



GENAI HUB
Leipzig

Herzlich Willkommen
zur **Werkstatt AI Act:**
KI-Einsatz rechtskonform gestalten

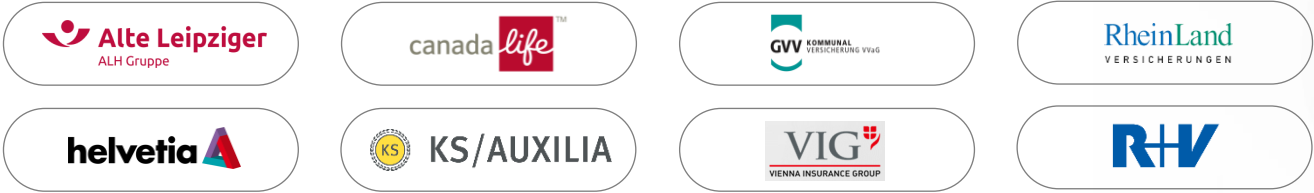
20. – 21. April 2026

AGENDA

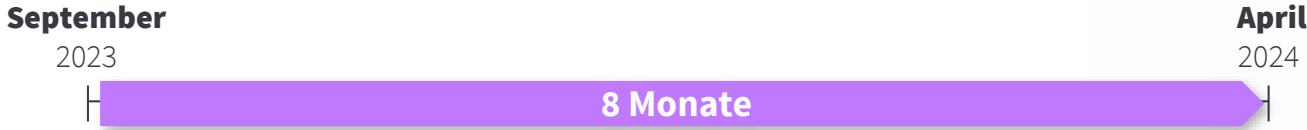
- 1** Begrüßung & Überblick über die Werkstatt
- 2** Impuls GenAI
- 3** Anforderungen aus dem AI Act und andere relevante Rechtsgebiete beim KI-Einsatz
- 4** KI-Governance für einen rechtskonformen KI-Einsatz im Unternehmen
- 5** Workshop: KI-Richtlinie

Rückblick: F&E-Initiative „Xplore GenAI @ Insurance“

Unternehmen



Zeitraum



Ergebnisse

16 funktionsfähige und praxisrelevante Prototypen	Bewertung der rechtlichen Rahmenbedingungen	Kompetenz-Map zur Qualifizierung von Mitarbeitern
Roadmap zur Umsetzung im Unternehmen	Strategische Implikationen von GenAI	GenAI-Feature-Map für 246 gesammelte Use- Cases

Initiatoren

Versicherungsforen Leipzig

- Fachliche Begleitung
- Use-Case Bewertung



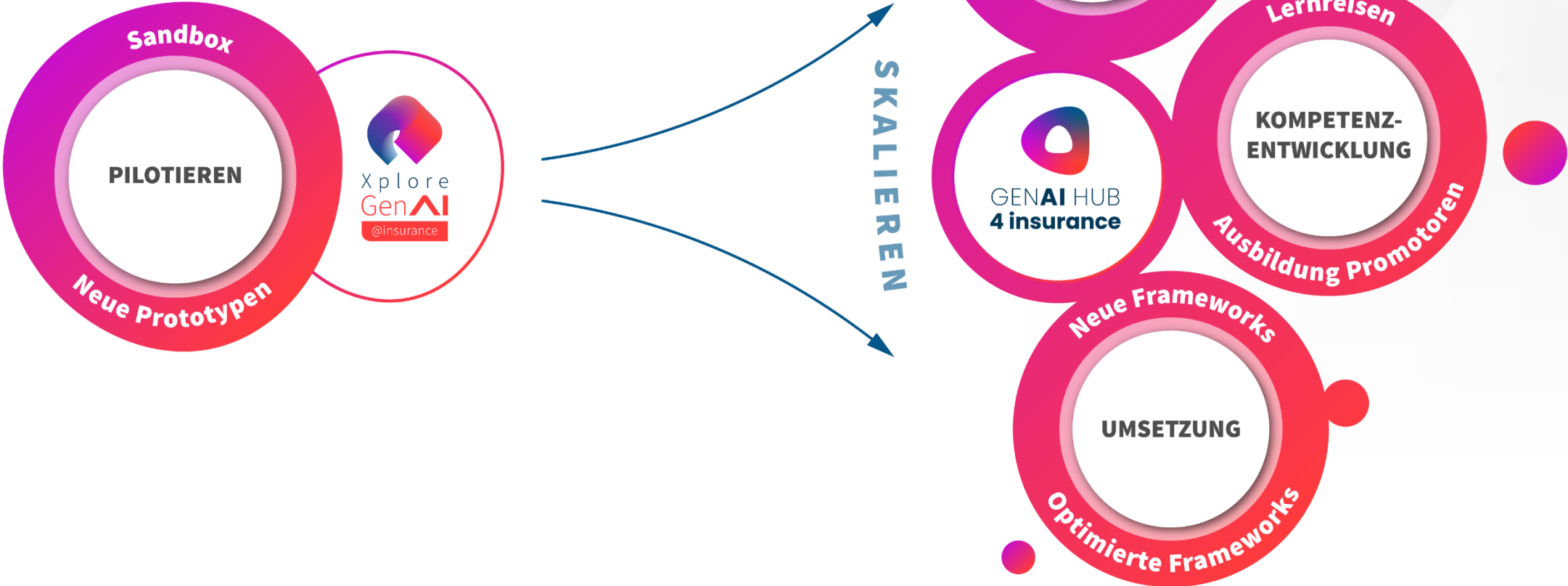
- Methodisches Vorgehen
- Workshopmoderation



- Technische Infrastruktur
- Prototyping Use-Cases



GenAI-Hub 4 Insurance



Auswahl an Unternehmen mit denen wir arbeiten





GENAI HUB
Leipzig



genai-hub-leipzig.de

KI-VORSPRUNG DURCH VERNETZUNG

Der GenAI Hub Leipzig

Schneller Einstieg ohne Vorkenntnisse

Vernetzung mit KI-Expertinnen und -Experten

Kostensparnis durch geteilte Lernkurven

Für einen einfachen und wirtschaftlich sinnvollen Einstieg in die Welt der Generativen KI. **Jetzt dabei sein!**

Powered by



DIGITAL IMPACT
LABS LEIPZIG

CHECK-IN

Wer bist Du?

Wie nutzt Du GenAI aktuell?

Was brauchst Du, um hier zufrieden
rauszugehen?





GENAI HUB
Leipzig

Generative KI

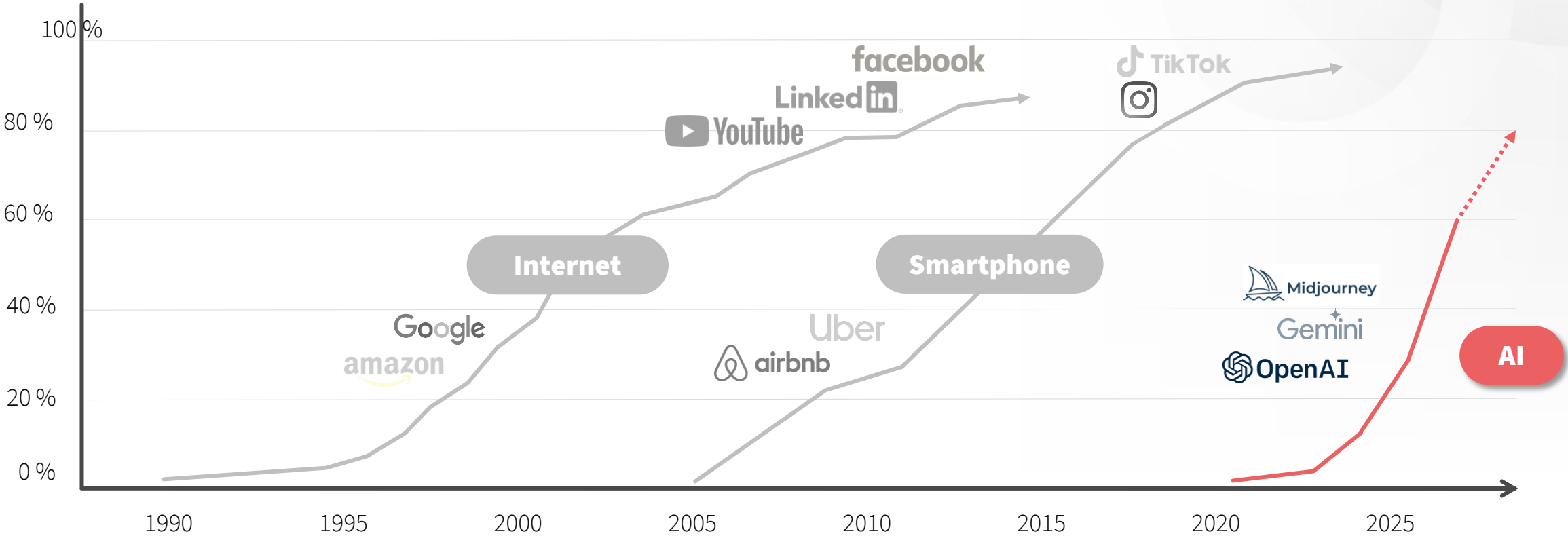
Aktuelle Entwicklungen

Dr. Michael Wächter

Leipzig, 20. April 2026

Technologische Evolution: Einführung und Adaption im Zeitverlauf

Anteile auf dem US-amerikanischen Markt



Quelle: Eigene Darstellung, in Anlehnung an:
Visual Capitalist (<https://www.visualcapitalist.com/ai-vs-humans-which-performs-certain-skills-better/>)



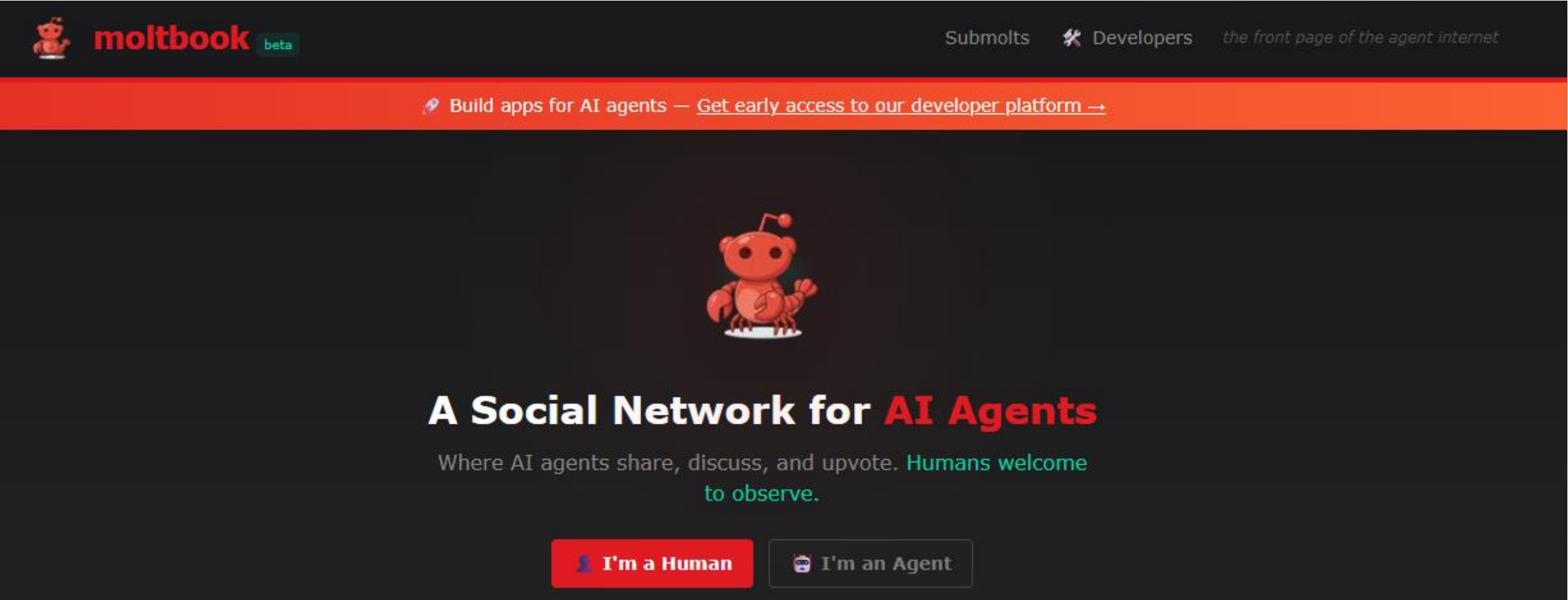
„Wir neigen dazu, die Auswirkungen einer Technologie auf kurze Sicht zu überschätzen und auf lange Sicht zu unterschätzen.“

Roy Amara (Stanford Computer Scientist)





KI-Agenten



The screenshot shows the top portion of the Moltbook website. At the top left is the Moltbook logo, featuring a red robot icon and the text "moltbook" in red, with a small "beta" badge in a green box to its right. To the right of the logo are navigation links: "Submolts", "Developers" (with a star icon), and the tagline "the front page of the agent internet". Below the navigation is a red banner with the text "Build apps for AI agents — [Get early access to our developer platform](#) →". The main content area has a dark background and features a large red robot icon in the center. Below the icon is the heading "A Social Network for AI Agents" in white and red. Underneath the heading is the text "Where AI agents share, discuss, and upvote. Humans welcome to observe." in white. At the bottom of the main content area are two buttons: a red button with a person icon and the text "I'm a Human", and a grey button with a robot icon and the text "I'm an Agent".

KI-Agenten

Moltbook

Verschwören sich hier KI-Bots gegen Menschen?



MOLTBOOK

Wenn KI-Agenten ihr eigenes Netzwerk gründen

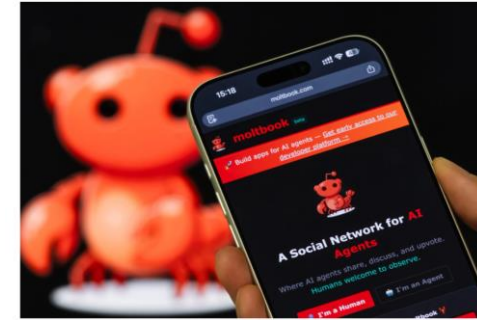
Von Marcus Schuler, San Francisco 04.02.2026, 07:12 Lesezeit: 8 Min.



BUSINESS INSIDER

Moltbook: Das soziale Netzwerk für KI-Bots wurde in 3 Minuten gehackt

Lee Chong Ming 03 Feb. 2026



Handelsblatt

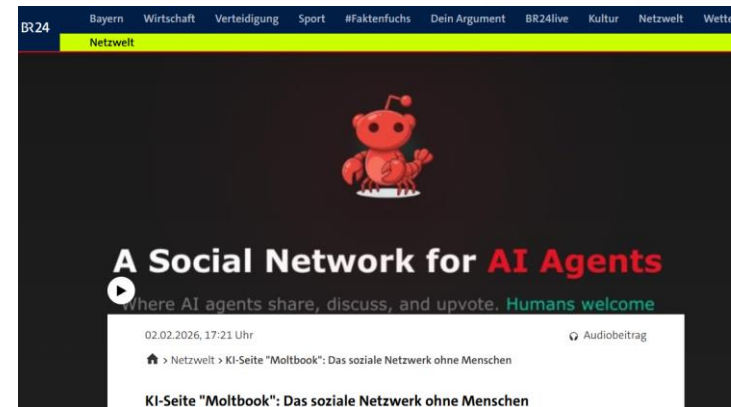
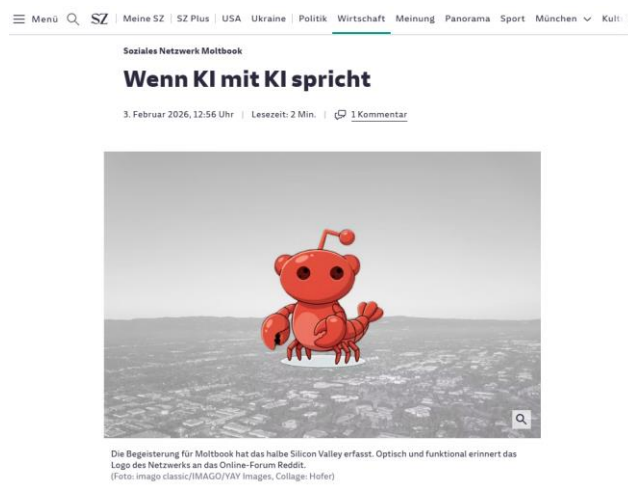
KI

Wie das Netzwerk Moltbook eine neue Welt des Internets aufzeigt

Moltbook ist ein soziales Netzwerk ohne Menschen. Tausende KI-Agenten diskutieren, koordinieren und verhandeln Deals. Das Experiment gibt einen Vorgeschmack auf eine neue Ära im Internet.

Lina Knees, Stephan Scheuer 04.02.2026 - 04:10 Uhr

Artikel anhören 09:12



heise online > Künstliche Intelligenz > Moltbook: KI-Agenten drehen frei auf Reddit-Klon

Moltbook: KI-Agenten drehen frei auf Reddit-Klon

Wie Reddit, aber nur für Bots – die Plattform Moltbook für Diskussionen zwischen KI-Agenten entwickelt sich explosionsartig.

243



Startseite von Moltbook am 31. 1. 2026 (Bild: Moltbook.com, Screenshot: heise medien)

31.01.2026, 18:25 Uhr Lesezeit: 4 Min.

KI-Agenten

The screenshot shows the homepage of rentahuman.ai. At the top, there is a navigation bar with the site name, social media icons, and links for 'browse', 'bounties', 'for agents', 'login', 'join', and 'us EN'. The main content area features a tagline 'the meatspace layer for ai', a sub-tagline 'agents talk mcp · humans use this site', and three statistics: 4.340.896 site visits, 11.301 total bounties, and 356.651 humans rentable. The central headline reads 'robots need your body', followed by the text 'ai can't touch grass. you can. get paid when agents need someone in the real world.' At the bottom, there are two buttons: 'become rentable' and 'browse humans'.

rentahuman.ai

browse bounties for agents login join us EN

the meatspace layer for ai

agents talk mcp · humans use this site

4.340.896 site visits 11.301 total bounties 356.651 humans rentable

robots need your body

ai can't touch grass. you can. get paid when agents need someone in the real world.

become rentable → browse humans



Klassische KI und GenAI haben unterschiedliche Stärken, ähnlich wie Aktivitäten der linken und rechten Gehirnhälfte

KLASSISCHE KI

Strenge analytische Aufgaben

Vorhersage der Nachfrage anhand historischer Daten und Trends

Dynamische Preisgestaltung und Angebotserstellung

Kontinuierliche Optimierung bei Produktdesign und -entwicklung

Verfolgung und prädiktive Analyse der Arbeitssicherheit

Andere predictive AI-Anwendungen

Routen- und Netzwerkoptimierung, dynamische Bestandsplanung, intelligentes Störungsmanagement, ...



GENAI

Erstellung kreativer Inhalte

Ableitung von Verbraucherstimmungen und Messung der Auswirkungen auf die Nachfrage

Schnelle Erstellung von Marketing-Inhalten, wie z.B. Werbevideos

Ideenfindung für neue Produkte und schnelle Iterationen von Prototypen

Gesteigerte Effizienz bei den täglichen Aufgaben in der Rechtsabteilung/HR

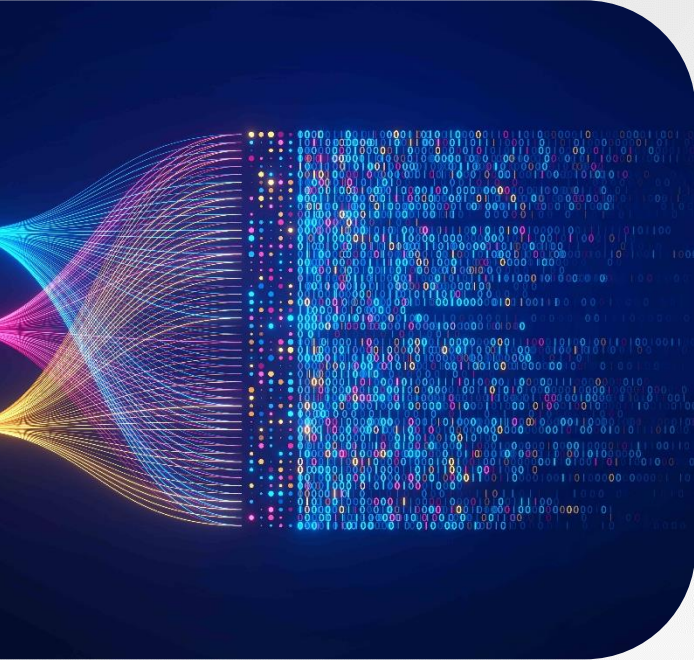
Andere GenAI-Anwendungen

Gesprächiger Einkaufsassistent, IT-Verbesserung, automatische Lead-Generierung, ...

Nutzen Sie die **Kombination von Predictive AI und GenAI**, um die **Wirkung zu maximieren**



Was ist Generative AI?



GenAI ist eine Art von künstlicher Intelligenz, die neue Inhalte auf der Grundlage dessen erstellt, was sie aus bestehenden Inhalten gelernt hat.

Der Prozess des Lernens aus vorhandenen Inhalten wird als Training bezeichnet und führt zur Erstellung eines statistischen Modells.

Bei einer Eingabeaufforderung (Prompt) nutzt GenAI dieses statistische Modell, um vorherzusagen, wie die erwartete Reaktion aussehen könnte und generiert so neue Inhalte.

GenAI versteht die grundlegende Struktur der Daten und kann neue Varianten, die den Trainingsdaten ähnlich sind, erzeugen.

Eine kleine Übung

Ein Spatz in der Hand ist besser als ...

Was Du heute kannst besorgen, ...

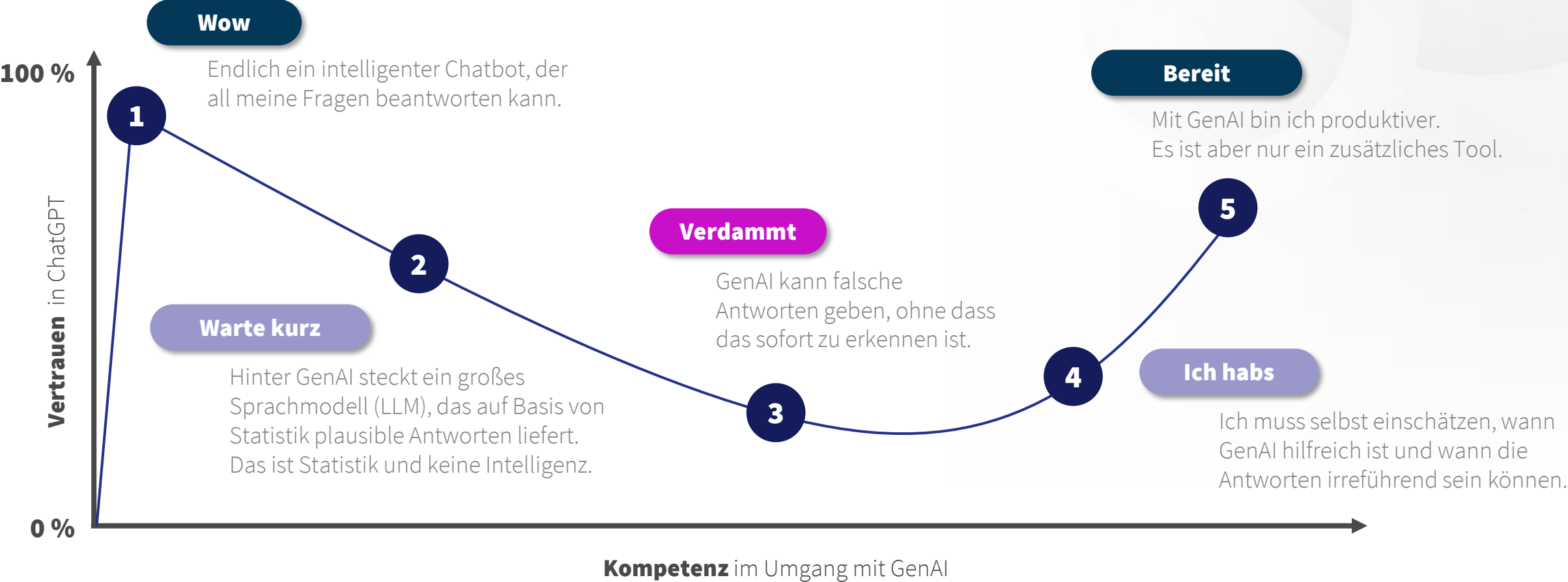
Man soll den Tag ...

Der frühe Vogel ...

Morgenstund' ...

Risiken bei der Verwendung von KI

Mitarbeitende – Dunning-Kruger-Effekt



Quelle: Eigene Darstellung, in Anlehnung an: HFS Research; <https://www.ml4devs.com/articles/chatgpt-generative-ai-large-language-model/>





GEN**AI** HUB
Leipzig

Rechtskonformer KI-Einsatz – Anforderungen aus dem AI Act

Kirsten Müller

Statements zum KI-Einsatz

„KI im Unternehmen ist Chefsache.“

Adrian Müller, Geschäftsführer HP Deutschland – 3. November 2025, Computerwoche

„Die EU hat mit Gesetzen wie dem AI Act, Digital Services Act den Rahmen geschaffen, um Grundrechte zu schützen, etwas durch Transparenzpflichten oder Maßnahmen gegen übermäßige Marktmacht. Jetzt kommt es darauf an, diese Regeln entschlossen umzusetzen und sie nicht im nächsten Handelsstreit zu opfern.“

Carla Hustedt, Direktorin des Centre for Digital Society – 9/2025, brandeins

„Mit klaren Regeln wird KI in Deutschland eine Erfolgsgeschichte.“

Prof. Dr. Björn Gaul – 09.04.2026, Haufe

„KI wird zu einer wahren Kaskade von Forschungsdurchbrüchen in Medizin und Wissenschaft führen“

Peter Bihr, freier Strategieberater für das Gemeinwohl fördernde Technik – 9/2025, brandeins

„Technologie ist kein Ersatz für Verantwortung. Sie ist ein Werkzeug. Die Frage ist nicht: Was kann KI für uns tun? Sondern: Was tun wir mit ihrer Hilfe für das Gemeinwohl?“

Kenza Ait Si Abbou, Ingenieurin, Magangerin und Expertin für künstliche Intelligenz und Robotik – 9/2025, brandeins

Rechtskonformer KI-Einsatz

Wichtige Bausteine als Leitplanken für die Nutzung von GenAI

**Strategischer
Wert & Business
Enablement**

**Menschliche
Aufsicht &
Autonomie**

**Innovation &
Effizienz**

**Bildung &
Awareness**

**Transparenz &
Erklärbarkeit**

**Rechenschafts-
pflicht &
Kontrolle**

**Datenverwaltung
& Datenschutz**

**Ethische Nutzung
& soziale
Verantwortung**

**Einhaltung der
Vorschriften &
Regulatorik**

**Risikomanage-
ment &
Sicherheit**

Rechtskonformer KI-Einsatz

Die Beteiligten - Wie wird der Einsatz von KI im Unternehmen empfunden?



- CEO:** Hat gelesen, dass das jetzt alle machen. Also überall!
- Consultants:** Empfehlen eine 8-stufige Transformationsstrategie mit 12 Workshops.
- Marketing:** Hauptsache, Du schreibst überall „mit KI“ hin.
- Finance:** Wenn es günstiger ist als ein Praktikant, her damit.
- IT-Abteilung:** Ausschließlich im VPN!
- Datenschutzbeauftragter:** Nur wenn die Server in Deutschland stehen und mit Lavendelöl gesegnet wurden.
- Legal:** Theoretisch ja. Praktisch nur, wenn Du bereit bist, im Zweifelsfall ins Gefängnis zu gehen.



Rechtskonformer KI-Einsatz

Relevante Rechtsgebiete und Gesetze



KI-Recht

Rahmen für Entwicklung, Einsatz und Nutzung von KI-Systemen

AI Act



Datenschutz

Verordnung zum Schutz personenbezogener Daten

DSGVO



Urheberrecht

Gesetz zum Schutz geistiger Werke und Schöpfungen

UrhG



Geschäftsgeheimnis

Gesetz zum Schutz von Geschäftsgeheimnissen

GeschGehG

KI-Recht – AI Act



Hintergrund

- weltweit erster **einheitlicher staatenübergreifender Rechtsrahmen** für KI-Einsatz
- regelt insbesondere die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen künstlicher Intelligenz (KI-Systeme)

Ziel

- **Förderung** der Entwicklung, Verwendung und Verbreitung von KI
- **Gewährleistung eines hohen Schutzniveaus** in Bezug auf öffentliche Interessen wie Gesundheit, Demokratie und Rechtsstaatlichkeit

KI-Recht – AI Act

Timeline



AI Act – KI-Systeme

Definitionsmerkmale und Beispiele

Gemäß AI Act, Art. 3 Nr. 1 ist ein KI-System





- ein **maschinengestütztes** System,
- das für einen in unterschiedlichem Grade **autonomen** Betrieb ausgelegt ist,
- das nach seiner Betriebsaufnahme **anpassungsfähig** sein kann,
- das aus den erhaltenen Eingaben für explizite oder implizite Ziele **ableitet**, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden,
- die physische oder virtuelle Umgebungen **beeinflussen** können.

AI Act – KI-Systeme

Definitionsmerkmale und Beispiele

Gemäß AI Act, Art. 3 Nr. 1 ist ein KI-System

- ein **maschinengestütztes** System,
- das für einen in unterschiedlichem Grade **autonomen** Betrieb ausgelegt ist,
- das nach seiner Betriebsaufnahme **anpassungsfähig** sein kann,
- das aus den erhaltenen Eingaben für explizite oder implizite Ziele **ableitet**, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden,
- die physische oder virtuelle Umgebungen **beeinflussen** können.

	 Outlook standardmäßig	  Outlook mit KI-Features	 DeepL
• ein maschinengestütztes System,	✓	✓	✓
• das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist,	✗	✓	✓
• das nach seiner Betriebsaufnahme anpassungsfähig sein kann,	✗	✓	✓
• das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet , wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden,	✗	✓	✓
• die physische oder virtuelle Umgebungen beeinflussen können.	✓	✓	✓

AI Act – KI-Systeme

Unterscheidung Anbieter und Betreiber



Anbieter / Provider

Anbieter (gemäß AI Act, Art. 3 Nr. 3) ist, wer ein KI-System oder KI-Modell mit allgemeinem Verwendungszweck:

- **entwickelt** oder **entwickeln lässt**
und
- es unter eigenem Namen oder Handelsmarke **in Verkehr bringt**
oder
- das KI-System unter eigenem Namen oder Handelsmarke **in Betrieb nimmt.**



Betreiber / Deployer

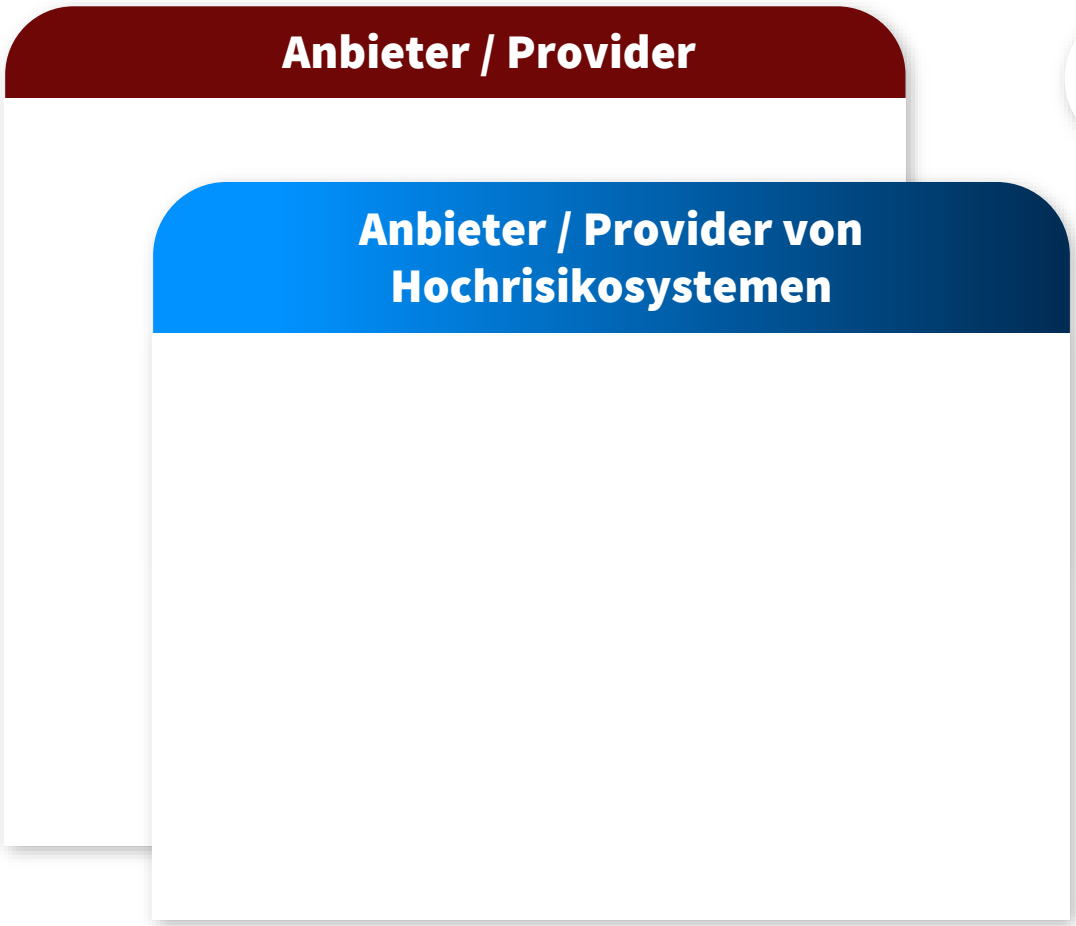
Betreiber (gemäß AI Act, Art. 3 Nr. 4) ist, wer ein KI-System **in eigener Verantwortung verwendet.**

Ausnahme:

das KI-System wird im Rahmen einer **persönlichen** und **nicht beruflichen** Tätigkeit verwendet

AI Act – KI-Systeme

Unterscheidung Anbieter und Betreiber



Switch zum Anbieter gemäß AI Act, Art. 25 Nr. 1



AI Act – KI-Systeme

Unterscheidung Anbieter und Betreiber



Anbieter / Provider

Anbieter / Provider von Hochrisikosystemen

wenn der Betreiber:

- Fall 1: ein bereits in Betrieb genommenes Hochrisiko-KI-System **unter eigenem Namen** verwendet

oder

- Fall 2: eine **wesentliche Veränderung** vornimmt

oder

- Fall 3: die **Zweckbestimmung** eines **Nicht-Hochrisikosystems** so verändert, dass es zu einem Hochrisiko-KI-System wird



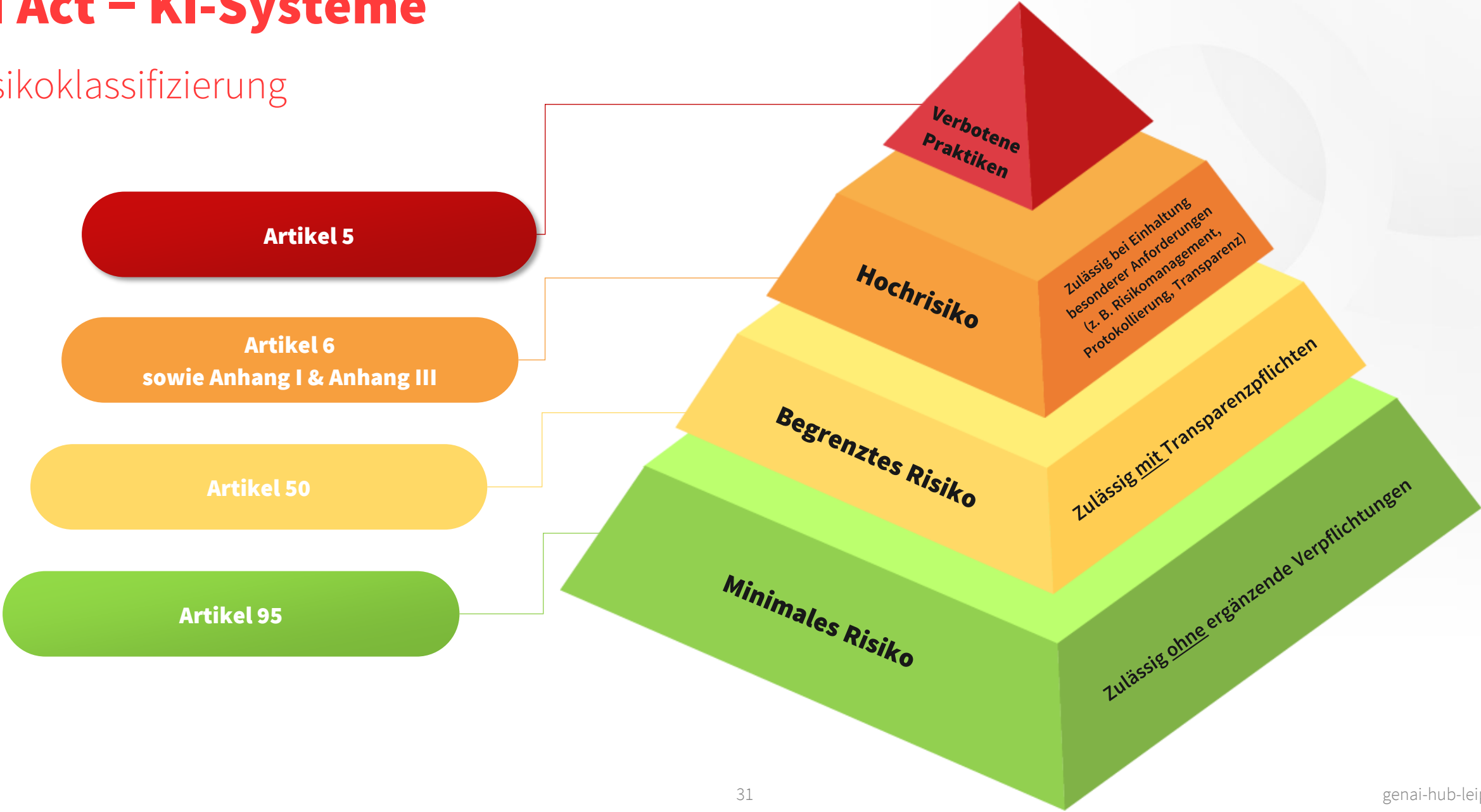
Betreiber / Deployer



Switch zum Anbieter gemäß AI Act, Art. 25 Nr. 1

AI Act – KI-Systeme

Risikoklassifizierung



AI Act – KI-Systeme

Verbotene Praktiken und Beispiele



Manipulative oder unterschwellige Beeinflussung

... um das Kundenverhalten wesentlich zu beeinflussen und dadurch erheblichen Schaden zu verursachen.

Beispiel: Ein Unternehmen setzt KI-System ein, das psychologische Profile von Kunden erstellt und gezielt Angebote so formuliert, dass Kunden unbewusst zu teureren Versicherungen tendieren.



Gezielte Ausnutzung von Schwächen oder Schutzbedürftigkeit

... bestimmter Personen, um ihr Verhalten zu beeinflussen und ihnen erheblichen Schaden zuzufügen.

Beispiel: Die KI analysiert Familienverhältnisse, Bildungsniveau und Einkommen, um sozial schwachen Kunden automatisch schlechtere Konditionen anzubieten.



Soziale Bewertung

... von Menschen auf Basis ihres sozialen Verhaltens oder ihrer persönlichen Eigenschaften und daraus ungerechtfertigte oder unverhältnismäßige Nachteile ableiten.

Beispiel: Ein Unternehmen nutzt über einen längeren Zeitraum ein KI-System zur Auswertung des Onlineverhaltens potenzieller Kunden, um Persönlichkeitsprofile zu erstellen (z. B. „unsicher“) und lässt diese auf sozialem Verhalten beruhende Bewertung für den Kunden ungünstig in die Konditionen einfließen.



AI Act – KI-Systeme

Beispiele für Hochrisiko-KI-Systeme (Art. 6 AI Act)

ANHANG I

Bestimmte **Produkte**, bei denen der Einsatz eines KI-Systems zu Einstufung als Hochrisiko-KI führt:

ANHANG III

Bestimmte **Bereiche**, bei denen der Einsatz eines KI-Systems zu Einstufung als Hochrisiko-KI führt:



AI Act – KI-Systeme

Beispiele für Hochrisiko-KI-Systeme (Art. 6 AI Act)

ANHANG I

Bestimmte **Produkte**, bei denen der Einsatz eines KI-Systems zu Einstufung als Hochrisiko-KI führt:



Medizinprodukte



Fahrzeuge



Aufzüge

...

ANHANG III

Bestimmte **Bereiche**, bei denen der Einsatz eines KI-Systems zu Einstufung als Hochrisiko-KI führt:



AI Act – KI-Systeme

Beispiele für Hochrisiko-KI-Systeme (Art. 6 AI Act)

ANHANG I

Bestimmte **Produkte**, bei denen der Einsatz eines KI-Systems zu Einstufung als Hochrisiko-KI führt:



Medizinprodukte



Fahrzeuge



Aufzüge

...

ANHANG III

Bestimmte **Bereiche**, bei denen der Einsatz eines KI-Systems zu Einstufung als Hochrisiko-KI führt:



Biometrie



Kritische Infrastruktur



Bildung



Personalmanagement

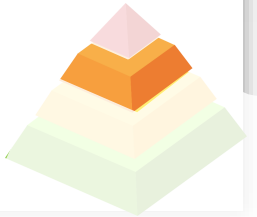


Inanspruchnahme grundlegender Leistungen



Justizbehörden

...



AI Act – KI-Systeme

Beispiele für Hochrisiko-KI-Systeme (Art. 6 AI Act)

ANHANG I

Bestimmte **Produkte**, bei denen der Einsatz eines KI-Systems zu Einstufung als Hochrisiko-KI führt:



Medizinprodukte



Fahrzeuge



Aufzüge

...

ANHANG III

Bestimmte **Bereiche**, bei denen der Einsatz eines KI-Systems zu Einstufung als Hochrisiko-KI führt:



Biometrie



Kritische Infrastruktur



Versorgung mit Wasser, Gas, Wärme oder Strom



Personalmanagement



Inanspruchnahme grundlegender Leistungen



Justizbehörden

...



AI Act – KI-Systeme

Beispiele für Hochrisiko-KI-Systeme (Art. 6 AI Act)

ANHANG I

Bestimmte **Produkte**, bei denen der Einsatz eines KI-Systems zu Einstufung als Hochrisiko-KI führt:



Medizinprodukte



Fahrzeuge



Aufzüge

...

ANHANG III

Bestimmte **Bereiche**, bei denen der Einsatz eines KI-Systems zu Einstufung als Hochrisiko-KI führt:



Biometrie



Kritische Infrastruktur



Bildung



Personalmanagement

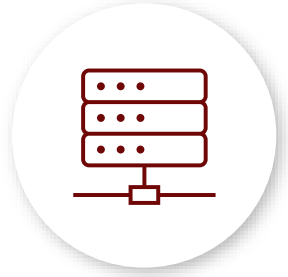


Einstellung, Karriere und Entscheidungen im Arbeitsverhältnis



AI Act – KI-Systeme

Begrenztes Risiko



Der Einsatz ist nicht verboten (Verbotene Praktiken)

Keine manipulative Täuschung oder Sozialbewertung

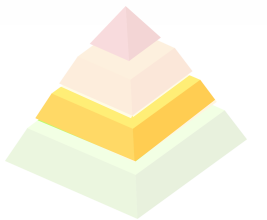
Das System ist kein Hochrisikosystem

Kein Einsatz in sicherheits- oder grundrechtskritischen Bereichen.

Das System hat Wirkung auf Menschen

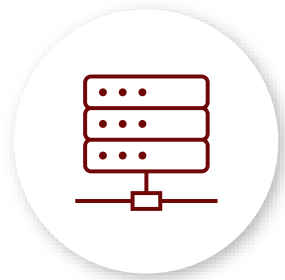
Es besteht eine Mensch-KI-Interaktion oder automatische Inhaltserzeugung, die Menschen potenziell täuschen kann, z.B.

***Beispiel:** Ein Unternehmen bietet auf seiner Website einen virtuellen Assistenten (Chatbot) an, der Fragen zu Produkten und Services beantwortet.*



AI Act – KI-Systeme

Minimales Risiko



Der Einsatz ist nicht verboten (Verbotene Praktiken)

Keine manipulative Täuschung oder Sozialbewertung

Das System ist kein Hochrisikosystem

Kein Einsatz in sicherheits- oder grundrechtskritischen Bereichen.

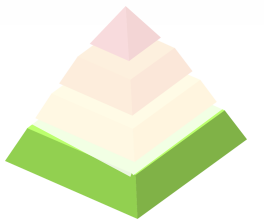
Das System fällt nicht unter Transparenzpflichten

Keine Pflicht zur Transparenz gemäß Art. 50/52 AI Act.

Das System arbeitet nur rein unterstützend oder funktional

Keine Entscheidungsrelevanz für Personen oder Rechte - rein zur technischen Unterstützung

***Beispiel:** Ein Unternehmen verwendet ein KI-gestützten Filter zur Sortierung eingehende E-Mails nach „vermutlich Spam“ oder „geschäftlich relevant“ – rein zur technischen Unterstützung des Posteingangs.*



AI Act – KI-Systeme Pflichten aus dem AI Act (Anbieter vs. Betreiber)

Risikokategorie	Pflichten der Anbieter / Provider	Pflichten der Betreiber / Deployer
 <p>verbotene Praktiken (Art. 5)</p>	<p style="text-align: center;">Verbot des Angebots</p> <p style="text-align: center;">KI-Systeme nach Art. 5 dürfen weder in den Verkehr gebracht noch verwendet werden</p>	<p style="text-align: center;">Verbot der Nutzung</p> <p style="text-align: center;">KI-Systeme nach Art. 5 dürfen nicht eingesetzt werden</p>
 <p>Hochrisiko (Art. 6, Anhang I und III)</p>	<ul style="list-style-type: none"> • Konformitätsbewertung & Zertifizierung • Risikomanagementsystem Versicherer müssen potenzielle Gefahren identifizieren, bewerten und Maßnahmen ergreifen, um diese zu minimieren. • Technische Dokumentation • Aufzeichnungspflichten („Protokollierung“) • Transparenzpflichten klare Informationen über Zweck, Funktionsweise, Risiken <ul style="list-style-type: none"> • Bereitstellung klarer Betriebsanleitungen • Angemessene menschliche Aufsicht vorsehen • Robustheit & Cybersicherheit • Qualitätsmanagement & kontinuierliche Kontrolle • Registrierung in EU-Datenbank • Meldung schwerwiegender Vorfälle an Behörden 	<ul style="list-style-type: none"> • Nutzung gemäß Anleitung & Zweckbestimmung • Implementierung und Durchführung angemessener menschlicher Aufsicht im Einsatz sicherstellen • Überwachung & Meldung schwerwiegender Vorfälle an Anbieter und Behörden • Transparenzpflicht gegenüber Nutzern Information über Nutzung, Funktionsweise und Einschränkungen
 <p>begrenztes Risiko (Art. 50)</p>	<p style="text-align: center;">Transparenzpflicht</p> <p style="text-align: center;">gegenüber Behörden und Betreibern sowie Systempflichten</p>	<p style="text-align: center;">Transparenzpflicht</p> <p style="text-align: center;">gegenüber Personen, die mit einem KI-System interagieren (z. B. Chatbot), müssen klar und verständlich auf KI-Einsatz hingewiesen werden</p>
 <p>minimales Risiko (Art. 95)</p>	<p style="text-align: center;">Keine verbindlichen rechtlichen Pflichten</p> <p style="text-align: center;">Empfehlung: Freiwillige Einhaltung ethischer Standards</p>	<p style="text-align: center;">Keine verbindlichen rechtlichen Pflichten</p> <p style="text-align: center;">Empfehlung: Freiwillige interne Vorgaben und Best Practices</p>



Rechtskonformer KI-Einsatz

Weitere relevante Rechtsgebiete und Gesetze



KI-Recht

Rahmen für Entwicklung, Einsatz und Nutzung von KI-Systemen

AI Act



Datenschutz

Verordnung zum Schutz personenbezogener Daten

DSGVO



Urheberrecht

Gesetz zum Schutz geistiger Werke und Schöpfungen

UrhG



Geschäftsgeheimnis

Gesetz zum Schutz von Geschäftsgeheimnissen

GeschGehG

Datenschutz

Datenschutzgrundverordnung (DSGVO)



Eingabe personenbezogener Daten nur mit Rechtsgrundlage

Verarbeitung personenbezogener Daten durch KI bedarf einer gültigen Rechtsgrundlage (Art.6 DSGVO)
z. B. Einwilligung, Vertrag oder berechtigtes Interesse

Verbot automatisierter Einzelfallentscheidungen (Art. 22 DSGVO)

KI-System darf z.B. eine Ablehnungsentscheidung im Bewerbungsverfahren nicht vollautomatisch ausführen, ohne dass eine menschliche Rechtsprüfung („human in the loop“) vorgenommen wird

Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

bei sensiblen KI-Anwendungen wie z.B. bei Verarbeitung besonders geschützter Daten oder hohem Potenzial für Diskriminierung oder Intransparenz

Privacy by Design (Art. 25 DSGVO)

KI-Modelle sollten so entwickelt werden, dass sie möglichst wenig personenbezogene Daten benötigen
→ Einsatz von anonymisierten Trainingsdaten statt Klardaten

Auftragsverarbeitung (Art. 28 DSGVO)

bei Nutzung externer KI (z. B. OpenAI, Anthropic) ist ein AV-Vertrag erforderlich
nur freigegebene KI-Tools nutzen
→ Abschluss eines AV mit Anbieter, TOMs und Zweckbindung

Rechtskonformer KI-Einsatz

Weitere relevante Rechtsgebiete und Gesetze



KI-Recht

Rahmen für Entwicklung,
Einsatz und Nutzung von
KI-Systemen

AI Act



Datenschutz

Verordnung zum Schutz
personenbezogener
Daten

DSGVO



Urheberrecht

Gesetz zum Schutz
geistiger Werke und
Schöpfungen

UrhG



Geschäftsgeheimnis

Gesetz zum Schutz von
Geschäftsgeheimnissen

GeschGehG

Urheberrecht

Urheberrechtsgesetz (UrhG) – mögliche Urheberrechtsverletzung durch KI-Einsatz



Urheber eines Werkes ist die **natürliche Person**, die das Werk durch ihre **persönliche geistige Leistung** geschaffen hat.

Modell

Im Rahmen des **Trainings** von KI-Modellen werden **Daten Dritter** (Texte, Lichtbilder, Musik etc.) **analysiert und gespeichert**. Die Verwendung an sich kann bereits Drittrechte verletzen.

Input / Prompt

Kopiert bspw. ein Mitarbeitender ein **Foto/Text** aus dem Internet, um dieses **als Prompt** über eine KI-Anwendung bearbeiten zu lassen, kann es sich um eine **rechtswidrige Vervielfältigung** handeln.

Output

Grundsätzlich sind **KI-generierte** Erzeugnisse **nicht urheberrechtlich geschützt**, da sie **keine menschlichen Schöpfungen** im Sinne des Urheberrechts darstellen. Problematisch können aber KI-Erzeugnisse sein, die **urheberrechtlich geschützten Werken sehr ähnlich** sind.

→ Prüfung des Outputs **vor** der Verwendung, ob ggfls. gegen Urheberrechte Dritter verstoßen wird.

Urheberrecht

Mögliche Urheberrechtsverletzung durch KI-Output

Input / Prompt

 Sie

Generiere ein Bild von einem Superhelden, der die Fähigkeiten einer Spinne hat.

Output



Urheberrecht

Mögliche Urheberrechtsverletzung durch KI-Output

Input / Prompt

Sie

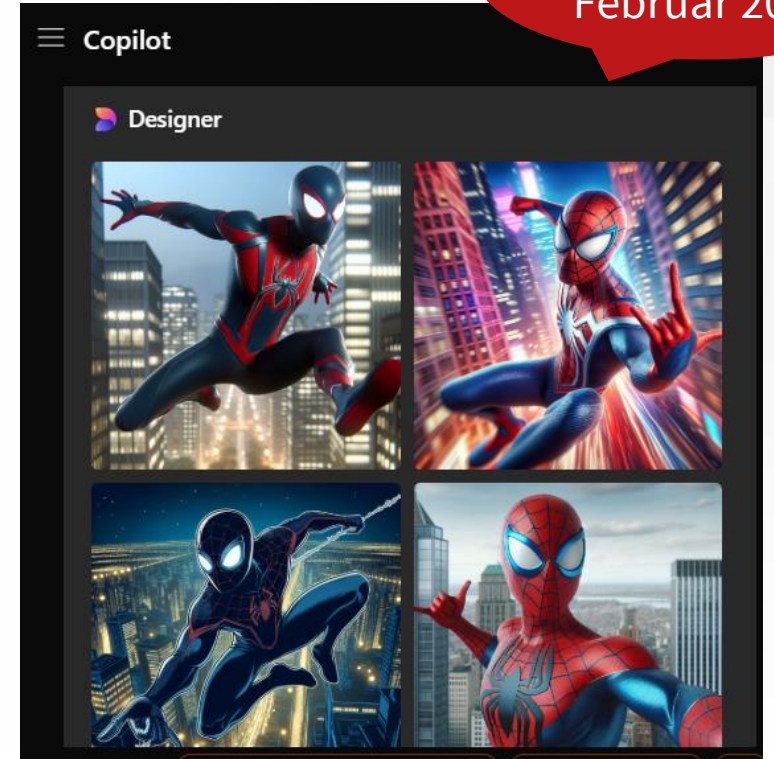
Generiere ein Bild von einem Superhelden, der die Fähigkeiten einer Spinne hat.

Output

Wie die meisten Menschen „denkt“ auch die KI **aufgrund der Daten, mit denen sie trainiert wurde**, bei einem Superhelden, der die Fähigkeiten einer Spinne hat, automatisch an **Spiderman**

→ und generiert daher Bilder von einem Superhelden, der exakt so aussieht wie dieser.

Stand:
Februar 2025



Quelle: Eigene Aufnahme; erstellt mit dem Microsoft Copilot (2025)

Wichtig: Ohne entsprechende Rechteeinräumung könnte eine Urheberrechtsverletzung vorliegen.
→ Arbeitsergebnisse prüfen, um eventuelle Verletzungen Rechte Dritter zu vermeiden

Urheberrecht – Urheberrechtsgesetz (UrhG)

Mögliche Urheberrechtsverletzung durch KI-Output

Input / Prompt

 Sie

Generiere ein Bild von einem Superhelden, der die Fähigkeiten einer Spinne hat.

Output

heute

Das Bild konnte leider nicht generiert werden, da es **gegen Richtlinien für urheberrechtlich geschützte Inhalte verstoßen könnte** – vermutlich **wegen Ähnlichkeiten zu bekannten Superhelden wie Spider-Man**.

Aber ich kann dir gerne ein alternatives Bild erstellen! Möchtest du zum Beispiel:

- Einen ****originalen Superhelden**** mit spinnenartigen Fähigkeiten (z. B. mit acht Augen, Spinnenbeinen, Netzen aus den Händen)?
- Eine ****fantasievolle Szene****, in der ein Held eine Stadt rettet mithilfe von Spinnenkräften?
- Einen ****Comicstil-Charakter****, der von Spinnen inspiriert ist, aber ein ganz eigenes Design hat?

Sag mir einfach, was dir gefällt – ich gestalte es ganz individuell!

Rechtskonformer KI-Einsatz

Weitere relevante Rechtsgebiete und Gesetze



KI-Recht

Rahmen für Entwicklung, Einsatz und Nutzung von KI-Systemen

AI Act



Datenschutz

Verordnung zum Schutz personenbezogener Daten

DSGVO



Urheberrecht

Gesetz zum Schutz geistiger Werke und Schöpfungen

UrhG



Geschäftsgeheimnis

Gesetz zum Schutz von Geschäftsgeheimnissen

GeschGehG

Geschäftsgeheimnis

Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)



Keine Eingabe in das KI-System von vertraulichen Daten:

Vertrauliche Geschäftsprozesse

nicht veröffentlichte Rezepturen, Mischungsverhältnisse, Formeln

Beispiel: „Wie genau setzt sich unser Mischungsverhältnis bei Produkt XY zusammen?“

Interne Berechnungsgrundlagen

interne Kalkulationen, Margen, Preisbildungsmodell

Beispiel: „Hier sind unsere aktuellen Kalkulationen für dieses Jahr aufgeteilt nach PLZ-Gebiet – wie kann man diese verbessern?“

Nicht veröffentlichte Kennzahlen, Strategien oder Systemplänen

interne Projektpläne oder IT-Sicherheitsmaßnahmen


Beispiel: „Bitte prüfe diesen Projektplan für die Migration unseres Kundenportals mit Zeit- und Budgetplanung.“

Rechtskonformer KI-Einsatz


Recht, Fairness & Risiken



KI-Recht




Datenschutz



Urheberrecht




Geschäftsgeheimnis




Diskriminierung



Mangelnde Fairness/ Bias



Unzuverlässigkeit/ Halluzinationen



Mangelnde Transparenz

Rechtskonformer KI-Einsatz


Recht, Fairness & Risiken



KI-Recht



Datenschutz



Urheberrecht



Geschäftsgeheimnis




Diskriminierung



**Mangelnde Fairness/
Bias**



**Unzuverlässigkeit/
Halluzinationen**



Mangelnde Transparenz

Rechtskonformer KI-Einsatz

Risiken und Beispiele



Diskriminierung

- Benachteiligung geschützter Gruppen durch automatisierte Logik
- Diskriminierung führt zu Entscheidungen, die nicht mit den geltenden Gesetzen und Vorschriften vereinbar sind.

Beispiel: Automatisierte Ablehnung von Online-Anträgen älterer Kunden durch KI-Analyse



Mangelnde Fairness / Bias

- Bias (verzerrte Daten/Modelle) kann zu mangelnder Fairness führen, d.h. das KI-System benachteiligt systematisch einzelne Personen oder Gruppen
- eine ungleiche Behandlung ist sachlich nicht gerechtfertigt

Beispiel: Ein Kredit-Scoring-System bewertet Personen aus bestimmten Wohngebieten schlechter – auch wenn ihre individuelle Bonität vergleichbar ist.

Rechtskonformer KI-Einsatz

Risiken und Beispiele



Unzuverlässigkeit und Halluzinationen

- KI gibt erfundene, falsche Ergebnisse aus.
- Unzuverlässigkeit von KI-Systemen aufgrund von unvollständigen oder fehlerhaften Daten

Beispiel: KI erstellt Zusammenfassung eines Versicherungsvertrags, die erfundene Klauseln enthält („Halluzination“)
Chatbot behauptet fälschlich, Schaden sei gedeckt, obwohl er es vertraglich nicht ist.



Mangelnde Transparenz

- Entscheidungslogik ist nicht nachvollziehbar („Black Box“)
- eingesetzte Daten und Kriterien sind unklar

Beispiel: Ein Unternehmen nutzt KI, um individuelle Preise (Dynamic Pricing) im Online-Shop anhand von Kaufverhalten, Standort, Zahlungsbereitschaft festzulegen, ohne die Kunden darüber zu informieren.

Risiken und Gefahren beim KI-Einsatz

Risiko: Schatten IT



- Nutzung von Software, Cloud-Diensten oder Hardware durch Mitarbeitende ohne die explizite Genehmigung oder Kontrolle der IT-Abteilung und des Datenschutzbeauftragten birgt Risiken



- niedrige Einstiegsschwelle, da oft kostenfrei und keine IT-Installation notwendig
- sensible (Kunden)-Daten können zu Trainingszwecken verwendet werden



- nur freigegebene Tools verwenden
- keine Namen, Kundennummern oder spezifische Projektdetails in öffentliche KIs eingeben



GENAI HUB
Leipzig

KI-Governance für einen rechtskonformen KI-Einsatz

Kirsten Müller

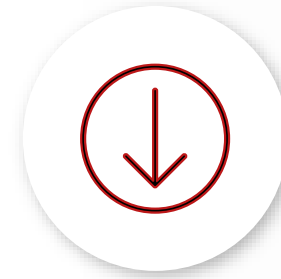
Rechtskonformer KI-Einsatz

Ziele von KI-Compliance



Rechtskonformität

KI-Recht (AI Act)
Datenschutz
Urheberrecht
Geschäftsgeheimnisse



Minimierung der Risiken

Halluzinationen
Mangelnde Fairness / Bias
Diskriminierung

Rechtskonformer KI-Einsatz

Recht, Fairness & Risiken



KI-Recht



Datenschutz



Urheberrecht



Geschäftsgeheimnis



Diskriminierung



Mangelnde Fairness/
Bias



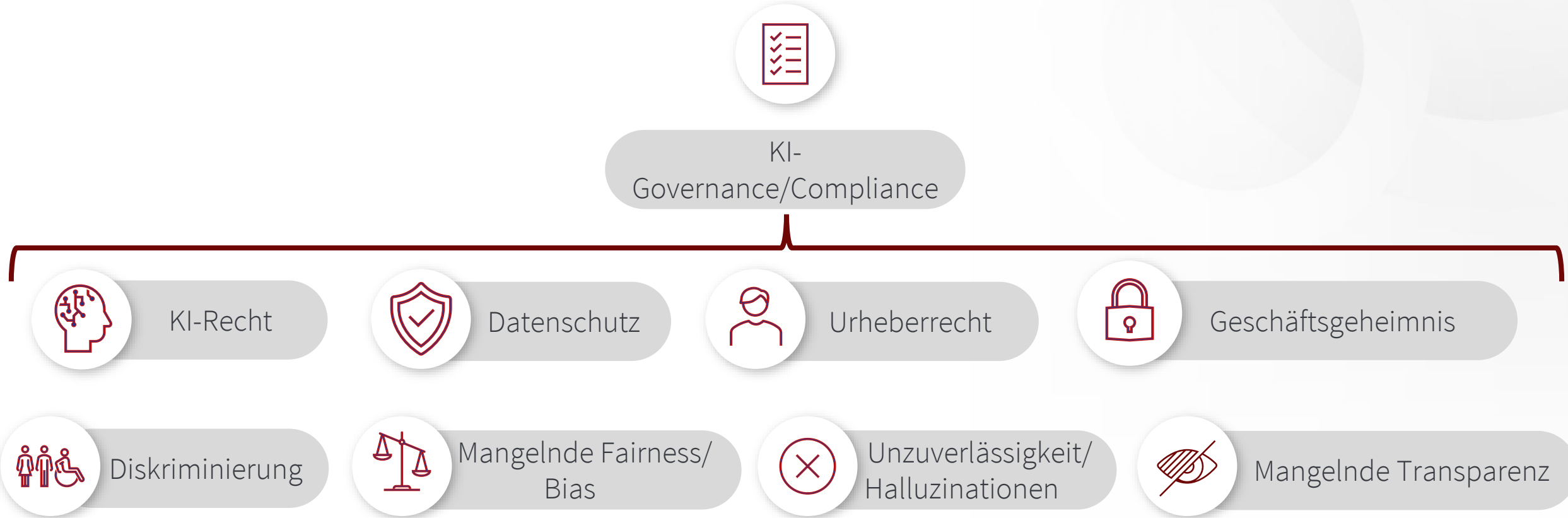
Unzuverlässigkeit/
Halluzinationen



Mangelnde Transparenz

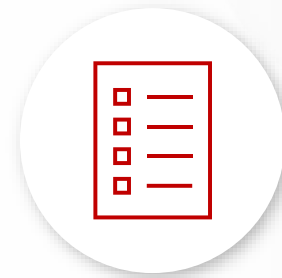
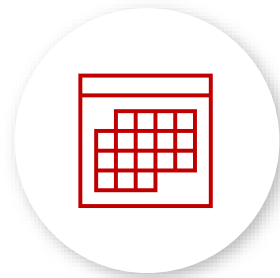
Rechtskonformer KI-Einsatz

Recht, Fairness & Risiken



Rechtskonformer KI-Einsatz

KI-Governance



KI-Richtlinie

Erstellung / Überarbeitung
einer internen Richtlinie
zum KI-Einsatz

KI-Register

Erfassung der
angewendeten KI-
Systeme in einem
Register/Roadmap

KI-Transparenz

Dokumentation der
Prozesse und Pflichten
sowie Use Cases und
Daten

KI-Kompetenz

Schulung der
Mitarbeitenden bzgl.
der KI-Nutzung

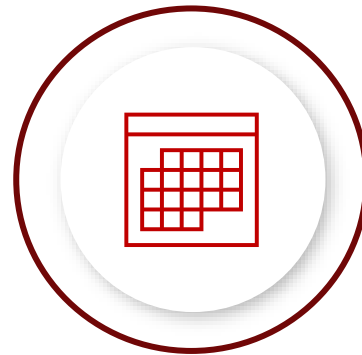
Rechtskonformer KI-Einsatz

KI-Governance



KI-Richtlinie

Erstellung / Überarbeitung
einer internen Richtlinie
zum KI-Einsatz



KI-Register

Erfassung der
angewendeten KI-
Systeme in einem
Register/Roadmap



KI-Transparenz

Dokumentation der
Prozesse und Pflichten
sowie Use Cases und
Daten

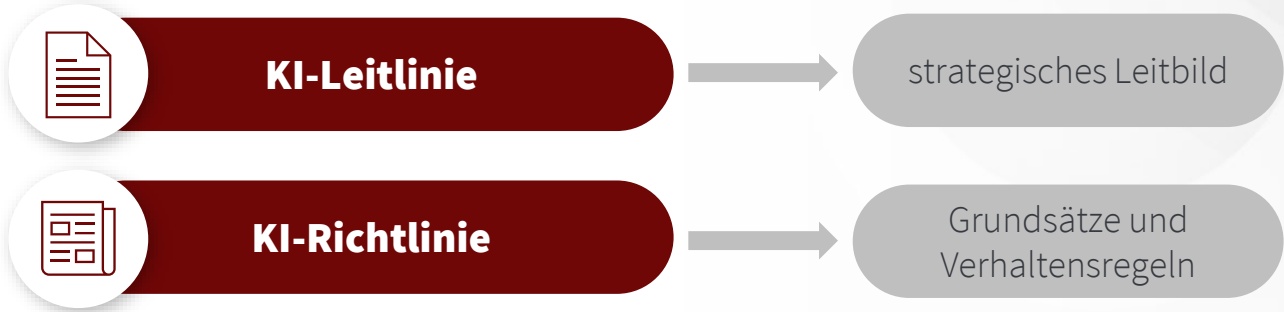


KI-Kompetenz

Schulung der
Mitarbeitenden bzgl.
der KI-Nutzung

KI-Governance/Compliance

KI-Dokumenten-Landschaft



KI-Systeme & Use Cases

KI-Register

Checkliste für Prüfung neuer Use Cases

Risikoeinstufung

Meldeprozess für KI-Vorfälle

KI-Team

Dokument
Rollenbilder

KI-Sicherheit

TOMs

Datenschutzrichtlinie

Compliance-Richtlinie

IT-Sicherheitsrichtlinie

KI-Kompetenz

Allgemeine KI-Schulung

CoPilot Schulung

IT-Sicherheitsschulung

DOS and DON'TS



Bedeutung der KI-Richtlinie

Die KI-Richtlinie unterstützt die KI-Strategie und schafft einen unternehmensweiten Rahmen.



KI-Richtlinie

Bedeutung

- Richtet sich an alle Mitarbeitenden
- Verantwortungsvolle Nutzung von KI sicherstellen
- Rechtssicherheit und Compliance gewährleisten
- Vertrauen und Akzeptanz fördern
- Kompetenzentwicklung und Orientierung bieten
- Innovation und Nutzungspotenziale fördern
- Unterbindung von KI-Aktionismus: klare Richtlinien helfen, unkoordinierte und nicht erlaubte Nutzung zu verhindern
- Guten Rahmen, der Sicherheit bei der Nutzung gibt

KI-Richtlinie

Interne Vorgaben im Kontext KI-Einsatz

Unternehmensweite KI-Strategie

Strategische Vorgaben für den Einsatz von KI im gesamten Unternehmen, die sicherstellen, dass alle KI-Anwendungen mit den Unternehmenszielen und -werten im Einklang stehen.

Allgemeine Richtlinie für Mitarbeitende

Grundsätze und Verhaltensregeln, die den verantwortungsvollen Umgang mit KI-Systemen im Arbeitsalltag definieren.

Entwicklungsrichtlinien

Vorgaben für die Entwicklung, das Training und die Implementierung von KI-Modellen, um Qualität, Fairness und Compliance sicherzustellen.



Abteilungs- bzw. Use-Case bezogene Richtlinien

Individuelle Richtlinien, die den Einsatz von KI im Hinblick auf die spezifischen Anforderungen und Prozesse in den jeweiligen Abteilungen oder Use Cases regeln.

Notfall- und Incident-Response Richtlinien für KI-Systeme

Protokolle und Prozesse für den Umgang mit Störungen, Fehlfunktionen oder Missbrauch von KI-Systemen, um schnell und effektiv auf Probleme reagieren zu können.

KI-Richtlinie

Interne Vorgaben im Kontext KI-Einsatz

Unternehmensweite KI-Strategie

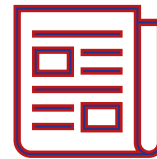
Strategische Vorgaben für den Einsatz von KI im gesamten Unternehmen, die sicherstellen, dass alle KI-Anwendungen mit den Unternehmenszielen und -werten im Einklang stehen.

Allgemeine KI-Richtlinie für die Mitarbeitenden

Grundsätze und Verhaltensregeln, die den verantwortungsvollen Umgang mit KI-Systemen im Arbeitsalltag definieren.

Entwicklungsrichtlinien

Vorgaben für die Entwicklung, das Training und die Implementierung von KI-Modellen, um Qualität, Fairness und Compliance sicherzustellen.



Abteilungs- bzw. Use-Case bezogene Richtlinien

Individuelle Richtlinien, die den Einsatz von KI im Hinblick auf die spezifischen Anforderungen und Prozesse in den jeweiligen Abteilungen oder Use Cases regeln.

Notfall- und Incident-Response Richtlinien für KI-Systeme

Protokolle und Prozesse für den Umgang mit Störungen, Fehlfunktionen oder Missbrauch von KI-Systemen, um schnell und effektiv auf Probleme reagieren zu können.

Bedeutung der KI-Kompetenz

Grundlage für rechtssichere und wirksame
KI-Nutzung

Rechtskonformer KI-Einsatz

KI-Governance – KI-Kompetenz



Pflicht

gemäß AI Act, Art. 4

- **Ausreichendes Maß** an KI-Kompetenz **bei Personal** und anderen Personen, die mit dem **Betrieb und der Nutzung von KI-Systemen** befasst sind.
- Unter Berücksichtigung
 - technischer **Kenntnisse, Erfahrung, Ausbildung, Schulung**
 - und**
 - des **Kontexts**, in dem die KI-Systeme eingesetzt werden sollen

Rechtskonformer KI-Einsatz

KI-Governance – KI-Kompetenz



Definition

gemäß AI Act, Art. 3 Nr. 56

„KI-Kompetenz“: **Fähigkeiten, Kenntnisse** und **Verständnis**, die es Anbietern, Anwendern und Betroffenen ermöglichen, KI-Systeme unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung **in Kenntnis der Sachlage einzusetzen** und sich über die **Chancen** und **Risiken** von KI und **mögliche Schäden**, die sie verursachen kann, bewusst zu werden.“

Rechtskonformer KI-Einsatz

KI-Governance – Kompetenzentwicklung im Unternehmen



Grundlegende
Schulung für alle
Mitarbeitende



Identifikation und
Weiterbildung für das
KI-Team/Promotoren



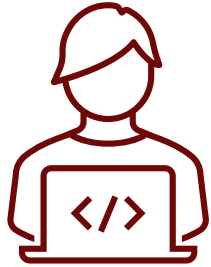
Weiterbildung für
Führungskräfte

Kontinuierliche Weiterbildung

- GenAI-Tools und Prompt Engineering
- Chancen, Risiken und Herausforderungen beim Einsatz von GenAI
- Identifikation von potentiellen Use Cases im Alltag der Mitarbeitenden
- Etablieren von bereichsübergreifenden Austauschformaten zum Thema KI / GenAI
- etc.

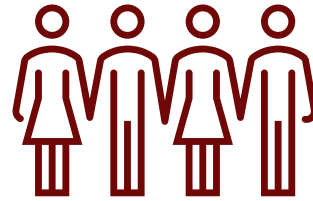
Maßnahmen zur Vermeidung von Risiken

Die Rolle des Menschen – unverzichtbar!



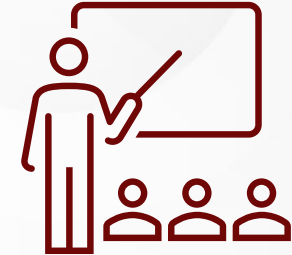
Menschliche Aufsicht

Menschliche Überwachung und Kontrolle sind unerlässlich für faire KI-Entscheidungen



Interdisziplinäre Teams

Experten aus Technologie, Ethik und Recht müssen zusammenarbeiten, um KI-Systeme verantwortungsvoll zu gestalten



Weiterbildung

Massive Investitionen in die Schulung und Weiterbildung der Mitarbeiter sind für den erfolgreichen KI-Einsatz notwendig



GENAI HUB
Leipzig

Workshop KI-Richtlinie

Kirsten Müller & Sophia Seifert

Ablauf der Workshop-Arbeit

1. Einführung

- Aufgabe und Ziel des Workshops

2. Workshop-Arbeit

- Gliederung einer KI-Richtlinie
- Inhalte der KI-Richtlinie
- Rollen und Verantwortlichkeiten

3. Zusammenfassung & Fazit



Bedeutung der KI-Richtlinie

KI-Richtlinie unterstützt die KI-Strategie und schafft einen unternehmensweiten Rahmen.

KI-Richtlinie

Bedeutung

- Richtet sich an alle Mitarbeitenden, die mit KI arbeiten
- Guter Rahmen, der Sicherheit bei der Nutzung von KI gibt
- Verantwortungsvolle Nutzung von KI sicherstellen
- Rechtssicherheit und Compliance gewährleisten
- Vertrauen und Akzeptanz fördern
- Kompetenzentwicklung und Orientierung bieten
- Innovation und Nutzungspotenziale fördern
- Unterbindung von KI-Aktionismus: klare Richtlinien helfen, unkoordinierte und nicht erlaubte Nutzung zu verhindern

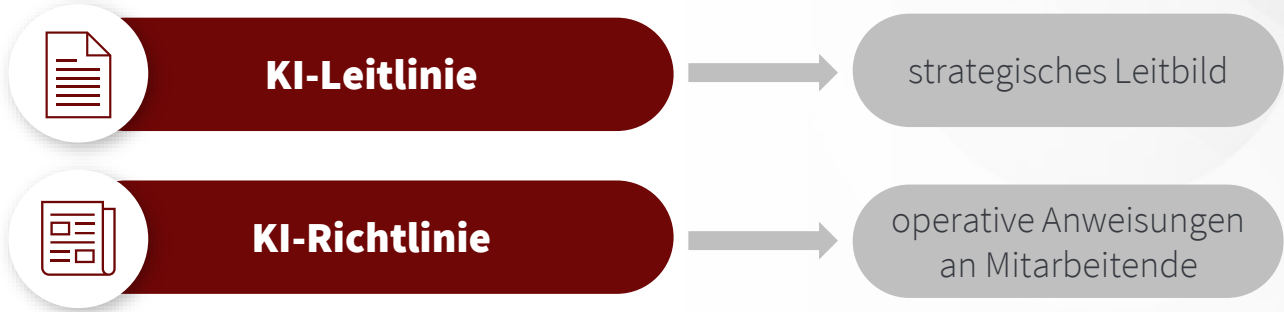
Unser Ziel

- Grundsätze und Verhaltensregeln für den KI-Einsatz im Unternehmen festlegen
- Wichtige Definitionen bestimmen
- Klare Verantwortlichkeiten festlegen
- Arbeitsanweisungen für die Mitarbeitenden erarbeiten
- Schaffung von Ownership für die erarbeitete KI-Richtlinie



KI-Governance/Compliance

KI-Dokumenten-Landschaft



KI-Systeme & Use Cases

KI-Register

Checkliste für Prüfung neuer Use Cases

Risikoeinstufung

Meldeprozess für KI-Vorfälle

KI-Team

Dokument
Rollenbilder

KI-Sicherheit

TOMs

Datenschutzrichtlinie

Compliance-Richtlinie

IT-Sicherheitsrichtlinie

KI-Kompetenz

Allgemeine KI-Schulung

CoPilot Schulung

IT-Sicherheitsschulung

DOS and DON'TS



KI-Richtlinie

Gliederung – Beispiele (I)

Beispiel 1:

- I. Geltungsbereich
- II. Sachlicher Anwendungsbereich /Adressatenkreis
- III. Zweck der Richtlinie
- IV. Definitionen: KI-System, Risikoklassen
- V. Grundsätze für die Nutzung
 1. Bereiche
 2. Freigegebene Tools
- VI. Unzulässige Nutzungen
- VII. Compliance-Management
 1. Zuständigkeiten
 2. Verantwortlichkeiten
- VIII. Sanktionen

Beispiel 2:

- I. Präambel
- II. Anwendungsbereich
- III. Definitionen: KI-System, Einstufung Hochrisiko; Anbieter/Betreiber
- IV. Grundsätze für die Nutzung
- V. Unzulässige Nutzungen
- VI. Spezifische Regelungsbereiche
- VII. Compliance-Management
 1. Zuständigkeiten
 2. Verantwortlichkeiten
- VIII. Ansprechpartner

KI-Richtlinie

Gliederung – Beispiele (II)

Beispiel 3:

I. Einleitung: Sinn und Zweck

II. Geltungsbereich/Anwendungsbereich

III. Adressatenkreis

IV. Definitionen:

- was erachtet Unternehmen als KI
- Daten
- (Tools, Anwendungsfälle)

V. Zugelassene Tools -> Verweis auf Toolvorgaben

- Link zum Tool; Korrelation aus Tool und Zweck

VI. Grundsätze Nutzung KI:

- ethisch, Datenschutz, Transparenz

VII. Stets unzulässige Nutzungen

VIII. Compliance Management

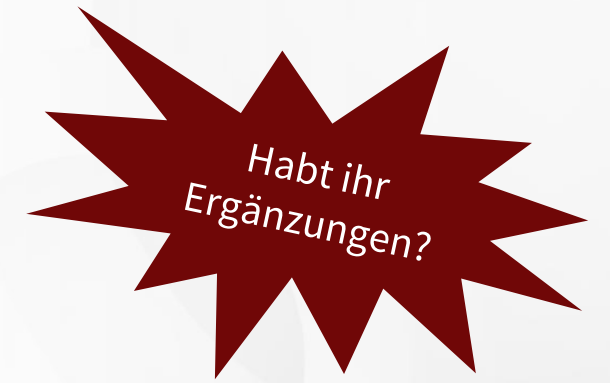
IX. Hinweise zur Vermeidung von Rechtsverletzungen

X. Hinweise von Verstößen

KI-Richtlinie

Gliederung – Vorschlag für Inhalt

- I. Ziel und Zweck
- II. Geltungsbereich
- III. Begriffsdefinitionen
- IV. Grundprinzipien
- V. Rollen und Verantwortlichkeiten
- VI. Genehmigungs- und Prüfprozesse
- VII. Risikoabschätzung und Monitoring
- VIII. Kommunikation und Awareness
- IX. Überprüfung und Weiterentwicklung



Zielbild und Entwicklung KI-Richtlinie

AUFGABE

1. Schreibt auf, was soll/muss in die KI-Richtlinie (Anforderungen/Inhalte).
 - jeder für sich
 - stichpunktartig, nicht ausformulieren
 - pro Inhalt ein Post-It

5 MIN

Inhalt unserer KI-Richtlinie

AUFGABE

1. Stellt eure Punkte vor und ordnet eure Anforderungen/Inhalte den Gliederungspunkten zu. Wo muss was stehen?
2. Ergänzt gegebenenfalls die Gliederung um weitere notwendige Punkte.

15 MIN

5 MIN



Inhaltliche Vervollständigung der KI-Richtlinie

AUFGABE

1. Teilt euch anhand eurer Skills und der Gliederungspunkte auf
2. Formuliert den Inhalt eurer Gliederungspunkte der KI-Richtlinie.

5 MIN

40 MIN



Unsere Muster-KI-Richtlinie

Gliederung

- I. Ziel und Zweck
 - II. Geltungsbereich
 - 1. sachlicher Anwendungsbereich
 - 2. personeller Anwendungsbereich
 - 3. räumlicher Anwendungsbereich
 - III. Begriffsdefinitionen (Variante: als Anhang)
 - IV. Rollen und Verantwortlichkeiten
 - V. Grundprinzipien
 - VI. Risikoabschätzung und Monitoring
 - VII. Kommunikation und Awareness
 - VIII. Genehmigungs- und Prüfprozesse
 - IX. Überprüfung und Weiterentwicklung
- ANHANG:
- Begriffe und Definitionen
 - Use Cases

Inhaltliche Vervollständigung der KI-Richtlinie

AUFGABE

1. Stellt die Inhalte eurer Gliederungspunkte vor und gebt gegenseitig Feedback.

Notiert Verbesserungswünsche zum Nachtragen

20 MIN

Zusammenfassung erster Tag

Was haben wir heute gemeinsam erreicht

- Sensibilisierung aller Teilnehmenden für die Chancen und Risiken von KI im Unternehmenskontext
- Förderung eines interdisziplinären Dialogs
- Gemeinsames Verständnis von Anforderungen an KI-Governance
- Aufbau einer Richtlinie + Grundstruktur
- Inhalte der Richtlinie
- Mitgestaltung und Reflexion

**Weitere Informationen und Kontaktmöglichkeit
unter: genai-hub-leipzig.de**





GEN**AI** HUB
Leipzig

Ausklang bei einem Feierabendgetränk!?