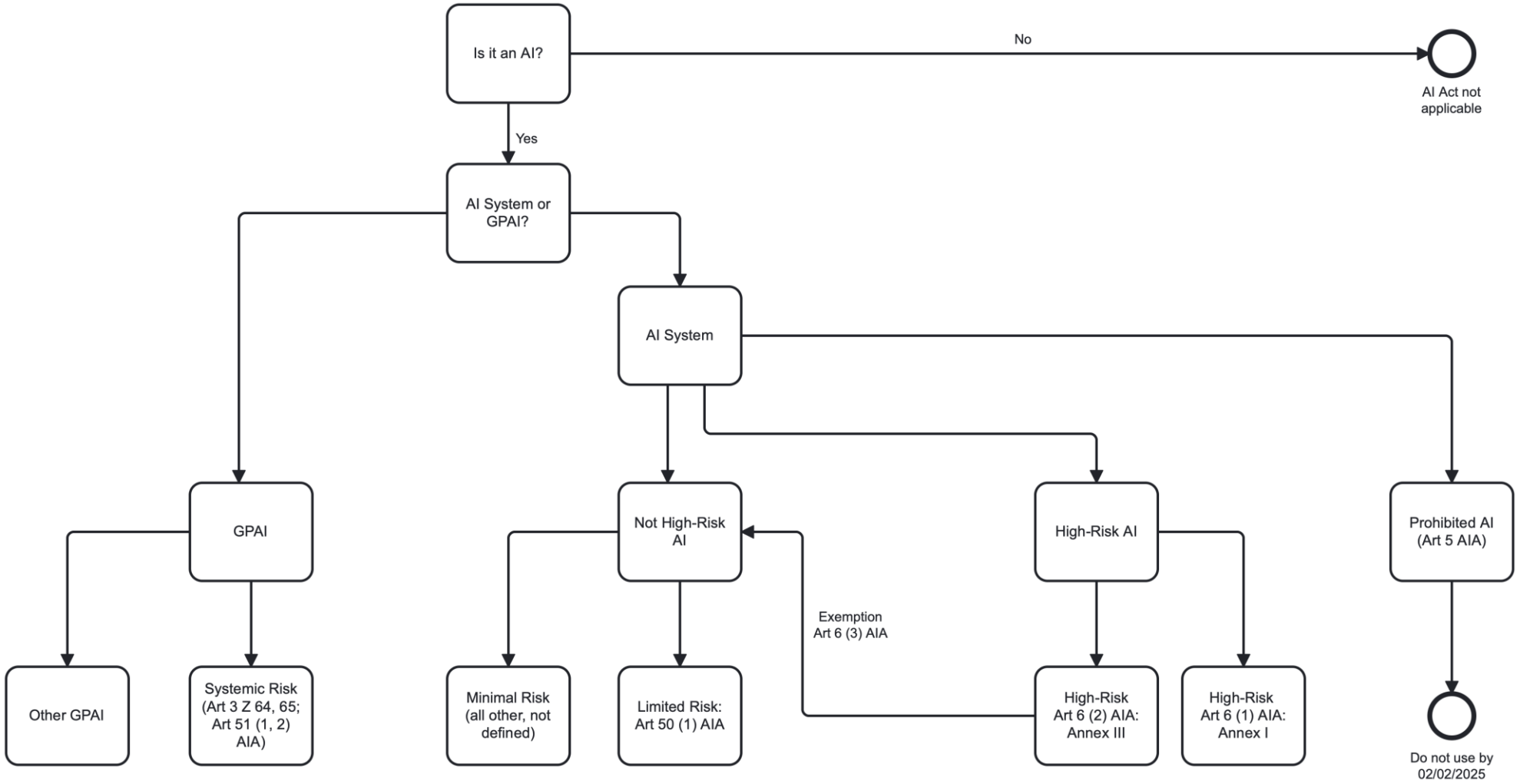
ANBIETER [**ist, wer**] […] ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck

1. **entwickelt oder entwickeln lässt** und
2. es unter ihrem eigenen Namen oder ihrer Handelsmarke […] **in Verkehr bringt** oder das KI-System […] in Betrieb nimmt […]

KI-Entwickler?

BI§ET

Welche KI ist reguliert?



BISET

AI Act: Risikostufen für KI-Systeme

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

BI§ET

Hochrisiko KI

KI im Arbeitsverhältnis

Bewerbungsverfahren

- die Einstellung oder Auswahl
- gezielte Stellenanzeigen
- Bewerbungen zu sichten oder zu filtern
- Bewerber zu bewerten

Arbeitsverhältnis am Ende

- Bedingungen von Arbeitsverhältnissen
- Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen
- Zuweisung von Aufgaben auf Grund individuellem Verhaltens, persönliche Merkmale oder Eigenschaften
- Beobachtung und Bewertung von Leistung/Verhalten

BISET

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 *sofern Arbeitgeber:in Hochrisiko-KI-Systeme am Arbeitsplatz einsetzt*	Art. 26 (7)		
Registrierungspflicht *sofern EU-Organe, EU-Einrichtungen und sonstige EU-Stellen*	Art. 26 (8), 49		
Genehmigungspflicht einer Justiz- oder Verwaltungsbehörde *sofern Einsatz zur nachträglichen biometrischen Fernidentifizierung*	Art. 26 (10)		
Erstellung einer Grundrechte-Folgenabschätzung *sofern u. a. öffentl. oder private Einrichtungen öffentliche Dienste erbringen*	Art. 27		

Anbieter
Entwickelt KI und vertreibt diese

Betreiber
Nutzung der KI in eigener Verantwortung (nicht privat)

BISET

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)		
Bennenung Bevöllmächtigter (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				

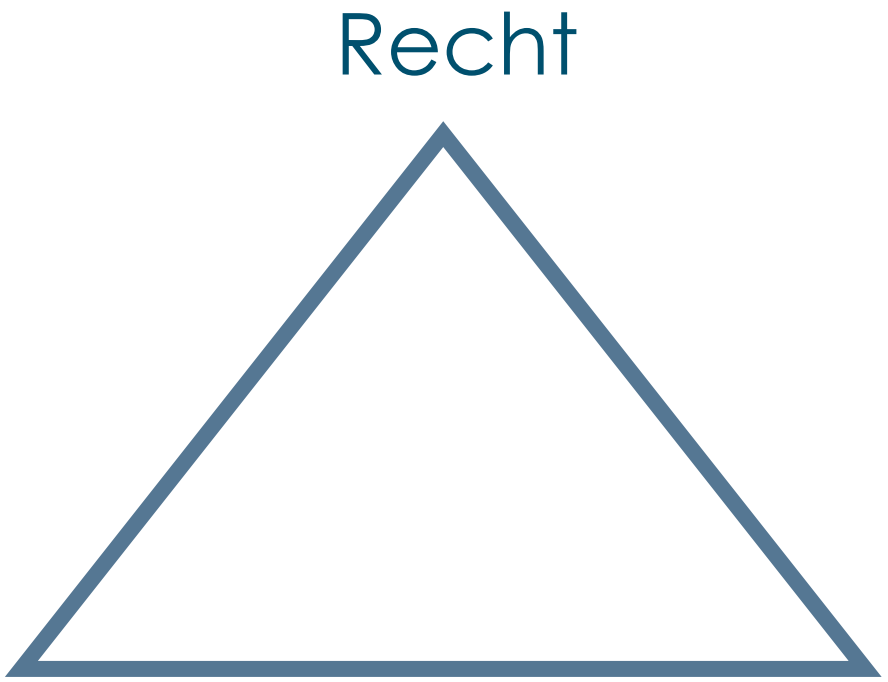
KI-Servicestelle ki.rtr.at **RTR**

BI§ET

KI Kompetenz

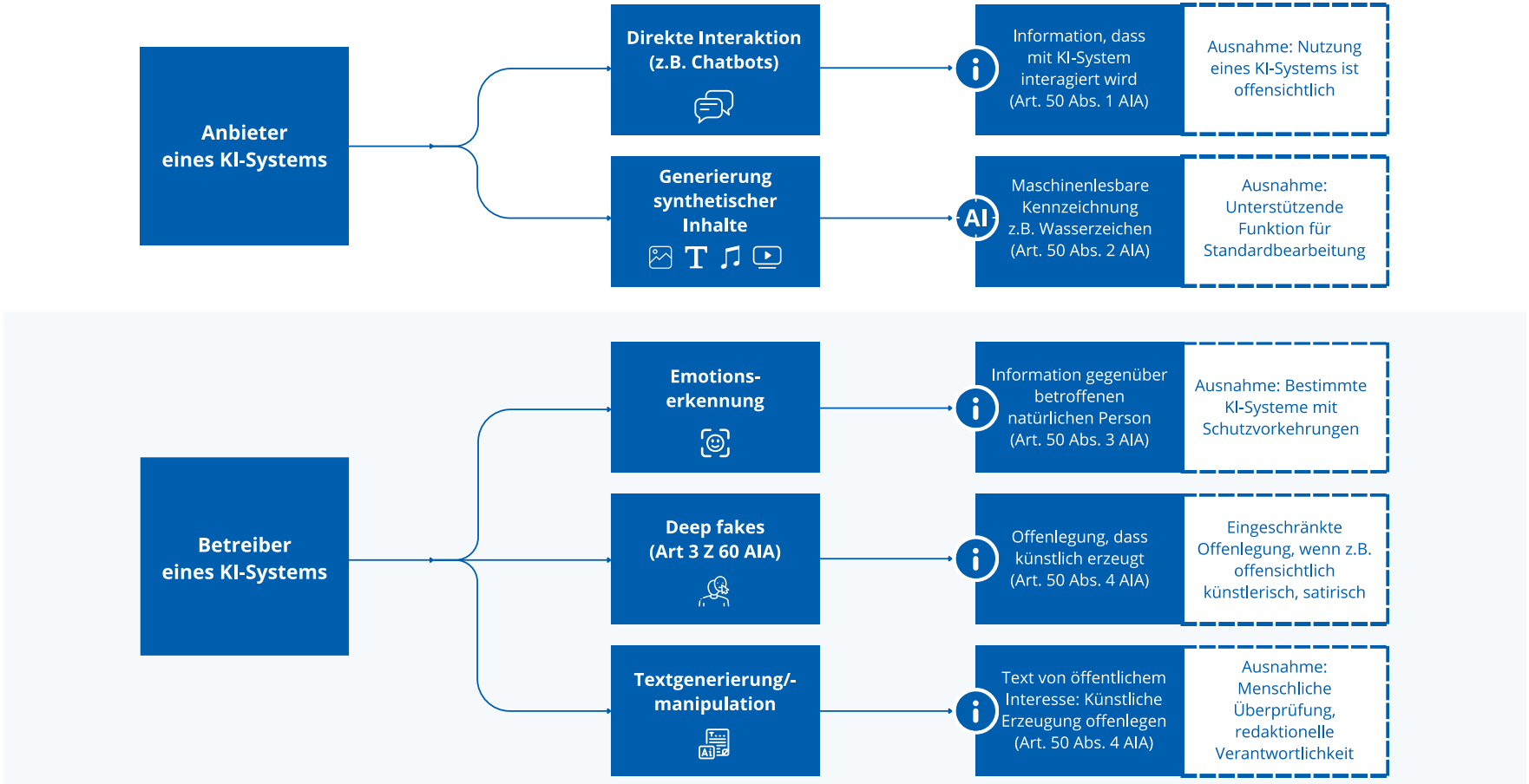
Art 4 AIA

- Für Betreiber und Anbieter
- Gilt seit 02.02.2025



AI Act: Transparenzpflichten

KI-Systeme mit begrenztem Risiko lösen Informations-, Offenlegungs- und Kennzeichnungspflichten aus



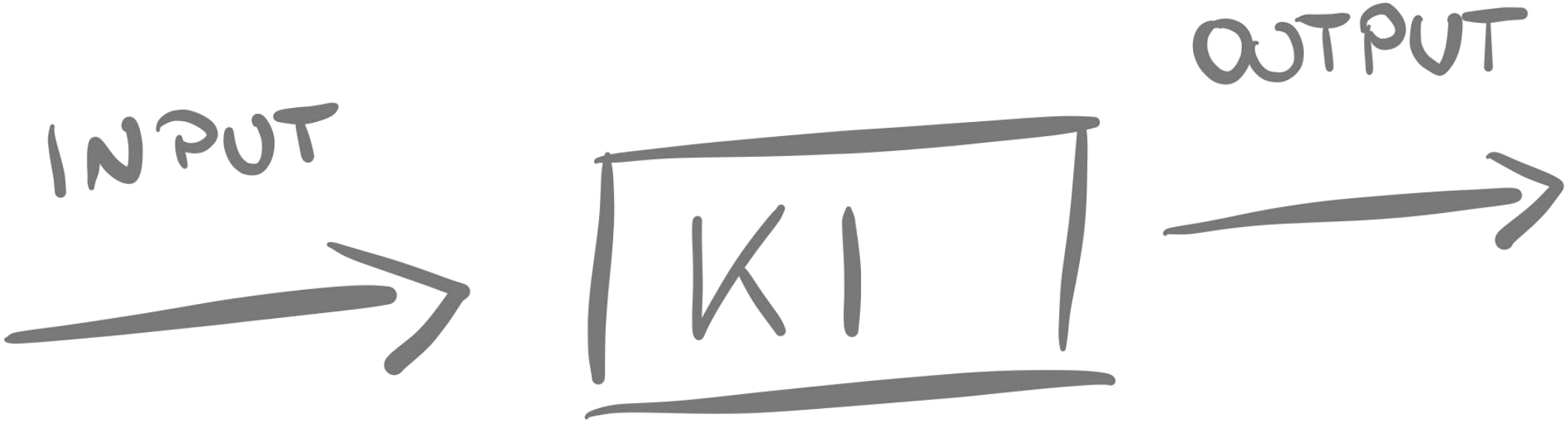
BISET

Nur der AI Act?

nicht auf den Rest vergessen!

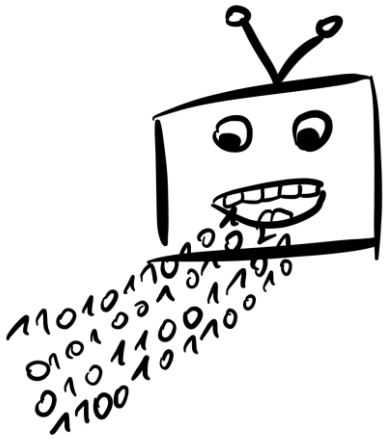
BI§ET

Was darf ich mit der KI machen?



BI§ET

Datenschutz - Training

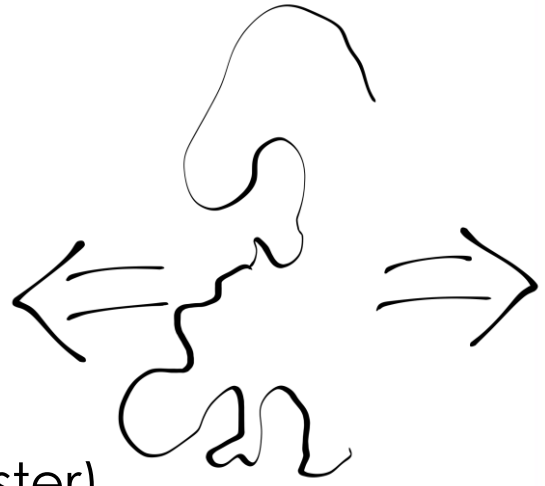


Zu beachten:

- Training nicht vom Zweck der ursprünglichen Verarbeitungstätigkeit umfasst
- Eigene Rechtsgrundlage erforderlich
- Möglichkeit des überwiegenden berechtigten Interesses (EDPB Opinion; Art 6 Abs 1 lit f DSGVO)
  - LIA – Legitimate Interest Assessment
  - Für sensible Daten nicht möglich
- Betroffenenrechte (Löschung, Informationspflichten, …) praktisch schwer einzuhalten

BI§ET

Datenschutz - Input



Vorabfragen:

- Sollen personenbezogene Daten eingegeben werden?
- Prüfung des Anbieters wie jeden anderen (zB Cloud Dienstleister)
- Wo gehen die Informationen, die eingegeben werden, hin?
- Anbieter in der EU? Außerhalb der EU?
- Geheimhaltung und Datenschutz gewährleistet?
- Wird mit den Informationen weitertrainiert?

To Dos:

- Festlegen, welche Daten in welche KI-Systeme eingegeben werden dürfen
- Vereinbarungen mit Dienstleistern abschließen (Geheimhaltung, AVV,…)

BI§ET

Datenschutz - Output

To Dos:

- Ist die Nutzung Automatisierte Entscheidung im Einzelfall (Art 22 DSGVO)?
- Muss ein DPIA durchgeführt werden?
- Sind die Daten im Output korrekt?

Automatisierte Entscheidung im Einzelfall:

- Profiling (Bewertung persönlicher Aspekte)
- Entscheidung hat rechtliche Wirkung (zB Chatbot)
- Erheblich benachteiligt

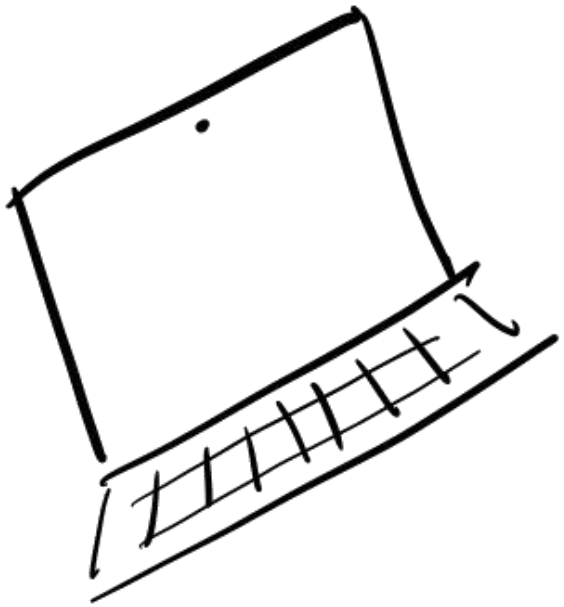
BI§ET

Geschäftsgeheimnisse

Auch Daten ohne Personenbezug können Geschäftsgeheimnisse enthalten!

Was ist ein Geschäftsgeheimnis?

- Geheim
- Von kommerziellem Wert
- Angemessene Geheimhaltungsmaßnahmen (!)



BI§ET

Urheberrecht / IP: Training

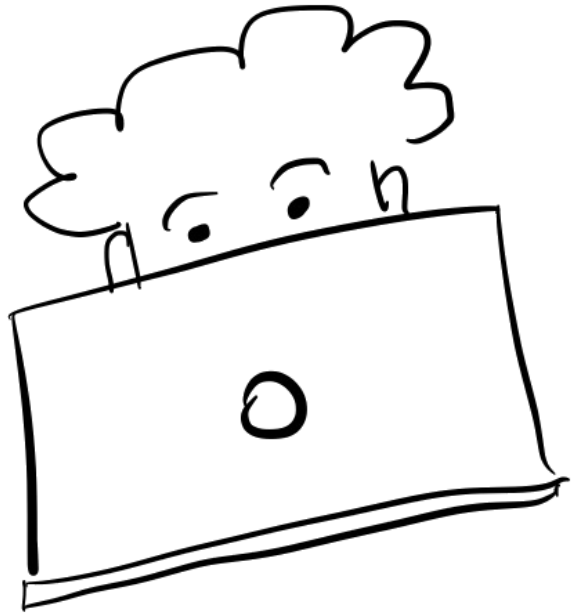
- **Rechte des Urhebers:** u.a. Verwertung, Vervielfältigung, Verbreitung, Namensnennung…
- **Text and Data Mining:** Ausschlüsse beachten, nicht für andere Medien, Nutzungsvorbehalte, kommerziell in Praxis schwierig
- **USA:** Verfahren zu Urheberrechtsverstößen durch KI- Training anhängig (Text, Bild, Source Code) –> Outputs teilweise ident zu Trainingsdaten!
- **GPAI:** Policy für Copyright und allg. IP Compliance
- **Training eigener Systeme:** IP-Rechte einholen!

BI§ET

Urheberrecht / IP: Input

Fragen:

- Wird mit den Inputs weitertrainiert?
- Wird mit den Prompts weitertrainiert?



Optionen:

- Nutzung ohne (Weiter-)Training
- RAG als Alternative
- Training eigener Systeme (meist unrentabel)
- Festlegen, welche Inhalte eingegeben werden dürfen!

BI§ET

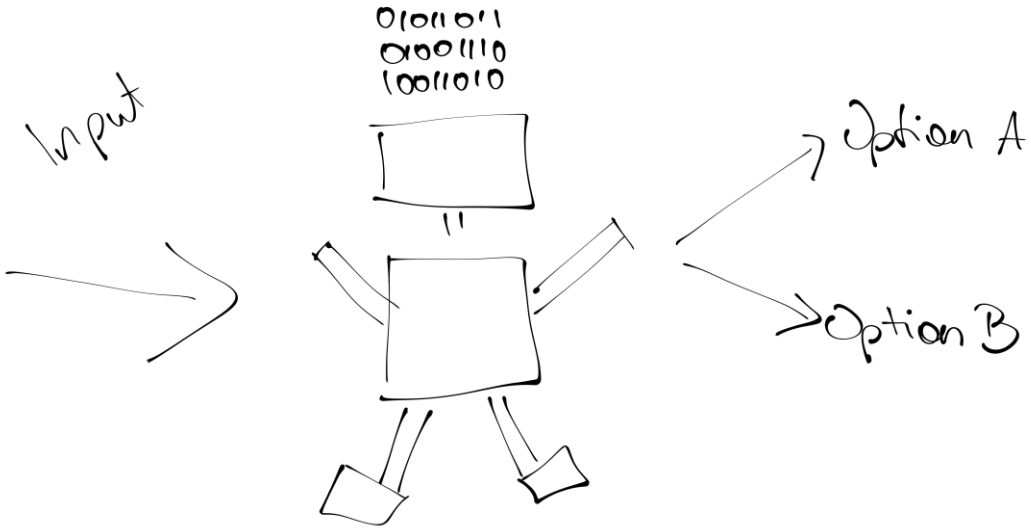
Urheberrecht / IP: Output

- Werden Outputs verwendet, die Urheberrechte verletzen, haftet der sie benutzt hat gegenüber Rechteinhaber!
- Regress an Anbieter oft schwierig
- Werden Logos generiert, müssen diese trotzdem auf bestehende Marken/Kennzeichnen überprüft werden
- Output nach hM nicht urheberrechtlich geschützt

- **Optionen:**
- Bearbeiten, um Schutz zu erreichen
- Outputs als Inspiration, nicht 1:1 übernehmen

BI§ET

Haftung



Deliktischer vs vertraglicher Schadenersatz

Voraussetzungen und Herausforderungen

- Schaden
- Verursacht → kausal?
- Rechtswidrig
- Verschulden → vorwerfbar?

→ **eine Frage der Beweise**

BI§ET

Was kann ich mit den Outputs tun?

Falsche Info von Airline-Chatbot führte zu teurem Ticket (16.02.2024)
https://futurezone.at/produkte/airline-chatbot-unnoetig-teure-flugtickets-air-canada-kuenstliche-intelligenz/402781174

- Vorsicht vor Falschinformationen!
- Risiko von Outputs, die Rechte Dritter verletzten
- Menschliche Kontrolle

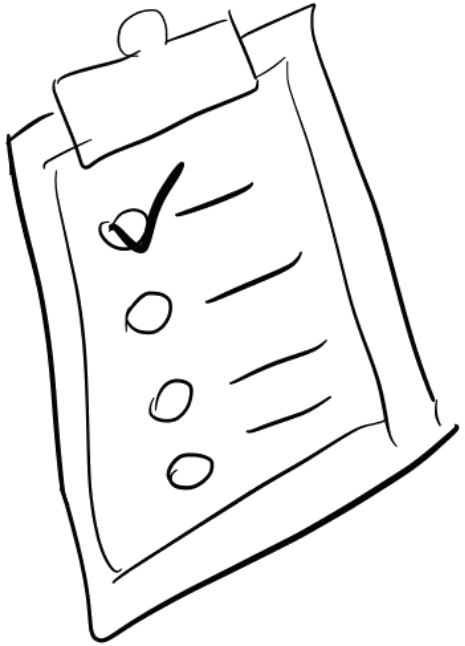
BISET

Organisation

BI§ET

Check für Betreiber

Ist wirklich KI im Tool?



- Datenschutz-Check
- Für welchen Zweck soll es verwendet werden?
- Wird mit den Inputs weitertrainiert?
- Qualität, Funktionalitäten, Bias,…
- Haftungsregelungen (insbesondere für IP)
- Funktionalitäten: Bias, Halluzinationen, …
- Implementierung in Guidelines für Input und Output

BISET

Noch Fragen?

BI§ET

Danke für Ihre Aufmerksamkeit!