Webinar AI Act kompakt

Was Unternehmen jetzt wissen müssen

28.02.2024 | Ressort KI | Lab Responsibility

Katharina Jäger

Leiterin Innovation & Technology

- **Ressort KI**
- Ressort Metaverse

jaeger@bvdw.org

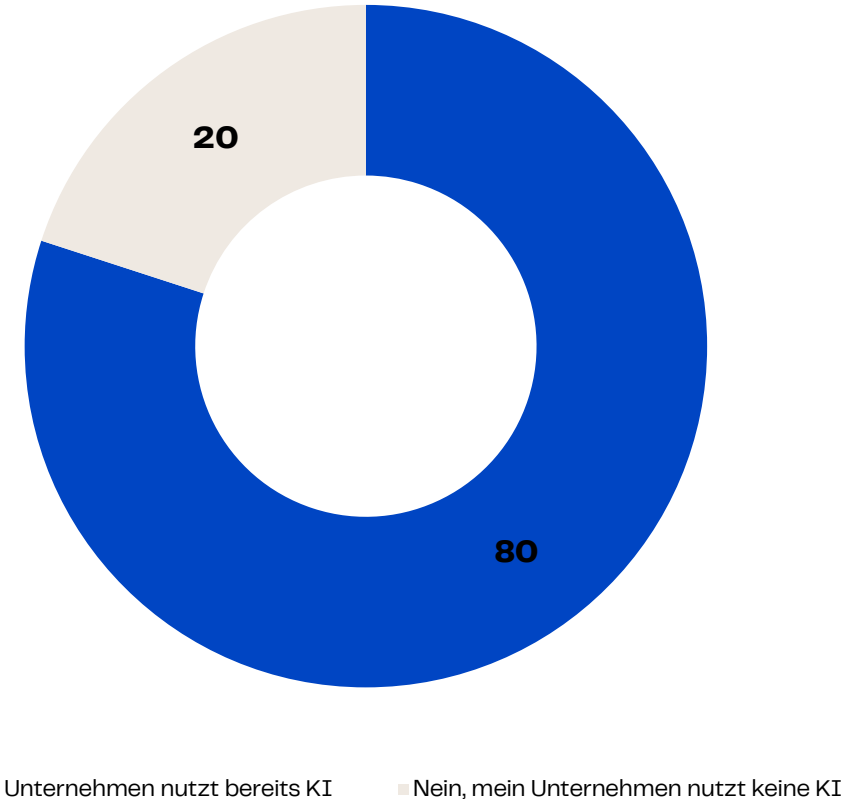
Tel.: +49 30 2062186 16
Mobil: +49 173 8999 073

Ihr habt Interesse am Ressort KI teilzunehmen?

Wir treffen uns alle 4 Wochen, Freitags von 10 – 11 Uhr!

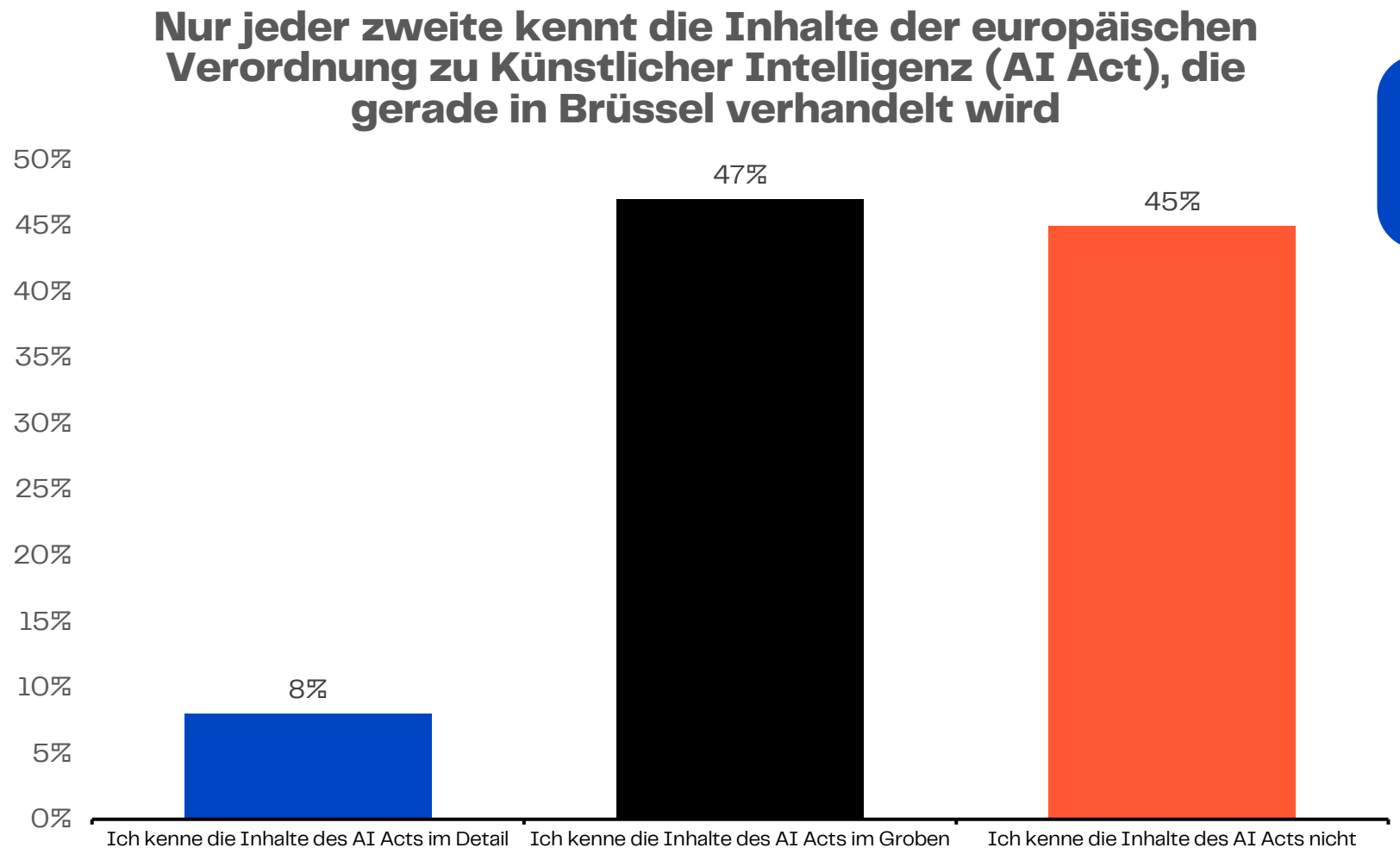
Einleitung

80% aller teilgenommenen Unternehmen nutzen bereits KI



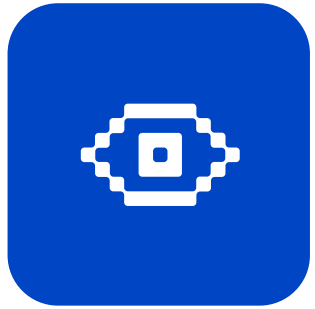
Quelle: https://www.bvdw.org/news-und-publikationen/ki-befragungen/

Einleitung



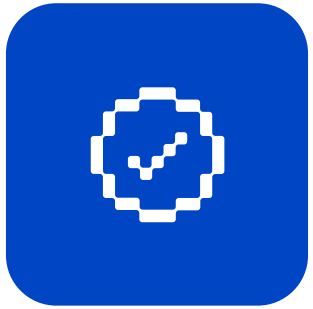
Quelle: https://www.bvdw.org/news-und-publikationen/ki-befragungen/

Ziele des Webinars



Überblick über den AI Act

... die zentrale gesetzliche Regelung im Bereich der Künstlichen Intelligenz in Europa.



Grundlegendes Verständnis

... für diesen wichtigen Rechtsakt.

Bedeutung der Regulatorik

... für eure unterschiedlichen Unternehmen.

AI Act kompakt: Was Unternehmen jetzt wissen müssen 2 – Q & A Session mit Svenja Hahn

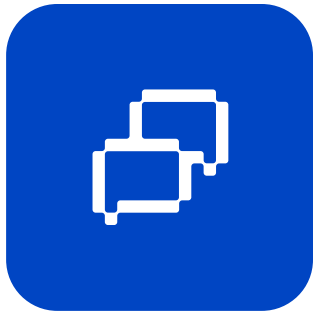
Svenja Hahn MdEP

Abgeordnete im Europäischen Parlament für die FDP und Schattenberichterstatterin für die Renew-Fraktion zum AI Act im federführenden Binnenmarktausschuss (IMCO)

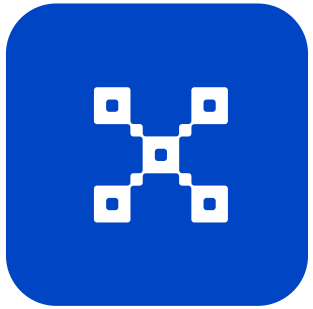
Hier geht's zur Anmeldung

06.03.2024
13:15 – 14:00 Uhr
Online
Exklusiv für BVDW-Mitglieder

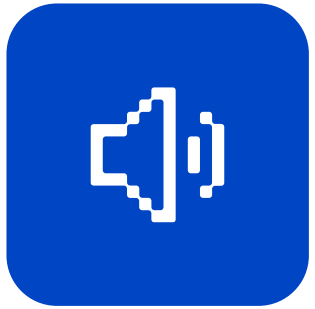
How To



- Stelle Eure Fragen gerne jederzeit im Chat!
- Wir werden diese in den letzten 10 Minuten beantworten!
- Der Chat steht euch auch im Nachhinein zur Verfügung!



- Folien senden wir per Mail an euch!



- Bitte muted euch, um die Referenten nicht zu unterbrechen!

Disclaimer

Disclaimer zum Grundlagen-Webinar zum AI Act

Die Inhalte dieses Webinars dienen nur zu Bildungs- und Aufklärungszwecken und reflektieren den Stand der Dinge zum Zeitpunkt 28. Februar 2024. Da der Bereich der Künstlichen Intelligenz und die zugehörige Gesetzgebung, insbesondere der AI Act, sich rasch entwickeln, könnten sich einige Informationen zeitnah anpassen. Dieses Webinar stellt keine Rechtsberatung dar und ersetzt diese auch nicht. Die Vortragenden übernehmen keine Haftung für die Richtigkeit oder Aktualität der bereitgestellten Informationen, wenngleich wir im Besten Wissen und Gewissen die Informationen zusammengestellt haben. Die Nutzung der Webinar Inhalte erfolgt auf eigenes Risiko.

Webinar AI Act – Speaker

Fabiane Buchheister
Abteilung Innovation
EWE AG

Fritz-Ulli Pieper, LL.M.
Rechtsanwalt Fachanwalt für Informationstechnologierecht
Taylor Wessing

Eva Werle
Inhaberin und Geschäftsführerin
Basilicom GmbH

Dr. Marian Klingebiel
Rechtsanwalt
Senior Legal Counsel
ePrivacy GmbH

Tobias Kellner
Industry Relations Manager,
Germany Google

Agenda

1. Einleitung & Einordnung
2. Der AI Act – Das Gesetzgebungsverfahren
   - Was ist die EU-Verordnung?
   - Timeline im Gesetzgebungsprozess
3. Grundlagen
   - Regelungsbereich
   - Betroffene
   - Anwendungsbereich
4. Definitionen
5. Die Risikostufen
   - Verbotene KI
   - Hochrisiko-KI
   - Risikoarme KI
6. KI-Systeme
   - Foundation Models
   - Gen AI
7. Governance
8. Wie sich BVDW-Mitglieder vorbereiten können
9. Diskussion & Fragen

Der AI Act – Das Gesetzgebungsverfahren

Fritz-Ulli Pieper, Taylor Wessing

Basics: Was ist der AI Act?

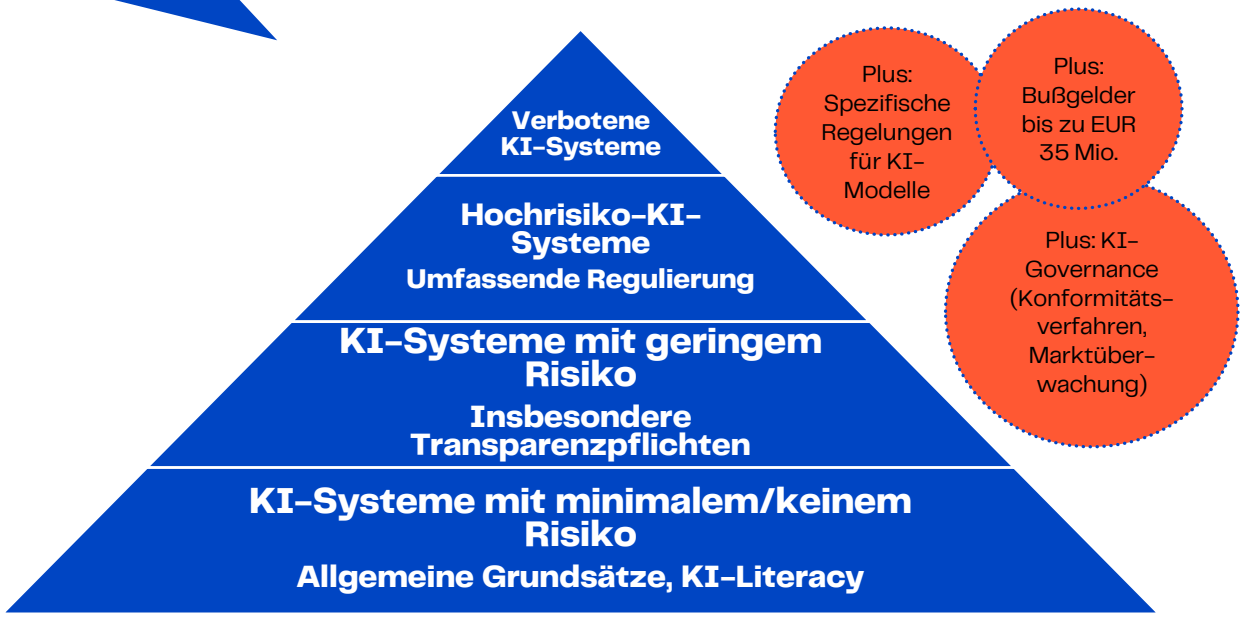
EU-Verordnung

- Als EU-Verordnung ist der AI Act ein verbindlicher Rechtsakt, der unmittelbar anwendbar ist (kein Umsetzungsakt national nötig).

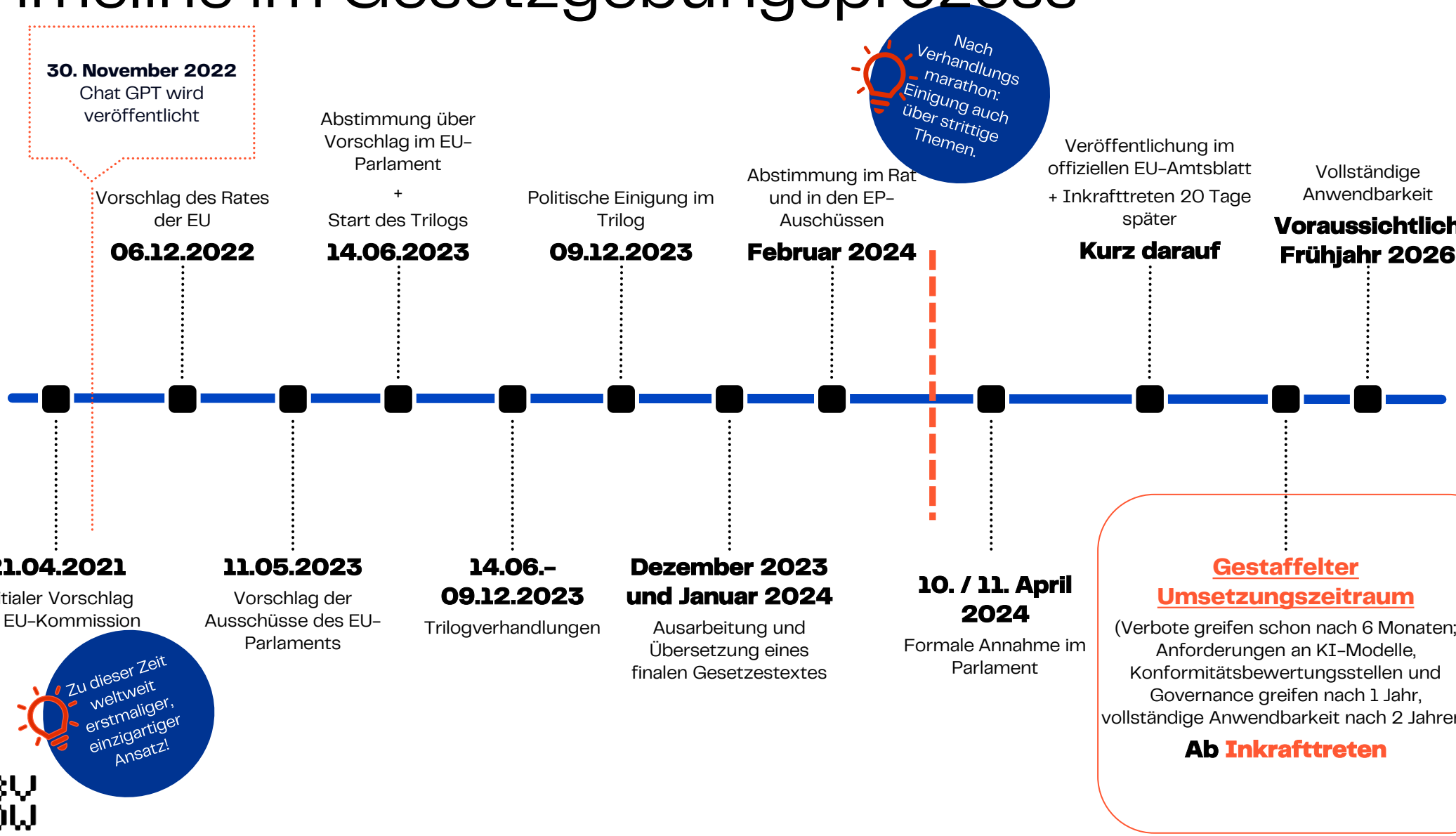
Ziele

- Schutz von Grundrechten und Werten der EU.
- Innovationsförderung durch Rechtssicherheit.
- Governance stärken.
- Erschaffen eines harmonisierten europäischen Marktes.

Risikobasierter Ansatz



Timeline im Gesetzgebungsprozess



Grundlagen

Eva Werle, Basilicom
& Marian Klingebiel, ePrivacy

Der Regelungsbereich

Der AI Act gilt für AI-Systeme ...

mit allen Ebenen der Autonomie ...

die in bestimmten Bereichen innerhalb der EU eingesetzt werden ...

oder das Verhalten von Personen in der EU wesentlich beeinflussen ...

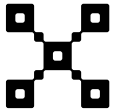
... unabhängig von der Rechtsform der Organisation oder ihres Sitzes.

Betroffene

Kern der Regelung: Der AI Act stellt Anforderungen...

...an Entwickler.

...Anbieter von KI-Systemen.



...Anwender von KI-Systemen.

Das Ziel:

- Risiken minimieren.
- Grundlegende Rechte und die Sicherheit der Bürger schützen.

Betroffene

Anbieter (provider)

- Inverkehrbringen oder Inbetriebnehmen in EU
- (Niederlassung egal)

Bereitsteller/Betreiber (deployer)

- EU Niederlassung / ansässig

Anbieter/Betreiber (providers & deployers)

Niederlassung / ansässig außerhalb der EU

Output used in EU

- Importeure und Händler von KI-Systemen (Konformitätskennzeichnung CE, Unterlagen...)
- Produkthersteller: Inverkehrbringen oder Inbetriebnehmen zusammen mit ihrem Produkt unter eigenem Namen oder Marke
- Bevollmächtigte von Nicht EU-Anbietern
- Betroffene EU-Personen

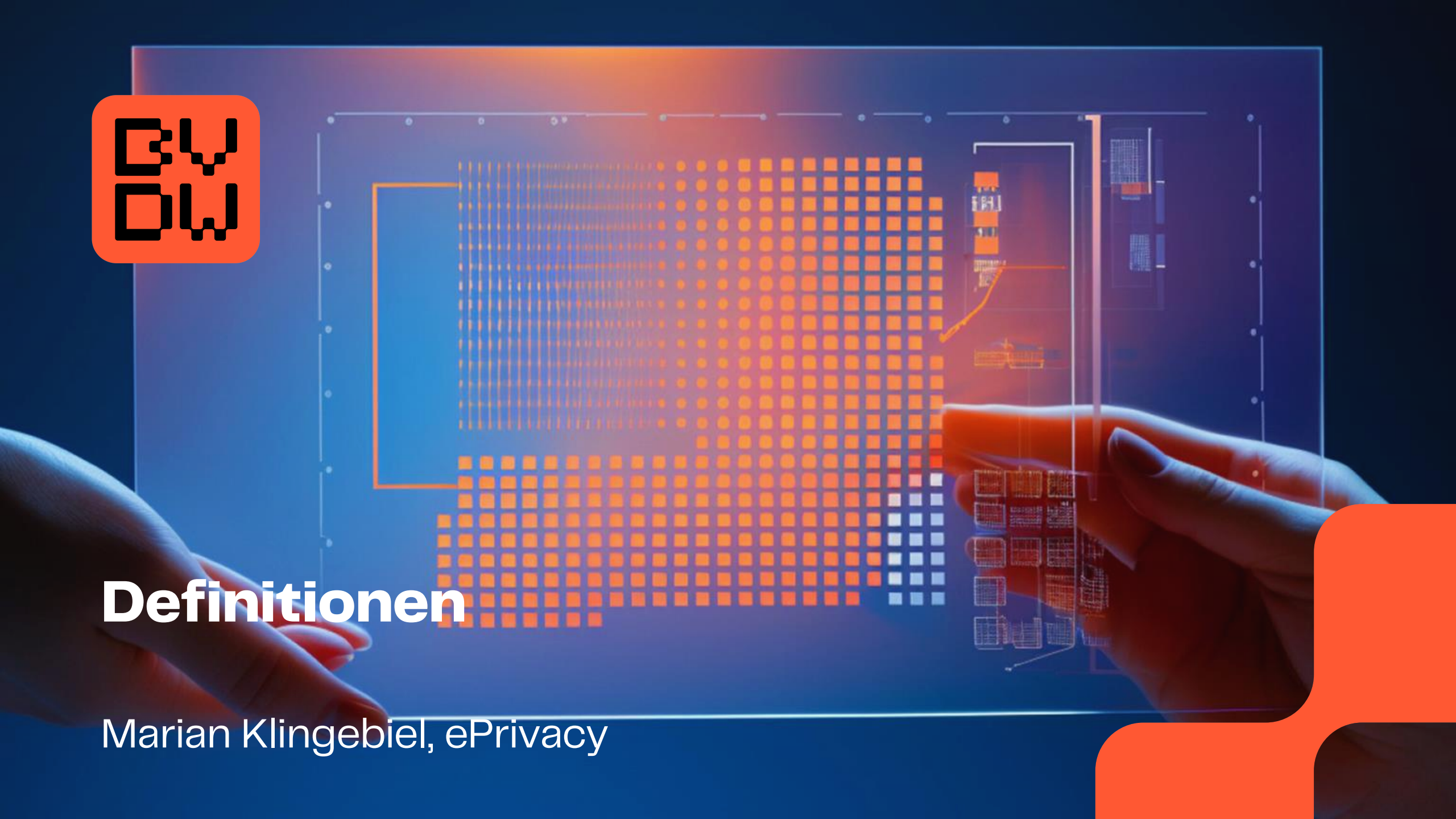
Regelungs- / Anwendungsbereich

Regelungen neben AI Act:

- **Datenschutz** (z.B. sensible Daten für Training) – DSGVO
- **Urheberrecht** – UrhG
- Zugang zu Daten – Data Act
- Komponenten in MedTech Geräten – MDR
- KFZ mit autonomer Fahrfunktion (Level 4) – AFGBV
- ...

Nicht erfasst:

- **KI-Systeme des Militärs und der nationalen Sicherheit**
- KI-Systeme zur internationalen Strafverfolgung / justiziellen Zusammenarbeit
- Forschung, Erprobung und Entwicklung bevor die KI auf den Markt gebracht oder in Betrieb genommen wird (keine Tests unter realen Bedingungen)
- Natürliche Personen, die KI-Systeme rein privat/unprofessionell nutzen
- Open-Source-KI-Systeme, sofern nicht verboten oder mit hohem Risiko behaftet



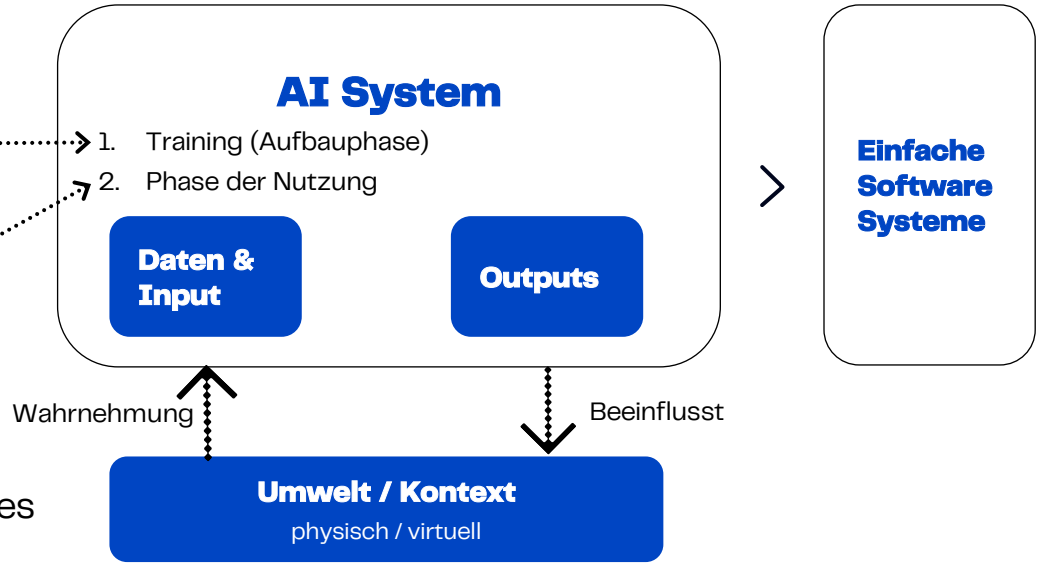
Definitionen

Marian Klingebiel, ePrivacy

Definitionen

KI-Systeme

- A **machine-based** system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that,
- for **explicit or implicit objectives, infers,** from the **input** it receives, how to **generate outputs** such as predictions, content, recommendations, or decisions
- **that can influence physical or virtual environments**



GPAI

GPAI Model: Model weißt **erhebliche Allgemeinheit** auf / kann breites Spektrum unterschiedlicher Aufgaben ausführen und kann **in eine Vielzahl von nachgelagerten Systemen** integriert werden

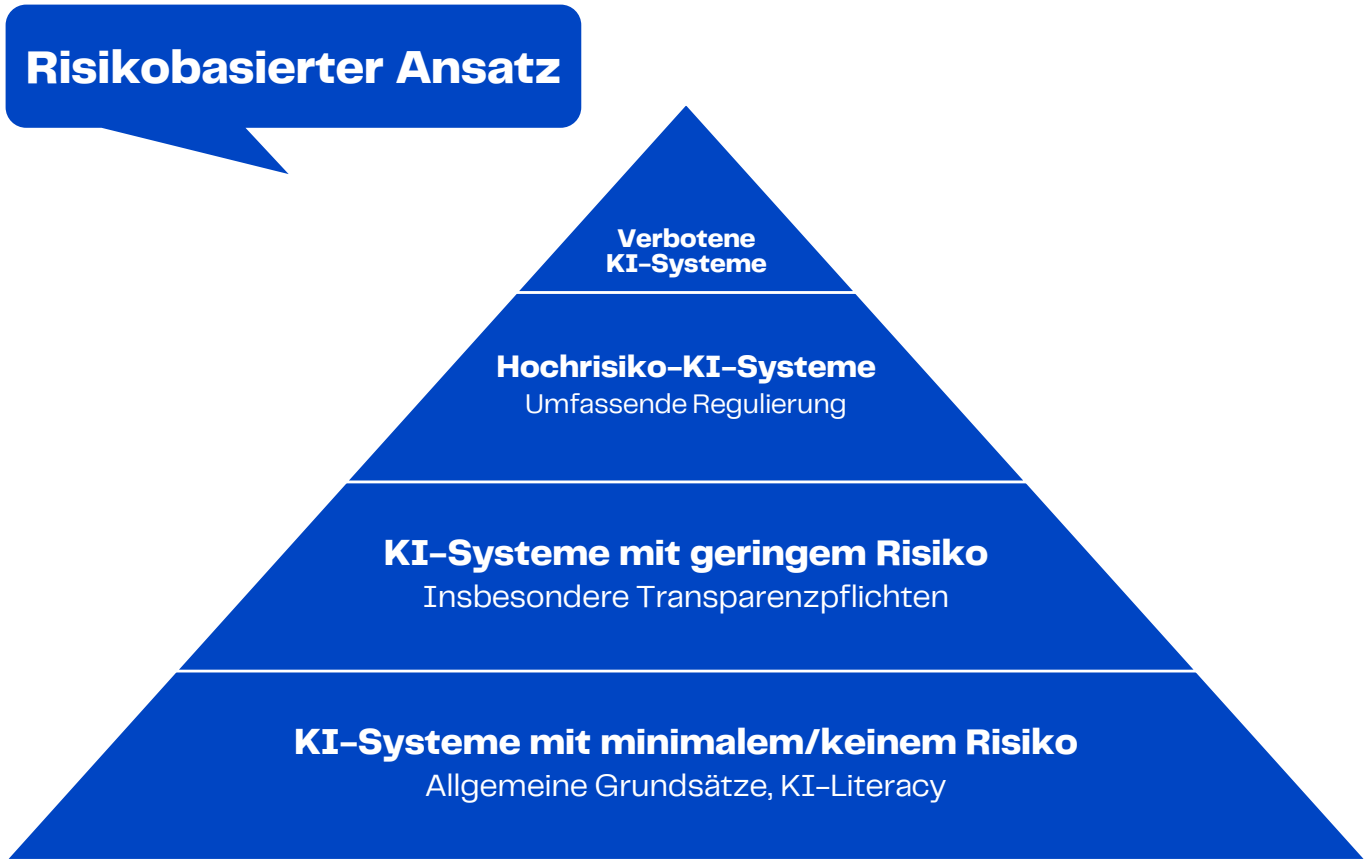
GPAI System basiert darauf und kann **Vielzahl von Zwecken** erfüllen (Direktnutzung oder Integration)

Technische Unterlagen, Gebrauchsanweisungen, Urheberrechtsrichtlinie einhalten
Zusammenfassung Trainingsinhalte
Wenn Systemrisiko (10^25 FLOPS): Modell-Evaluierungen, Gegentests, schwerwiegende Vorfälle verfolgen und melden, Cybersicherheit gewährleisten.

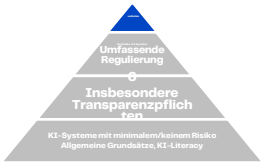
Die Risikostufen

Fabiane Buchheister, EWE AG

Risikobasierter Ansatz



Risikostufe: unannehmbares Risiko / verbotene KI



Verbotene KI-Systeme

KI-Systeme, die durch **Manipulation** die Entscheidungsfindung beeintrachtigen und dadurch erheblichen Schaden zufügen

KI-Systeme zur **Emotionserkennung** bei Strafverfolgung, Grenzkontrollen, am Arbeitsplatz & in Bildungseinrichtungen

KI-Systeme, die unter **Ausnutzung von Schwächen** das Verhalten von Personen beeinflussen und dadurch erheblichen Schaden zufügen

Ungezieltes Auslesen von Gesichtsbildern aus Internet & Videoüberwachung zur Erstellung von Datenbanken zur **Gesichtserkennung**

Biometrische Kategorisierungssysteme, die sensible Merkmale wie Geschlecht, ethische Zugehörigkeit oder Religion verwenden

Präventive Strafverfolgung auf Basis von “Profiling”

Social Scoring, das zur Benachteiligung in sozialen Kontexten führt

Biometrische Echtzeit-Fernidentifikationssysteme in öffentlich zugänglichen Räumen

Risikostufe: Hochrisiko-KI / KI Governance aufbauen

KI-Systeme, die in Produkten verwendet werden, die unter die EU-Produktsicherheits-gesetzgebung fallen (z.B. Medizinprodukte, Kraftfahrzeuge, Spielzeug, Luftfahrt, Aufzüge)

Wann handelt es sich um ein Hochrisiko-KI-System?

KI-Systeme, die in folgenden Bereichen zum Einsatz kommen & ein erhebliches Risiko für Gesundheit, Sicherheit und Grundrechte darstellen

- Klassifizierung und Identifizierung von Personen auf Basis biometrischer Merkmale
- Verwaltung & Betrieb kritischer Infrastruktur
- Bildung & berufliche Aus- und Weiterbildung
- Beschäftigung, Mitarbeiterverwaltung & Zugang zu Selbständigkeit
- Zugang zu & Nutzung von wesentlichen privaten & öffentlichen (Dienst-) Leistungen
- Strafverfolgung
- Migrations- & Asylangelegenheiten und Grenzkontrolle
- Rechtspflege & demokratische Prozesse

Ausnahme: wenn kein erhebliches Risiko für Gesundheit, Sicherheit & Grundrechte

Risikostufe: Hochrisiko-KI/ Pflichtenkatalog

Die Rolle bestimmt die Pflichten & Anforderungen an Hochrisiko-KI-Systeme

Grds. Anforderungen

Pflichten von Anbietern

Pflichten von Nutzern, Händlern, Importeuren, Verteilern oder. sonst. Dritten

v.a. Einhaltung grds. Anforderungen

- Hochrisiko-KI-System wird unter eigenem Namen / Marke vertrieben
- Hochrisiko-System wird wesentlich verändert
- Verwendungszweck wird geändert, so dass es erst zu einem Hochrisiko-KI-System wird

Risikostufe: Hochrisiko-KI Pflichtenkatalog

Anbieterpflichten

- Einhaltung grds. Anforderungen
- Konformitätsbewertung & CE-Kennzeichnung
- Korrekturmaßnahmen & Informationspflichten
- "post-market monitoring"-System
- Zusammenarbeit mit Behörden

- Qualitäts- & Risikomanagement
- Daten-Governance-Struktur & Qualitätsanforderungen an Daten
- Technsiche Dokumentation & Aufzeichnungspflichten
- Transparenz & Informationspflichten gegenüber Nutzern
- Menschliche Aufsicht
- Genauigkeit, Robustheit & Cybersicherheit

Nutzerpflichten

- Befolgen der Gebrauchsanweisung
- Sicherstellung menschlicher Aufsicht
- Sicherstellung der Relevanz der Eingabedaten für die bestimmungsgemäßen Verwendungszwecke
- Überwachungs- & Informationspflichten
- Aufbewahren von "logging"-Daten
- Folgenabschützung bzgl. Grund- & Menschenrechte

Risikostufe: geringes Risiko

Wenn nicht verboten und nicht Hochrisiko-KI, aber direkte Interaktion mit natürlichen Personen

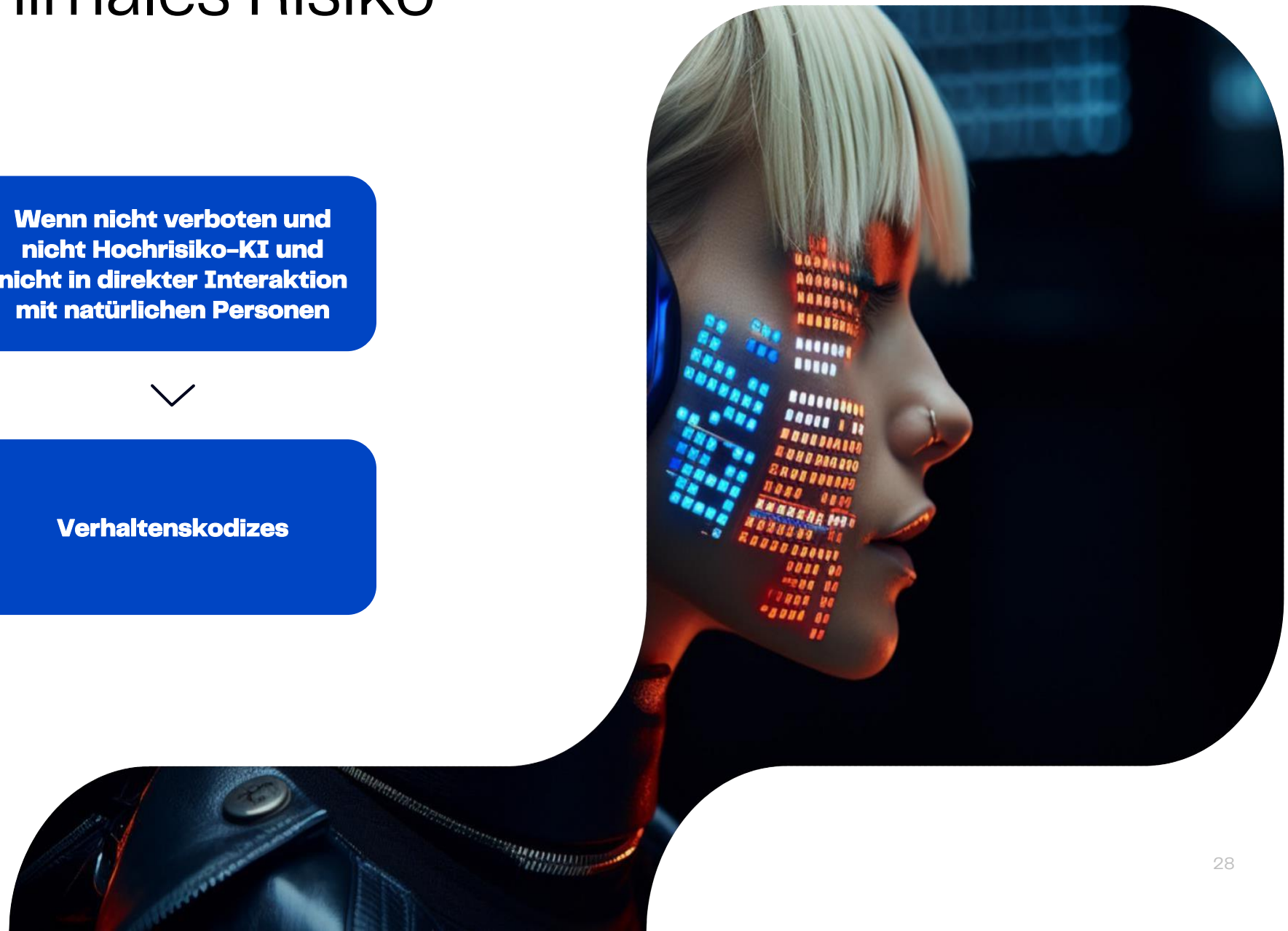
> **Transparenz- & Kennzeichnungs-pflichten** + **Technische Dokumentation** + **Verhaltenskodizes**

- Offenlegung, dass Inhalte KI-generiert sind
- Keine Generierung illegaler Inhalte
- Auskunft darüber, welche (urheberrechtl. geschützten) Trainingsdaten verwendet wurden

Risikostufe: minimales Risiko

Wenn nicht verboten und nicht Hochrisiko-KI und nicht in direkter Interaktion mit natürlichen Personen

Verhaltenskodizes



KI-Systeme

Tobias Kellner, Google

Foundation model / General Purpose AI (GPAI)

Was sind sie und was ist ihr besonderes Merkmal?

→ Grundlegende (foundational) = große Systeme, die in der Lage sind, ein breites Spektrum unterschiedlicher Aufgaben erfolgreich auszuführen, wie z. B. **Video-, Text- und Bilderzeugung, Konversation in einer Fremdsprache, Datenverarbeitung oder Erzeugung von Computercode.** Oft werden sie auch als Allzweck-KI-Modelle (GPAI) bezeichnet.

Mehrere Studien kommen zum Ergebnis, dass generative KI mehrere hundert Milliarden zur deutschen Wertschöpfung beitragen kann.
Mögliche Risiken, denen die Regulierung vorbeugen möchte:

(1) fortgeschrittene Desinformation,

(2) Ausbeutung von Minderheiten und gefährdeten Gruppen,

(3) historische und andere Verzerrungen in den Daten, die zum Trainieren von generativen KI-Modellen verwendet werden, die Stereotype reproduzieren.

https://der-digitale-faktor.de/

Die Unterscheidung zwischen grundlegenden und generativen KI-Modellen

Der Hauptunterschied zwischen grundlegenden und generativen KI-Modellen liegt in ihrer Spezialisierung und Anwendungsbreite. Grundlegende (Foundation)-KI-Modelle sind für allgemeine Zwecke konzipiert und bieten eine Grundlage für verschiedene KI-Anwendungen. Im Gegensatz dazu sind generative KI-Modelle auf bestimmte Aufgaben zugeschnitten, beispielsweise auf die Generierung realistischer Bilder oder die Übersetzung von Sprachen.

Beispiele Grundlegende Modelle:

Natural Language Processing, Computer Vision
GPT-3, LaMDA, BERT

Beispiele Generative KI Modelle:

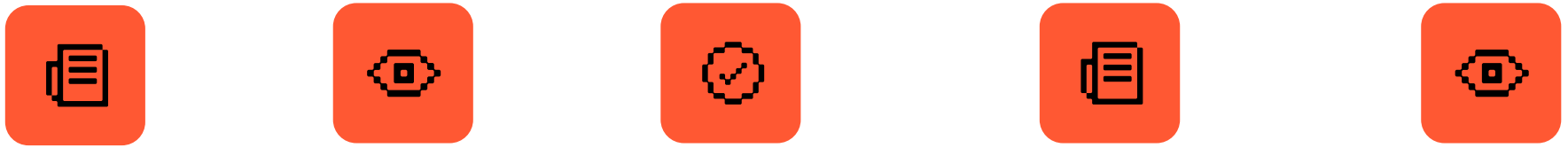
Kreative Content Erstellung, Code Generierung
Gemini, Chat-GPT, Chat, Midjourney (Generative Bilder), aber auch Google Translate

Feature	Foundation AI Models	Generative AI Models
Specialization	General-purpose	Task-specific
Versatility	High	Medium
Adaptability	High	Medium
Range of tasks	Wide	Narrow
Accuracy for specific tasks	Medium	High

Verpflichtungen für Basismodelle / General Purpose AI (GPAI)

Es gibt eine Reihe von strengen Verpflichtungen, um den Gefahren zu begegnen

Generative KI-Systeme fallen unter die Kategorie der "KI-Systeme mit hohem Risiko" im EU-KI-Gesetz und unterliegen daher besonderen Verpflichtungen.. Alle Anbieter von GPAI-Modellen müssen diese erfüllen (mit Ausnahme von GPAI-Modellen, Forschung und Entwicklung, oder Kleinunternehmen und Kleinstunternehmen – nur bestimmte Verpflichtungen):



Risiko-management | **Transparenz** | **Fairness** | **Datensicherheit** | **Menschliche Aufsicht**

- Zusätzliche Anforderungen:
- Registrierung: Generative KI-Systeme müssen bei der Europäischen KI-Agentur registriert werden
- Konformitätsbewertung: Entwickler und Betreiber von generativen KI-Systemen müssen die Konformität ihrer Systeme mit dem EU-KI-Gesetz nachweisen
    - Offene Fragen sind etwa wie sich andere Vorschriften wie der DSA und seine Transparenzanforderungen mit dem AI Act vereinbaren lassen.

Governance

Fabiane Buchheister, EWE AG
& Marian Klingebiel, ePrivacy

Wie wird der AI Act nun durchgesetzt?

Governance

Überwachung

Beratung

European AI Office

"Eur. AI Board"

Advisory Forum

Scientific Panel

National Authorities

Umsetzung AI Act

Marktüberwachung

Wie sich BVDW-Mitglieder vorbereiten können

Tobias Kellner, Google

Mögliche Anwendungsfelder von generativer KI

Vieles wird möglich

Generative KI

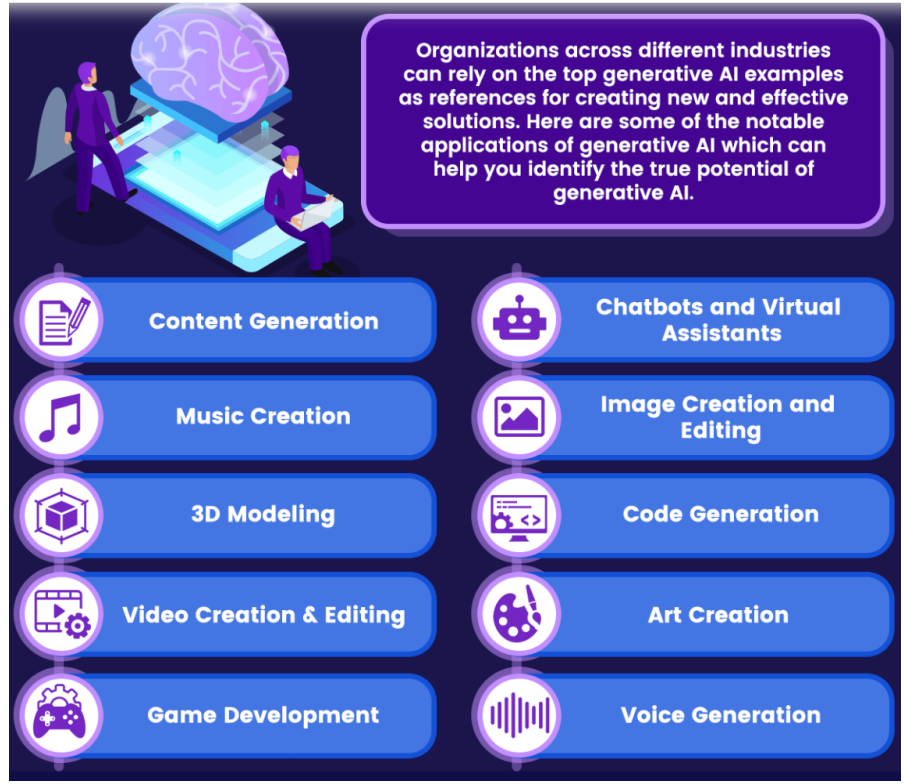
Generative KI-Modelle zeichnen sich, wie der Name schon sagt, durch die Generierung neuer Inhalte aus, egal ob es sich um Text, Bilder, Code oder andere Formen von Daten handelt.

Beispiele aus DE:

- **Siemens:**
  Entwicklung von KI-gestützten Lösungen für die Industrie: Siemens MindSphere nutzt generative KI, um Daten aus Produktionsanlagen zu analysieren und Optimierungspotenziale zu erkennen.

- **SAP:**
  Erstellung von personalisierten Lernerfahrungen: SAP Learning nutzt generative KI, um personalisierte Lernerfahrungen für Mitarbeiter zu erstellen.

- **Allianz:**
  Entwicklung von KI-gestützten Lösungen für die Versicherungsbranche, z. B. zur Betrugserkennung und Risikobewertung.



Wie sich BVDW-Mitglieder vorbereiten können

Eure Aufstellung zum Erfolg im KI-Paradigma

Informiere Dich über den AI Act

#diesesWebinar

Evaluiere Deine KI-Systeme

Implementiere ein Risikomanagement-Framework

#ethischeRichtlinien

Schaffe eine Kultur der Transparenz und Fairness

Investiere in Schulungen und Weiterbildungen

#BVDW

Arbeite mit anderen Unternehmen und Organisationen zusammen

Nutze die Unterstützung der Europäischen Kommission

Diskussionsrunde

Eure Fragen, Eure Key Take Aways

Eva Werle, Basilicom

BVDW Convention & Convention Night
Wir gestalten Zukunft!

Gemeinsame Gremiensitzung

Wir verbinden Daten, Kreativität und Verantwortung in einer technologischen sich stetig weiterentwickelnden Welt.

20. März 2024
10 – 16 Uhr
Wartehalle am Nordbahnhof, Berlin

Netzwerk und Austausch im Fokus

Die BVDW Convention ist mehr als nur eine Konferenz – sie ist ein Ort des Austauschs, des gemeinsamen Lernens und der Inspiration.

Hier geht's zur Eventwebseite & den ersten Inhalten

Von Mitgliedern für Mitglieder

Die Agenda der Convention bietet eine Mischung aus Fachvorträgen, Diskussionsrunden und interaktiven Workshops, die von Mitgliedern für Mitglieder organisiert und geleitet werden.

Hier geht's zur kostenfreien Anmeldung

AI Act kompakt: Was Unternehmen jetzt wissen müssen 2 – Q & A Session mit Svenja Hahn

Svenja Hahn

Abgeordnete im Europäischen Parlament für die FDP und Schattenberichterstatterin für die Renew-Fraktion zum AI Act im federführenden Binnenmarktausschuss (IMCO)

Hier geht's zur Anmeldung

06.03.2024
13:15 – 14:00 Uhr
Online
Exklusiv für BVDW-Mitglieder


BYBW
THANK YOU