KI-Workshop

Do you trust AI?

4.5.2023

Mag. Alexandra Ciarnau

DORDA

WIR SCHAFFEN KLARHEIT.

Vortragende

Alexandra Ciarnau

Anwältin

IT/IP/Data Protection
Digital Industries

+43-1-533 4795-23
alexandra.ciarnau@dorda.at

- Co-Leiterin der DORDA Digital Industries Group
- IT/IP & Data Protection
- New Tech (AI, Blockchain, XR…)
- Konsumentenschutzrecht
- Nachhaltigkeitsrecht
- Women in AI Austria (Vorstand)
- Blockchain-Arbeitskreis der WKO
- Autorin zahlreicher Artikel und Vortragende auf Universitäten (zB Uni Salzburg, Stuttgart) und bei Seminaren
- Co-Autorin von Praxishandbüchern

"Alexandra Ciarnau was impressive. Extremely good service providers."
(Chambers Europe, 2021)

Top 250 Women in IP
Managing IP, 2022

Trade Mark Star (Trade Mark)
IP STARS, 2022

Recommended (Data - Data Privacy & Protection, Intellectual Property, Information Technology)
The Legal 500, 2023

Rising Star (Privacy and Data Protection)
Euromoney's LMG Rising Stars Expert Guide, 2022

Client Choice „Data – Information Technology"
Lexology Client Choice Award, 2022

Agenda

- **KI-Basics**
- **Anwendungsmöglichkeiten**
- **Datenschutzrechtliche Aspekte**
- **IP-rechtliche Aspekte**
- **Haftung**

KI-Basics und Anwendungsbeispiele im beruflichen Alltag

KI-Basics

Künstliche Intelligenz ist…

- …die Fähigkeit einer Maschine, menschliche Fähigkeiten zu imitieren.

Der AI Act definiert KI anhand der genutzten Techniken und Konzepte:

- … Systeme, die Deep Learning nutzen;
- … Logik- und wissensgeschützte Konzepte;
- … statistische Ansätze, bayessche Schätz-, Such- und Optimierungsmethoden.

KI-Basics

schwach

KI ist auf einem Gebiet richtig gut.

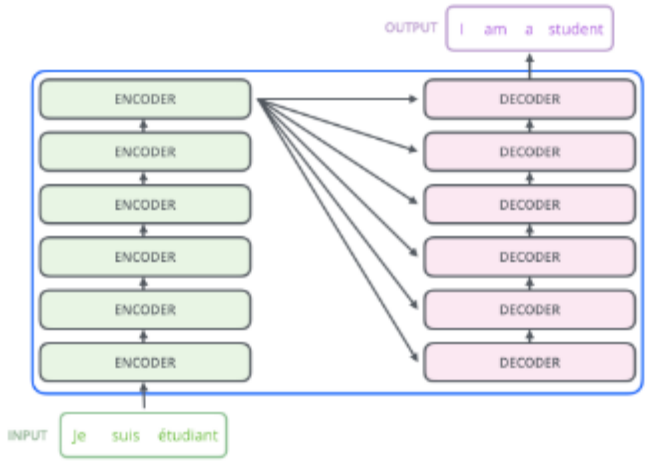
stark

KI erreicht die menschliche Intelligenz.

Anwendungsmöglichkeiten im beruflichen Alltag

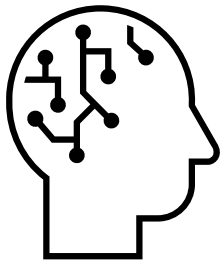
GPT-Modelle

- GPT-Modelle oder auch Transformer sind Sprachverarbeitungsmodelle, die u.a. eine Reihe von Zeichen und können verschiedene Funktionen erfüllen, wie zB:
  - Texte generieren
  - Texte zusammenfasen
  - Texte übersetzen



Einfache Darstellung eines Transformers.
Quelle: https://jalammar.github.io/images/t/The_transformer_encoder_decoder_stack.png

ChatGPT



- "*Chatbot Generative Pre-trained Transformer*"
- Seit Ende November 2022 bekannt
  - Kostenlose und kostenpflichtige Version
  - GPT 3.5 – mittlerweile GPT 4.0

- **What is ChatGPT?**:

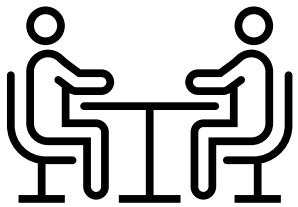
  "*Hello! I am ChatGPT, a large language model developed by OpenAI based on the GPT (Generative Pre-trained Transformer) architecture. I have been trained on a massive amount of text data and can perform a variety of natural language processing tasks, such as answering questions, generating text, and translating languages. My goal is to be a helpful and informative conversational agent.*"

  - Generative KI
  - Chatbot basierend auf Sprache und Text

ChatGPT - kontroverses Thema der Gegenwart

"*ChatGPT schafft große Teile der Matura*"[2]

"*ChatGPT passes exams from law and business schools*"[1]



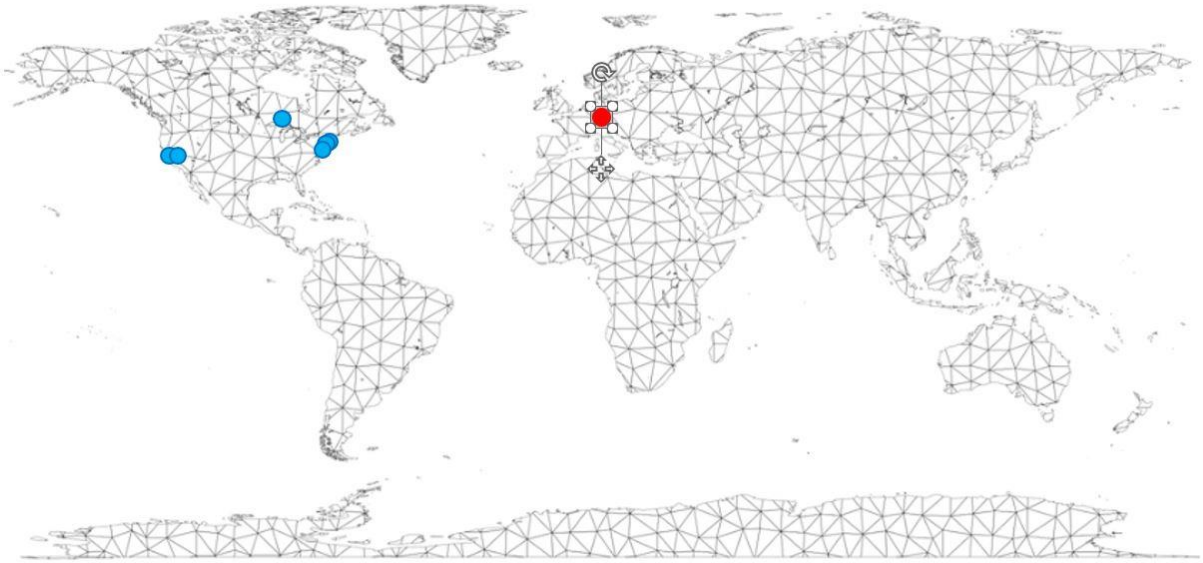
"*ChatGPT wird in Italien aus Datenschutzgründen gesperrt*"[3]

"*Australier will ChatGPT wegen Verleumdung klagen*"[4]

1: (<https://edition.cnn.com/2023/01/26/tech/chatgpt-passes-exams/index.html> (12.4.2023))
2: (<https://www.derstandard.at/story/2000144543271/chatgpt-schafft-grosse-teile-der-matura> (12.4.2023))
3: (<https://www.derstandard.at/story/2000145103559/chatgpt-wird-in-italien-aus-datenschutzgruenden-gesperrt> (12.4.2023))
4: (<https://www.diepresse.com/6272839/australier-will-chatgpt-wegen-verleumdung-klagen> (13.4.2023))

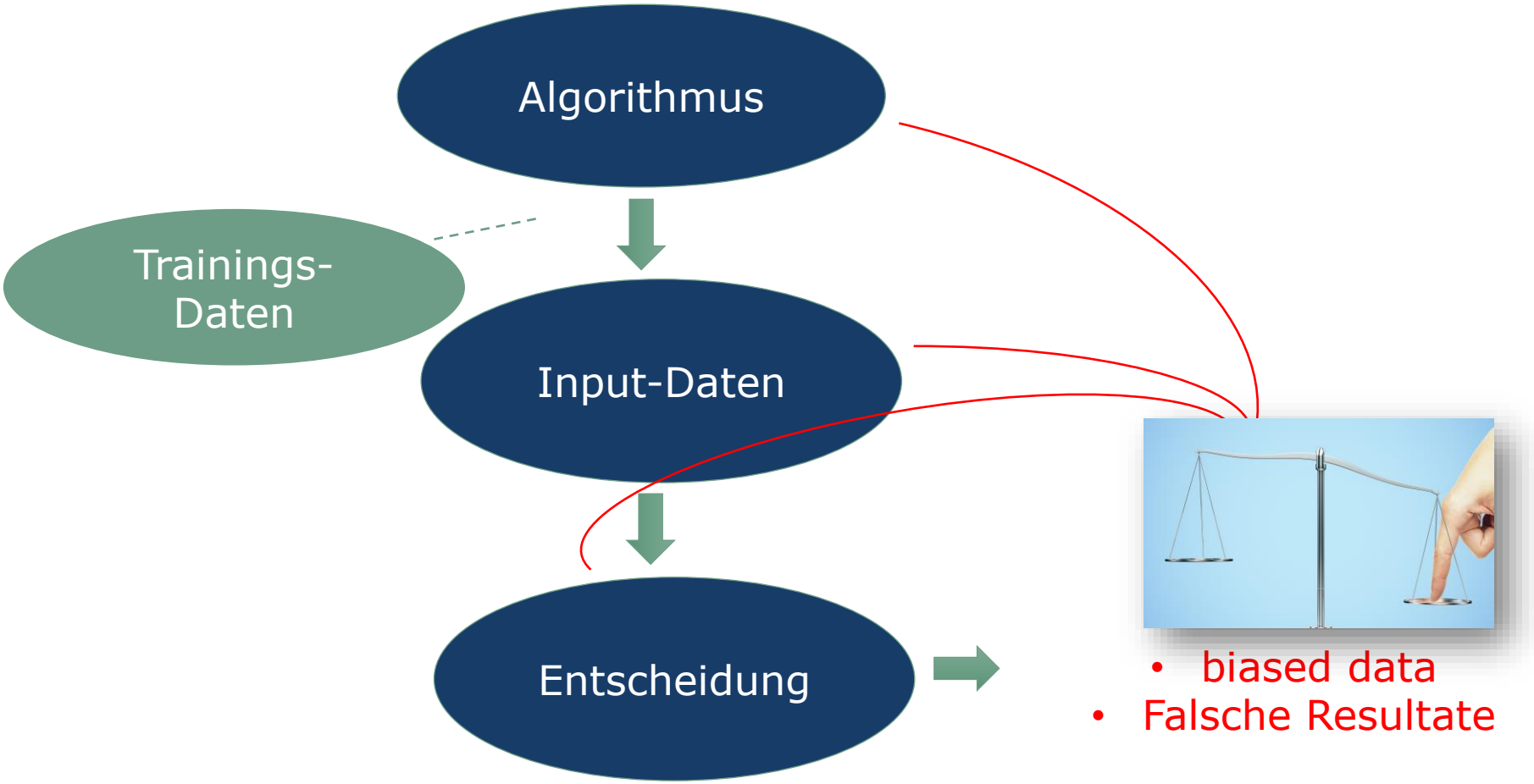
Im Rennen um die großen KI-Sprachmodelle

- Forefront
- Anthropic
- Open Playground
- Hugging Face
- co:here
- OpenAI
- Aleph Alpha



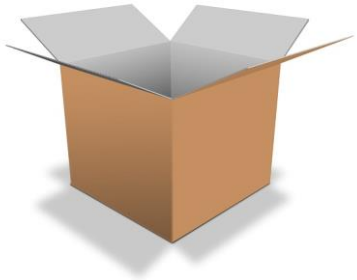
Web Tipp: https://nat.dev

Bausteine und Fehler eines KI-Systems

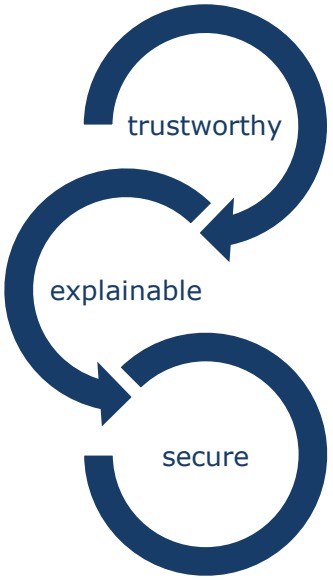


Bausteine und Fehler eines KI-Systems

Grundlegende Frage:



What is in the Box?



Rechtliche Aspekte bei der Verarbeitung von Input- und Trainingsdaten

Input- und Trainingsdaten

Urheber-schutz

- Schützt **Sprachwerke** als auch **grafische Darstellungen**
- § 15 UrhG – grds darf **nur der Urheber** das Werk **vervielfältigen**
- § 42h UrhG – **Text- and Data-Mining** als KI-Inkubator
- § 5 UrhG – stellt auf den Werkbegriff des UrhG ab - Schöpfung

Datenschutz-recht

- Schützt **Verarbeitung** von **personen-bezogenen Daten**
- Art 6 DSGVO – Verarbeitung **nur in bestimmten Fällen rechtmäßig**
- Art 12ff DSGVO – Umfangreiche **Informationspflichten** des Verantwortlichen
- Art 22 DSGVO – Besondere Anforderungen für **automatisierte Datenverarbeitung**

Know-How-Schutz

- § 26c UWG – Rechtswidriger Erwerb, **rechtswidrige Nutzung** und **rechtswidrige Offenlegung** von Geschäftsgeheimnissen

Persönlichkeits-rechte

- **Allgemeines Persönlichkeitsrecht** gem § 16 ABGB
- **Diverse Sondertatbestände** in anderen Materien

Urheberrechtliche Aspekte

- privilegierte Nutzungsmöglichkeit **zu Forschungszwecken** (§ 42h Abs 1-5 UrhG)
  - **freie Werknutzung zur Vervielfältigung**,

    "um damit Texte und Daten in digitaler Form für die wissenschaftliche […] Forschung automatisiert auszuwerten und Informationen unter anderem über Muster, Trends und Korrelationen zu gewinnen, wenn er zu dem Werk rechtmäßig Zugang hat […], soweit dies zur Verfolgung nicht kommerzieller Zwecke gerechtfertigt ist"
  - = **Unterfall der Vervielfältigung zum eigenen Gebrauch** (ErläutRV)
  - jede Nutzungshandlung, die der Einrichtung zugeordnet werden kann
    - auch Studenten, die für die Einrichtung Arbeiten verfassen

Datenschutzrechtliche Aspekte

- Mögliche Rechtsgrundlagen

Personenbezogene Daten	Sensible Daten	Bei Zugriff auf Informationen im Endgerät
→ Art 6 DSGVO, Art 22 DSGVO	→ Art 9 DSGVO	→ Art 5 Abs 3 ePrivacy-RL
Vertragserfüllung, Einwilligung, berechtigte Interessen	Einwilligung	Einwilligung, außer zur Bereitstellung des Dienstes erforderlich oder Übertragung über ein Kommunikationsnetzwerk

- Einzelfallbeurteilung
- Überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten als praxistauglichste Rechtsgrundlage
- Drei Grundvoraussetzungen für berechtigte Interessen
  - Berechtigtes Interesse des Verantwortlichen oder eines Dritten
  - Erforderlichkeit der Verarbeitung zur Wahrung der berechtigten Interessen
  - Kein Überwiegen der Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person

Datenschutzrechtliche Aspekte

Automatisierte Entscheidungsfindung?

- idR einwilligungspflichtig

Abgrenzungsfragen

- Automatisierung eines Prozesses, Ablaufs oder von Verarbeitungsschritten ist keine automatisierte Entscheidung, wenn Entscheidung
  - schon vor Automatisierung getroffen wird; oder
  - nach einem automatisierten Prozess durch einen Menschen erfolgt; oder
  - wenn ein Mensch mit ausreichend Abweichungsmöglichkeit eingreift

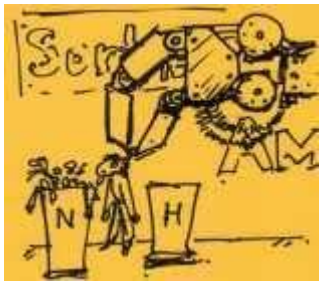
- selbst wenn Entscheidung automatisiert, greift Art 22 nur bei
  - rechtlicher Wirkung oder
  - ähnlich erheblicher Beeinträchtigung

- Profiling durch Art 22 daher weder untersagt noch beschränkt
  - marketinggetriebenes Profiling/Kundensegmentierung regelmäßig zulässig
  - dennoch greifen erhöhte Informations- und Auskunftspflichten (zur Logik)

Beispiel

Automatisierte Bewertung der Jobchancen am Arbeitsmarkt

BVwG W256 2235360-1 – Der AMS-Algorithmus



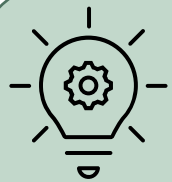
Rechtliche Aspekte bei der Verarbeitung von Outputdaten

Outputdaten

Urheber-schutz

Voraussetzung:
- Voraussetzung ist eine geistige Schöpfung durch einen Menschen

Schutzfähigkeit:
- KI dient nur als Werkzeug und menschlicher Einfluss überwiegt



Patentschutz

Voraussetzung:
- Denkbare Erfüllung der Voraussetzungen eines Patents (Erfindung auf dem Gebiet der Technik, Neuheit etc)
- **aber**: Voraussetzung für den Anspruch auf ein Patent nach § 4 PatG hat der "*Erfinder oder sein Rechtsnachfolger*"

Know-How-Schutz

Denkbare **Schutzfähigkeit** nach den Voraussetzung von **§ 26b UWG**:
Information, die
- Geheim ist,
- kommerziellen Wert hat und
- Gegenstand von Geheimhaltungsmaß nahmen ist

Outputdaten

- KI als "*Schöpfer„*?
  - Natürlichen Personen vorbehalten
- KI-Output urheberrechtlich geschützt?
  - Pro
    - Menschliche Anweisung/Steuerung
  - Contra
    - Der Mensch weiß nicht genau, wie die KI „denkt" und sich „weiterentwickelt"
  - Möglicher Lösungsweg über die Werkhöhe?
    - Bei ausreichend detaillierter Anweisung ist der Anwender Urheber

Beispiel
Regisseur gibt Story-Line, Akteure und wesentliche Plot-Szenarien vor
→ Anwender = Urheber

Rechtliche Risiken beim Einsatz von ChatGPT

ChatGPT – Steht der Chatbot vor dem Aus?

Italien: GPDP vs ChatGPT

Konkrete Bedenken

- Mangelnde Informationen
- Fehlende Rechtsgrundlage
- Data-Breach Informationen
- Ungenaue Datenverarbeitung
- Fehlende Altersüberprüfung
- **Sperrung ausgesetzt**

Weitere Länder nehmen ChatGPT unter die Lupe

Behörden anderer Länder

- **Frankreich**: CNIL prüft ChatGPT aufgrund von 5 Beschwerden
- **Spanien**: AEPD fordert EU-Behörden zum Handeln auf
- **Deutschland** – Ministerien für Regulierung
- **Kanada** –Prüfverfahren

Chat-GPT – Lessons learned?

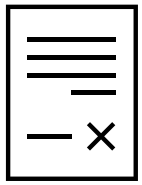
Fazit:

- Mangeldne Regulierung der Technologie: breitere Koordinierung der Regulierung ist gefragt (AI-Act)
- Effektivität einer Sperre: VPNs bieten eine Umgehungsmöglichkeit einer Sperre
- Dialog mit OpenAI wäre ebenfalls möglich gewesen um Themen wie Altersbestätigung etc auszuräumen

Haftung für KI-Fehler

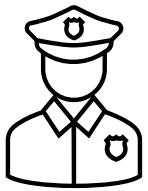
Haftung und KI - Wer muss für Fehler einstehen?

- Vertragshaftung
  - Schadenersatz nach §§ 1295 ff ABGB
  - Trifft den **schuldhaften Vertragspartner**



- Verschuldensunabhängige Produkthaftung
  - § 1 Produkthaftgesetz
  - Trifft den **Hersteller und Importeur**

- Behördliche Haftung
  - Art 83 DSGVO
  - Strafen bis zu 4% des Jahresumsatzes oder EUR 20.000.000,00
  - Trifft den **Nutzer der KI (Verantwortlichen)**



Ausblick auf die KI-Regulierung

Ausblick auf den AI Act

Verlässliche AI umfasst dabei 6 Dimensionen

1. Ist eine Anwendung „fair", sodass sie vorteilsfrei und transparent Entscheidungen trifft?

2. Ist sichergestellt, dass Nutzerinnen und Nutzer die Kontrolle haben und Entscheidungen einer Anwendung revidieren können?

3. Sind die Entscheidungen einer AI-Anwendung erklärbar und nachvollziehbar?

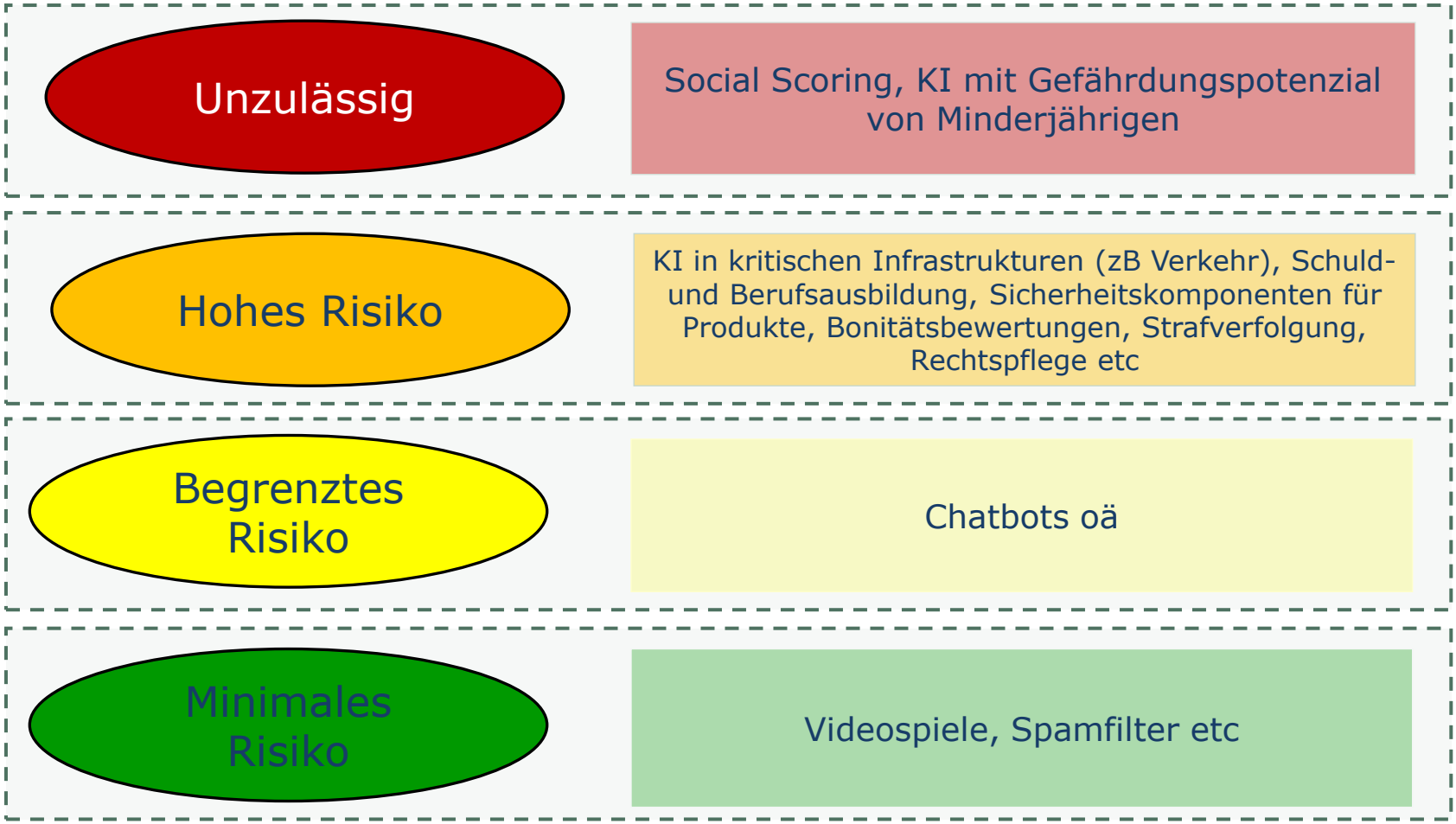
4. Ist die Anwendung technisch robust aufgebaut?

5. Bietet das AI-System Schutz vor unbefugtem Zugriff?

6. Ist der Datenschutz gewährleistet?

Ausblick auf den AI Act

Risikobasierter Ansatz und abgestuftes Pflichtenregime



Ausblick auf den AI Act

Maßnahmen zur Förderung von Innovation

- Regulatory Sandbox-Programme
  - Testing von KI-Anwendungen unter Behördenaufsicht
  - KMUs und Startups sollen bevorzugt aufgenommen werden

Strafen

- bis zu 6% des weltweiten Jahresumsatzes oder 30 Millionen Euro für bestimmte Verstöße (zB verbotene Praktiken gem Art 5)
- bis zu 4% des weltweiten Jahresumsatzes oder 20 Millionen Euro für bei Verstößen von KI-Systemen gegen die festgelegten Anforderungen und Pflichten
- bis zu 2% des weltweiten Jahresumsatzes oder 10 Millionen Euro bei falschen, irreführenden oder unvollständigen Angaben gegenüber Behörden auf deren Auskunftsverlangen

Haftung und KI - Wer muss für Fehler einstehen?

Neue EU-Haftungsregelungen in den Kinderschuhen

<u>Entwurf der Produkthaftungs-Richtlinie</u>

- Software = Produkt
- Definition des Produktfehlers
- Ausweitung des Schadensbegriffs
- Offenlegung von Beweismitteln in Verfahren

<u>Entwurf der KI-Haftungs-Richtlinie</u>

- Betrifft nicht-vertragliche Ansprüche
- Erweitere Offenlegungspflicht von Beweismitteln
- Kausalitätsvermutung bei Verschulden
- Verschuldensvermutung bei "Hochrisikosysteme" im Fall eines KI-Verordnungs-Verstoß

Q&A

Trend Anwaltsranking (2022)
Axel Anderl
Data Protection , IP and Media
Top 2 overall ranking

The Legal 500 (2023)
TMT
Tier 1

The Legal 500 (2023)
Data Privacy & Data Protection
Tier 1

The Legal 500 (2023)
Axel Anderl (TMT)
Hall of Fame

DORDA

Austria Firm of the Year

Talent Management – Firm of the Year

Women in Business Law Awards Europe 2021

Client Choice winner IT & Internet

Client Choice Awards 2021

Who's Who Legal (2022)
Axel Anderl (Data Privacy & Protection)
Thought Leader Global Elite

Chambers Europe (2023)
TMT:IT
Band 1

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien · www.dorda.at