KI & Recht – eine explosive Mischung

ADV Rechtstag| 7.11.2024

RA MMag. Norbert Amlacher

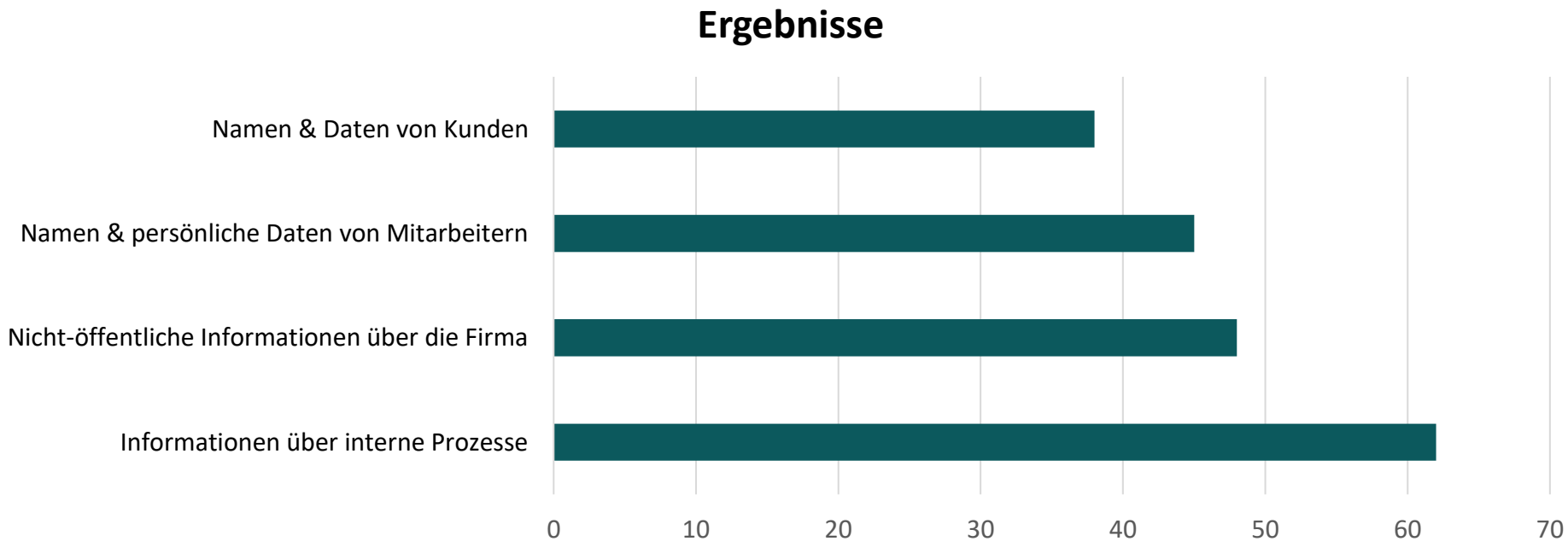
Partner bei andréewitch & partner rechtsanwälte GmbH (Wien)

Wie stellt sich die KI das vor?


stablediffusionweb.com

Welche Daten werden in generative KI-Tools eingegeben?

Befragt wurden **2.600 „Security Professionals“** in **12 Staaten** (u.a. USA, Brasilien, UK, Deutschland, Frankreich, Spanien, Italien, China, Japan) im Rahmen der **Cisco** Data Privacy Benchmark Study 2024 (Bericht im Handelsblatt)



Schatten-KI

Sieben von zehn Arbeitnehmern nutzen KI-Werkzeuge ohne Freigabe ihrer Firma

Der Druck bei der Arbeit ist hoch. Künstliche Intelligenz kann Abhilfe schaffen, aber viele Firmen zögern mit dem Einsatz. Beschäftigte handeln einfach selbst.

Stephan Scheuer
09.05.2024 - 15:07 Uhr

Quelle: Handelsblatt, https://www.handelsblatt.com/technik/ki/schatten-ki-sieben-von-zehn-arbeitnehmern-nutzen-ki-werkzeuge-ohne-freigabe-ihrer-firma/100037174.html

Übersicht

1. Was sind KI-Systeme?
2. Eigene Erstellung eines KI-Systems
3. „Zukauf“/Verwendung eines KI-Systems
4. Training eines KI-Systems
5. Inputs in & Outputs von KI-Systemen
6. Ausgewählte Anforderungen zu Daten aus dem AI-Act

1. Was sind KI-Systeme?

- aktuell **keine einheitliche Definition**
- Definition aus **Art 3 Z 1 AI-Act**

  *„ein **maschinengestütztes** System,*

  *das für einen in unterschiedlichem Grade **autonomen Betrieb** ausgelegt ist*

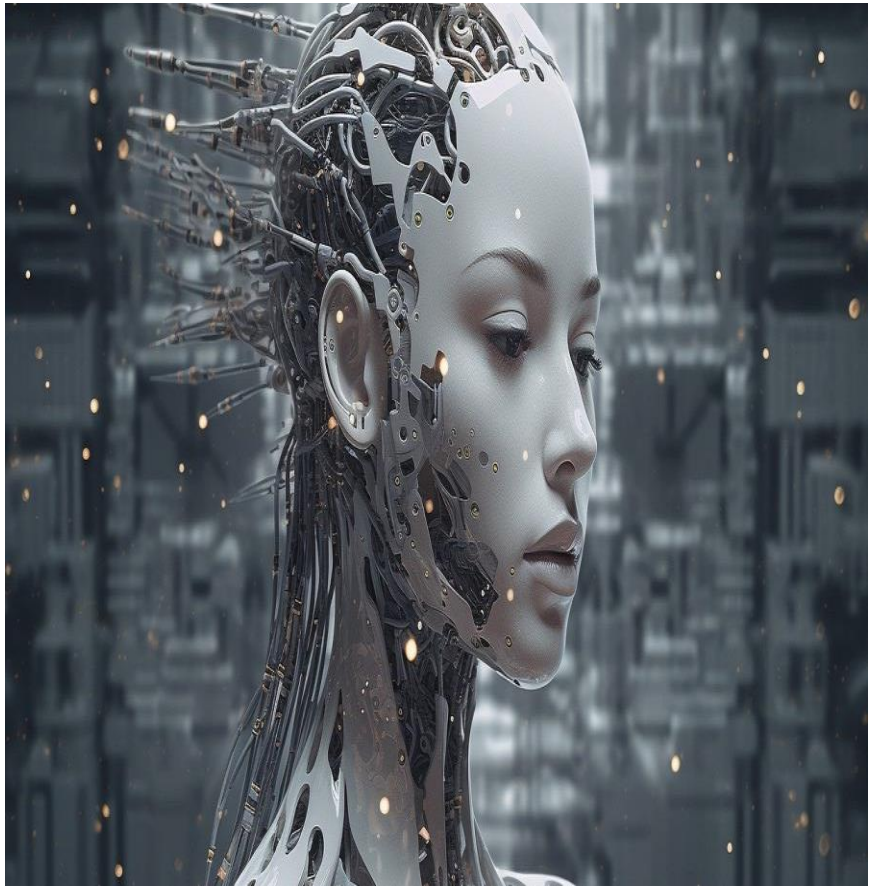
  *und das nach seiner Betriebsaufnahme **anpassungsfähig** sein kann und*

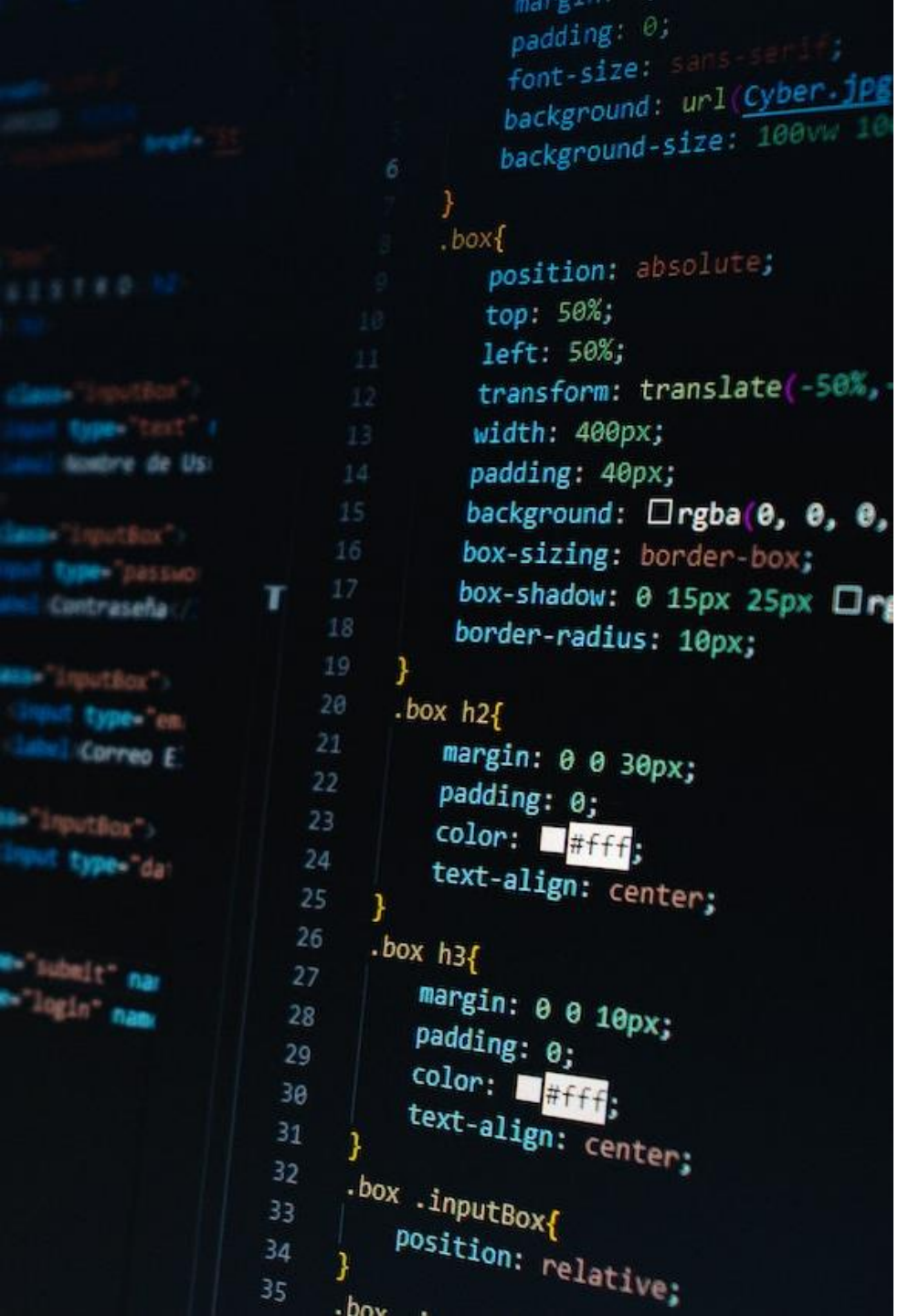
  *das aus den erhaltenen Eingaben für **explizite oder implizite Ziele ableitet**,*

  wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden,

  *die physische oder virtuelle Umgebungen **beeinflussen** können*"

- **Abgrenzung** zu klassischer **Software? ⇔ Erwägungsgrund 12 AI-Act** u.a. "*Ein wesentliches Merkmal von KI-Systemen ist ihre Fähigkeit, abzuleiten*" & „*Die Fähigkeit eines KI-Systems, abzuleiten, geht über die einfache Datenverarbeitung hinaus*" & Verweis auf **maschinelles Lernen**





2. Eigene Erstellung eines KI-Systems

i. Urheberrechtliche Schutzfähigkeit des **KI-Systems als Computerprogramm** (§ 40a UrhG)?

ii. Urheberrechtlicher **Schutz der Gewichtungen** (bzw. des trainierten Netzwerks)?

iii. Verwendung von **Open Source** Komponenten (Achtung: viraler Effekt)

iv. ggf. Schutz als **Betriebs- und Geschäftsgeheimnis** (§ 26a ff UWG)

- geheim
- kommerzieller Wert
- **angemessene Geheimhaltungsmaßnahmen**

3. „Zukauf“/Verwendung von KI-System

i. Welche **vertraglichen Regeln/Zusicherungen** werden beim Kauf/Verwendung gemacht?
   - Beschreibung des KI-Systems (Leistungsbeschreibung)
   - welche Rechte werden eingeräumt
   - Trainingsdaten / pre-training (Datenqualität; kein bias; Behebung von Trainingsfehlern)

ii. Wer macht die **Anpassung** (selbst oder extern?) – vertragliche Regelungen / Rechteeinräumung

iii. Erfolgt die Nutzung **on-premise** oder im Rechenzentrum des Anbieters (**SaaS**)? Themen insbesondere Datensouveränität & DSGVO (AVV, Drittlandstransfer, etc.)

4. Training eines KI-Systems

i. **Woher** bekomme ich die Daten?
   - Intern (Datenqualität? Datenumfang?)
   - extern (selbst beschafft/gecrawled)
   - externer „Zukauf“ (Zusicherungen)?

ii. **Qualität** der Daten sicherstellen (richtig, repräsentativ, etc.)

iii. **Urheberrechtliche Grenzen**, ggf. Text- und Data-Mining (§ 42h UrhG)

iv. **Datenschutzrechtliche Grenzen** (u.a. Big Data, Zweckbindung):
   - Rechtfertigung im Rahmen von Art 6 DSGVO und Art 9 DSGVO (sensible Daten)
   - Dokumentation
   - Datenschutzfolgenabschätzung
   - Betroffenenrechte

v. **Anonymisierung, synthetische Daten, federated learning**

5. Input in & Output von KI-Systemen

i. **Input durch den Anwender**

- Was darf ich als **Input/Prompt** verwenden? > **Nutzungsbedingungen** beachten
- Schutz von **Betriebs- und Geschäftsgeheimnissen** beachten > Vertraulichkeit
- **Richtlinien** für die Verwendung von KI-Systemen durch Mitarbeiter

ii. **Output eines KI-Systems**

- **Urheberrechtlicher Schutz** des Outputs: Menschliche Schöpfung? KI als Hilfsmittel?
- **Vertragliche Nutzungsrechte**? Was darf ich mit dem Output machen?
- **Haftung** für (unrichtigen) Output bzw. für Nutzung des KI-Systems
- **Automatisierte Entscheidung & Profiling** (Art 22 DSGVO) grds. bei personenbezogenen Daten verboten, wenn sie **rechtliche Wirkung** entfaltet oder sie in **ähnlicher Weise erheblich beeinträchtigt**, nur ausnahmsweise zulässig (z.B. ausdrückliche Einwilligung) + **Verpflichtung zur Information** über Existenz des autom. Entscheidungsprozesses, involvierte Logik, Tragweite & Auswirkung der Entscheidung; DSFA

6. Anforderungen aus dem AI-Act zu Daten

Zahlreiche Pflichten bei **„High Risk AI Systems“** bezüglich **Data & Data Governance (Art 10)**

i. Unterschiedliche **Datenkategorien**, z.B. „*Trainingsdaten*“ (Art 3 Z 29), „*Validierungsdaten*“ (Art 3 Z 30; kann Teil der Trainingsdaten sein) und „*Testdaten*“ (Art 30 Z 31; Überprüfung des KI-Systems vor Inverkehrbringen)

ii. Daten müssen „*im Hinblick auf die Zweckbestimmung* ***relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig*** *sein.*“ (Art 10 Abs 3)

iii. Es müssen grundsätzlich **geeignete Daten-Governance- und Datenverwaltungsverfahren** vorliegen, wobei insbesondere folgende Punkte berücksichtigt werden müssen (Auszug aus Art 10 Abs 2):

- **Datenerhebungsverfahren**, Herkunft der Daten und bei personenbezogenen Daten ursprünglicher Zweck der Datenerhebung
- Relevante **Datenaufbereitungsvorgänge**, wie Annotationen, Labelling/Kennzeichnung, Bereinigung, Aggregation, Anreicherung
- die Aufstellung von **Annahmen**, insbesondere in Bezug auf die Informationen, die mit den Daten erfasst und dargestellt werden sollen
- eine **Bewertung** der Verfügbarkeit, Menge und Eignung der benötigten Datensätze
- Eine Untersuchung im Hinblick auf mögliche Verzerrungen (**biases**) + geeignete Maßnahmen zur Erkennung, Verhinderung und Abschwächung solcher Biases
- die Ermittlung relevanter **Datenlücken** oder Mängel, die der Einhaltung dieser Verordnung entgegenstehen, und wie diese Lücken und Mängel behoben werden können

iv. Gesetzliche **Verarbeitungsgrundlage** für **sensible Daten** in sehr engen Grenzen iZm Bias-Detektion & Korrektur in Art 10 Abs 5 (aber nicht für „normale“ personenbezogene Daten?)

op-online

Robert Downey Jr. sicher: Marvel ersetzt ihn niemals mit KI

ORF
https://orf.at › stories

Klage der Musikindustrie gegen KI-Start-ups

Der Standard
https://www.derstandard.at › Web › Netzpolitik

Sammelklage von Autorinnen und Autoren gegen KI-Firma ...

SZ.de
https://www.sueddeutsche.de › Wirtschaft › Technologie

KI: Mutter verklagt Chatbot-Firma nach Suizid ihres Sohnes

Wiener Zeitung
https://www.wienerzeitung.at › wo-ki-vor-gericht-mitsp...

Wo KI vor Gericht mitspricht - Künstliche Intelligenz

Tagesspiegel Background
https://background.tagesspiegel.de › briefing › ki-proze...

KI-Prozess: Landgericht weist Klage von Fotografen ab

andréewitch & partner rechtsanwälte gmbh

Key Points

- Der AI-Act gilt zwar erst ab 2.2.2025, KI-Systeme operieren aber aktuell **nicht im „rechtsfreien“ Raum**
- Auf allen „Stufen“ sind **rechtliche Hürden** zu beachten
- Schon **vor Projektbeginn** sind diese Hürden zu identifizieren und mögliche Lösungen zu adressieren
- Frühzeitige **Auseinandersetzung** mit dem AI Act, ob bzw. inwiefern man selbst betroffen ist
- Organisationsweite **allgemeine Richtlinien** zu Umgang mit KI-Systemen (z.B. Mitarbeiter, Procurement, etc.) + **Schulungen** sind sinnvoll

Vielen Dank für Ihre Aufmerksamkeit!

Fragen? Anmerkungen?

RA MMag. Norbert Amlacher

andréewitch & partner rechtsanwälte GmbH
Stallburggasse 4, 1010 Wien
www.andlaw.at
Telefon: +43 (1) 533 31 58
E-Mail: office@andlaw.at