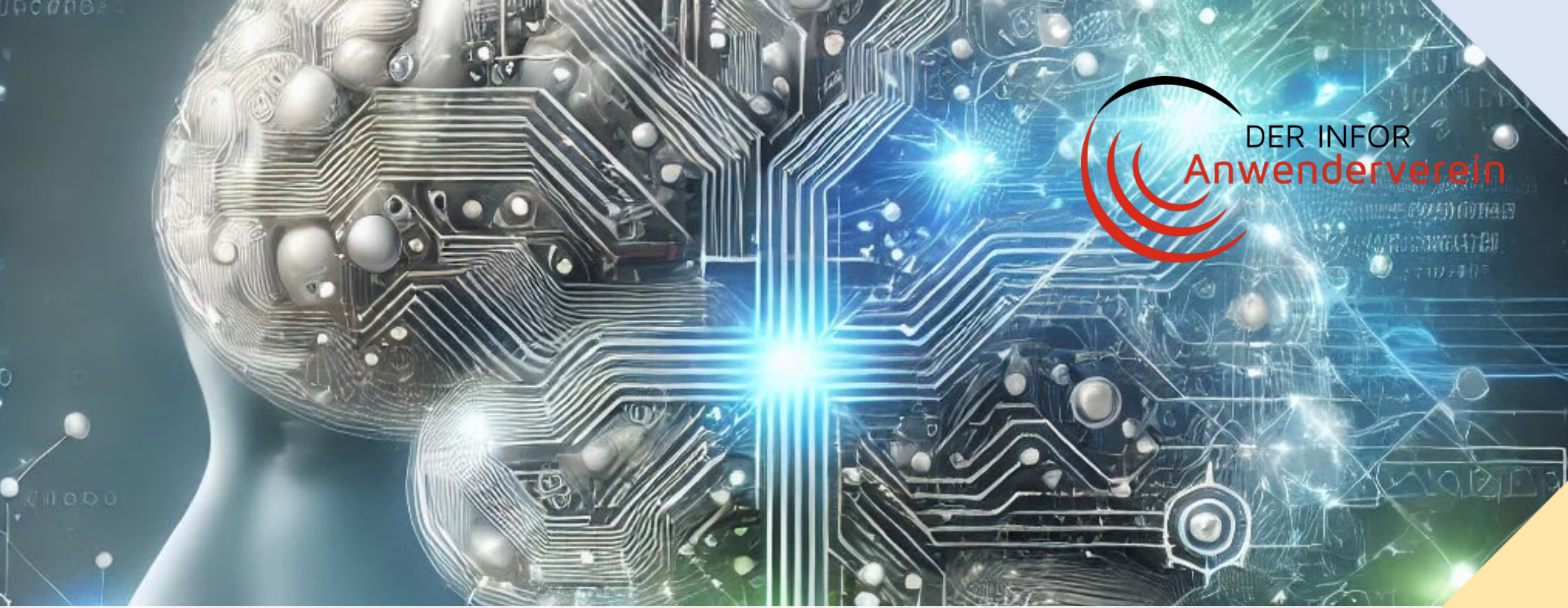


DER INFOR Anwenderverein

KI aus den Gesichtspunkten Datenschutz/Datensicherheit

SACHVERSTÄNDIGENBÜRO MÜLOT

Claus Wissing (Geschäftsführer SVB Mülot GmbH)

- Geschäftsführer und externer Datenschutzbeauftragter für sehr viele Organisationen
- Freier Sachverständiger in den Bereichen Datenschutz, Datensicherheit und Informationssicherheit
- Langjährige Erfahrung im Bereich der Telekommunikations- und IT-Technik
- Zertifizierter Datenschutzbeauftragter und Datenschutzauditor (TÜV-Rheinland)
- Compliance Officer (TÜV-Rheinland)

Fachgebiete

- Planung u. Aufbau von DSM-Systemen, ISMS-Systemen
- Datenschutz u. Informationssicherheit
- Schulungen
- Konzerndatenschutz

Spezialkompetenz(en)

- Telekommunikation
- Kirchlicher Datenschutz und soziale Einrichtungen

Ihr Referent

Denis Zensen

- Studium der Rechtswissenschaften (2. Staatsexamen)
- Langjährige Tätigkeit als zugelassener Rechtsanwalt und Fachanwalt
- Zertifizierter Datenschutzbeauftragter (TÜV-Rheinland)

Fachgebiete

- Datenschutz
- Compliance
- Kommunikation
- KI

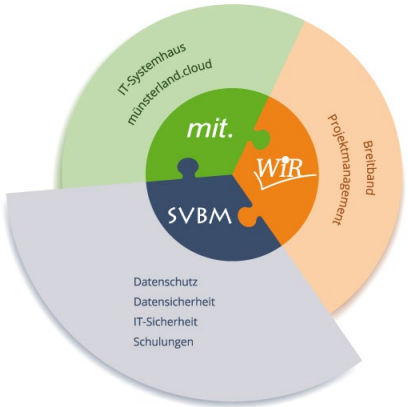
Spezialkompetenz(en)

- Verträge im Datenschutz
- Betroffenenrechte

Sachverständigenbüro Mülot GmbH

Wo kommen wir her?

- 1999 von Dirk-Michael Mülot als Einzelunternehmen gegründet
- 2018 Übergang in die Sachverständigenbüro Mülot GmbH mit Claus Wissing als Geschäftsführer
- Standorte in Greven und Langenberg



Was können wir?

- Über 20 Jahre Erfahrung in Datenschutz- und Datensicherheitsthemen nach DSGVO und kirchlichen Datenschutzgesetzen
- Starke Unternehmensgruppe für IT-Projektmanagement, Digitalisierung, Prozessautomatisierung, sichere Systemhauslösungen
- Insgesamt > 50 Beschäftigte mit Fachkompetenz (Ingenieure, Projektmanager, Rechtsanwälte, Planer, IT-Sicherheitsexperten, …)

25 Jahre Erfahrung und Lösungsorientierung

2024

- Ausweitung der innovativen Datenschutz-Dienste (Institut.com, VVT-Easy, DSMS-Dienste)
- Informationssicherheit (ISO 27001, Tisax, KRITIS, NIS2), Hinweisgeberschutz für verschiedenste Branchen
- Exzellente Dienstleistungen durch ausgebautes professionelles Datenschutz-Team
- Datenschutz- und Datensicherheitsthemen nach DSGVO und kirchlichen Datenschutzgesetzen

2018

- Übergang in die Sachverständigenbüro Mülot GmbH und weiterer Ausbau des Datenschutz-Teams
- Claus Wissing übernimmt die Geschäftsführung

1999-2018

- Stetige Erweiterung der Branchenberatung und Lehraufträge TÜV Rheinland sowie Fortbildungsakademie des Deutschen Caritasverbandes
- Tätigkeiten als „Freier Sachverständiger“ und Zertifizierung als Datenschutzbeauftragter und Datenschutzauditor
- Gegründet als Einzelunternehmen/Freiberufler durch Dirk-Michael Mülot

Über die Landesgrenzen hinaus tätig

Bisheriger Tätigkeitsradius:

EU-weit

- Für Unternehmen in Deutschland und deren Schwestergesellschaften

Europaweit/außerhalb der EU:

- Als Datenschutzvertretung nach Art. 27 DSGVO für Unternehmen außerhalb der EU, welche innerhalb der EU am Markt tätig sind
- In Zusammenarbeit mit Schwesterfirmen und Partner:innen wie der WiR Projects GmbH oder der datenschutzguide.ch GmbH in der Schweiz

International:

- Für international aufgestellte Mandant:innen, die z. B. Geschäftsbereiche oder Konzernmuttergesellschaften in den USA oder in anderen Drittländern haben

Typische Branchen unserer Kunden/Mandanten

Herstellende Industrie:

- Automobilindustrie (incl. Prototypenbau)
- Industrielle Fertigung, Maschinenbau
- Logistik, Reedereien, Distribution

Konsumgüter:

- Bekleidung und Mode
- Lebensmittel und Getränkeindustrie

Gesundheitswesen:

- Versicherungen, Kliniken, Arztpraxen
- Pflegeeinrichtungen

Finanzwesen:

- Versicherungen, Banken, Immobilienwesen

Soziale Organisationen:

- Kirchliche Träger: Bistümer, Kirchliche Gemeinden, Caritasverbände
- Sportverbände, Sportvereine

Bildungseinrichtungen:

- Große Träger der Erwachsenenbildung zur Sensibilisierung

Willkommen zum heutigen Stammtisch

Infos zur Durchführung

Regeln

- Die Mikrofone sind bitte ausgeschaltet, können aber von bei Bedarf eingeschaltet werden.
- Meldungen bitte über Handzeichen.
- Fragen – auch zur Technik – bitte in den Chat schreiben.

Unterlagen

- Foliensatz steht am Ende zur Verfügung.
- Feedback steht anschließend zur Verfügung.

Hinweis:
Das Web-Seminar wird **nicht** aufgezeichnet. Aufzeichnungen durch die Teilnehmenden sind **nicht** erlaubt!


1
Einleitung


AI
AI
2
Rechtliche Grundlagen


AI
3
Datenschutz und KI


4
Risiken kennen


AI
AI
AI
AI
5
Haftung und Künstliche Intelligenz


AI
6
Best Practices

1 Einleitung

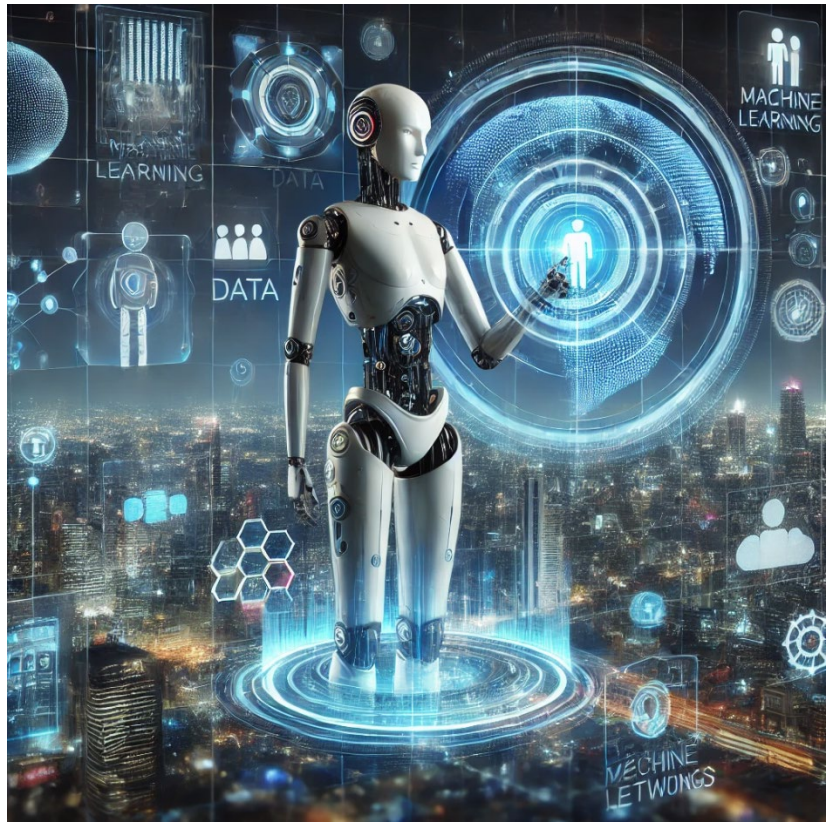
Einleitung

Was ist Künstliche Intelligenz?

Definition (Art. 3 Nr. 1 KI-VO)

- Maschinengestütztes System
- Grad an Autonomie
- Potenziell anpassungsfähig
- Leitet aus Eingaben Ausgaben ab (Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen)
- Beeinflusst Umgebung

Die künstliche Intelligenz (KI) ist der Versuch, menschliches Lernen und Denken auf Computersystemen nachzubilden.



Einleitung

Warum gerade jetzt?

Medizin

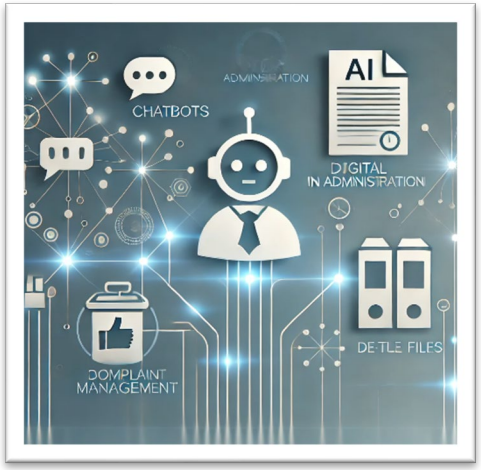
Medikamentenentwicklung
Krankheitsfrüherkennung
Tumorerkennung und Tumorklassifizierung
Operationen
Pflegedokumentation
Exoskelette
Spracherkennung

Industrie

Optimierung des Energieverbrauchs
Vorhersagen von Ausfallwahrscheinlichkeiten
Verbesserung der Prozessqualität
Qualitätsverbesserungen

Marketing

Produktempfehlungen
Textanalysen
Chatbots
Digitale Assistenten
Dynamische Präsentationen und Einkaufserlebnisse



Verwaltung

Chatbots
Beschwerdemanagement
Personaleinsatzplanung
Wissensmanagementsysteme
E-Akten

2 Rechtliche Grundlagen

Rechtliche Regelungen

Die KI-Verordnung

- Die künstliche Intelligenz (KI) und die rasante Entwicklung in diesem Bereich hat weitreichende Auswirkungen auf alle Lebensbereiche.

- Der Zweck der Verordnung ist es, die Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen künstlichen Intelligenz zu fördern und gleichzeitig ein hohes (Daten-)Schutzniveau in Bezug auf Gesundheit, Sicherheit und Einhaltung der Grundrechte vor schädlichen Auswirkungen von KI-Systemen zu gewährleisten.

- Die Europäische Union (EU) hat dies frühzeitig erkannt und am 12. Juli 2024 ein entsprechendes Gesetzgebungsverfahren (AI-Act, KI-Verordnung) im Amtsblatt der EU veröffentlicht.

- Die KI-VO trat zum 01. August 2024 in Kraft.

Rechtliche Regelungen

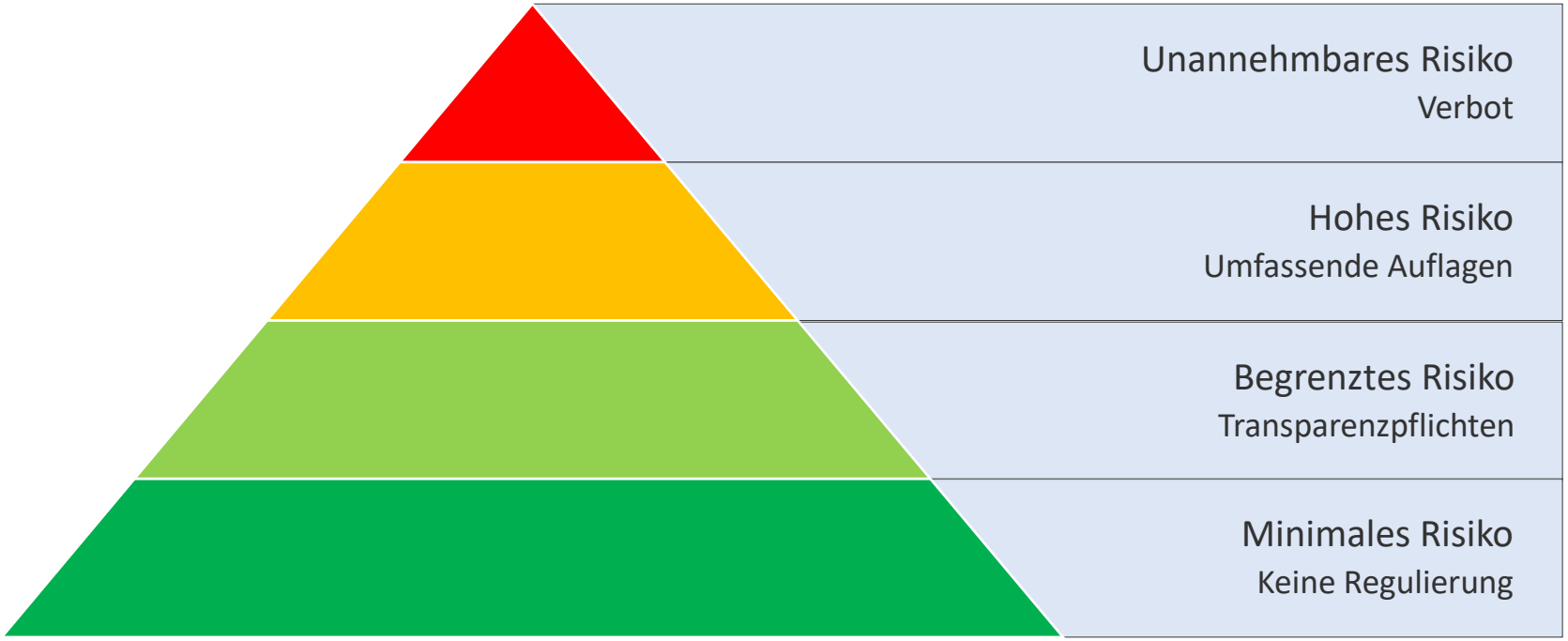
Umsetzungstermine

- **Ab 02. Februar 2025** (Art. 113 lit. a) AI-Act)
  - Die allgemeinen Vorschriften müssen umgesetzt und verbotene Praktiken eingestellt sein
  - Kapitel I und II der KI-Verordnung gelten ab diesem Termin
- **Ab 02. August 2025** (Art. 113 lit. b) AI-Act)
  - Beginn der Geltung von Regelungen mit allgemeinem Verwendungszweck
  - Beginn der Geltung und Umsetzung von vorgesehenen Sanktionsmechanismen
- **Ab 02. August 2026** (Art. 113 AI-Act)
  - Beginn der allgemeinen Geltung der Verordnung
- **Ab 02. August 2027** (Art. 113 lit. c) AI-Act)
  - Beginn der Geltung der Umsetzungspflicht der Harmonisierungsvorschriften aus Anhang I in Kombination mit weiteren EU-Richtlinien – Neue Hochrisiko-Anwendungsgruppen entstehen

KI-Verordnung

Risikobasierter Ansatz

- Die KI-Verordnung legt Verpflichtungen für Anbieter und Nutzer fest.
- Die Verpflichtungen richten sich nach den Risiken, die vom KI-System ausgehen.
- Jedes KI-System muss daher einzeln bewertet werden.



KI-Verordnung

AI-Act-Kompass für Anwender

KI-Verordnung

Hochrisiko-KI-Systeme

- Pflichten der Anbieter und Betreiber sowie anderer Beteiligter
  - Pflichten der Anbieter (Art. 16)
  - Einrichtung eines Qualitätsmanagementsystem (Art. 17)
  - Aufbewahrung der Dokumentation (Art. 18)
  - Automatisch erzeugte Protokolle mit mind. sechsmonatiger Aufbewahrung (Art. 19)
  - Korrekturmaßnahmen und Informationspflichten (Art. 20)
  - Zusammenarbeit mit Behörden und Bevollmächtigter der Anbieter (Art. 21 und 22)
  - Pflichten der Einführer und Händler (Art. 23 und 24)
  - Verantwortlichkeiten entlang der KI-Wertschöpfungskette (Art. 25)
  - Pflichten der Betreiber (Art. 26)
  - Grundrechte-Folgenabschätzung (Art. 27)

KI-Verordnung

Transparenzverpflichtungen für Systeme, die für die Interaktion mit Personen bestimmt sind

- Hiervon sind drei Arten von Systemen betroffen
  - KI-Systeme, die für die Interaktion mit natürlichen Personen bestimmt sind, sind so zu konzipieren, dass der Person mitgeteilt wird, dass sie mit einem KI-System interagiert.
  - KI-Systeme mit allgemeinem Verwendungszweck, welche Audio-, Bild-, Video- oder Textinhalte erzeugen, müssen sicherstellen, dass die Ergebnisse als künstlich erzeugt oder manipuliert erkennbar sind und in einem maschinenlesbaren Format gekennzeichnet sind.
  - Betreiber von Systemen zur biometrischen Kategorisierung müssen betroffene Personen über die Einbindung des KI-Systems informieren.

3 Datenschutz und KI

Datenschutz und KI

Rechtlicher Rahmen

DSGVO

- Primärer Rechtsrahmen für personenbezogene Daten, auch im KI-Kontext
  - ➢Datenverarbeitung
  - ➢DSFA
  - ➢Privacy by Design

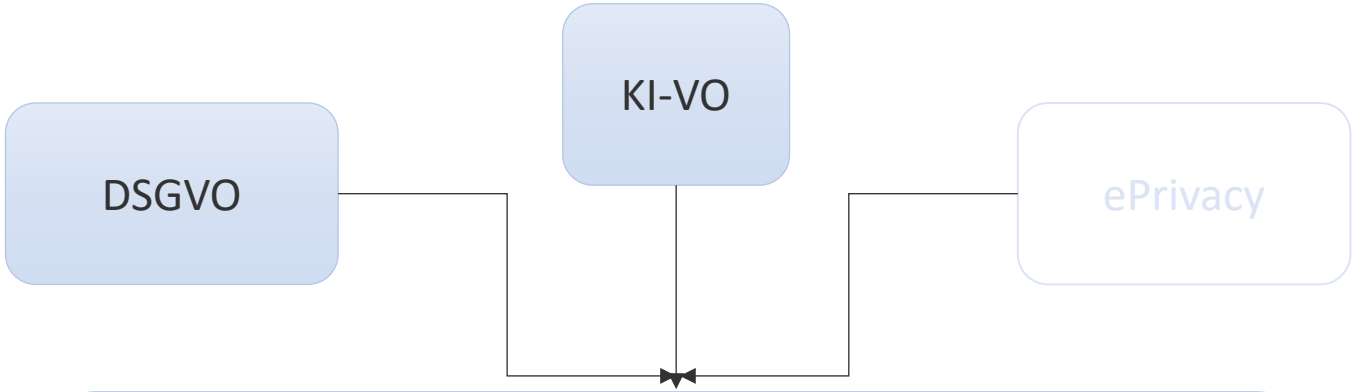
KI-VO

- zielt darauf ab, den Einsatz von KI-Technologien sicherer und transparenter zu gestalten, u.a.:
  - ➢Risikomanagement
  - ➢Konformitätsbewertung
- regelt nicht den Umgang mit personenbezogenen Daten
- Verweist auf DSGVO

DSGVO regelt **„Daten“**, die KI-VO regelt **„Systeme & Risiken“** – in der Praxis sind **beide** zu erfüllen

Datenschutz und KI

Rechtlicher Rahmen



Synergien

Risikomanagement (KI-VO) vs. Datenschutzfolgenabschätzung (DSGVO)

- Beide erfordern systematische Risikoidentifikation.
- DSFA als Umsetzungshilfe: Bereits durchgeführte Datenschutzfolgenabschätzungen decken Teile des KI-Risikomanagements ab

Managementsysteme (KI-Management)

- Kann an bestehende Datenschutzmanagementsysteme (DSMS) angeknüpft werden.
- Vorteil: Nutzung vorhandener Strukturen (z.B. Dokumentationsprozesse, Schulungen)

Rollen und Verantwortlichkeiten

- **DSB** kann **KI-relevante Aufgaben** übernehmen (z.B. Sensibilisierung, Beratung zu Datennutzung)

Datenschutz und KI

DSGVO-Kompass für KI

Die DSGVO unterscheidet nicht zwischen "normaler" und "KI-basierter" Datenverarbeitung. Für jede KI-Anwendung müssen Sie prüfen:

Rechtsgrundlage (Art. 6 DSGVO)

- Einwilligung (meist unpraktikabel)
- Berechtigte Interessen (häufigster Fall)
- Vertragserfüllung

Informationspflichten (Art. 13/14 DSGVO)

- Transparenz über KI-Nutzung
- Erklärbarkeit von Algorithmen

Betroffenenrechte

- Recht auf Auskunft über automatisierte Entscheidungsfindung
- Widerspruchsrecht bei berechtigten Interessen

Datenminimierung & Zweckbindung (Art. 5)

Trainingsdaten nur, wenn **erforderlich**

Pseudonymisierung/Anonymisierung bevorzugen

Datenschutz und KI

Prüfen der KI-Anwendung

Beispiel:

Startseite > News >

ChatGPT verbreitet falsche Infos über Personen – und OpenAI kann nichts tun

Data Subject Rights / Mon, 29.04.2024 - 07:00

Die DSGVO der EU verlangt von Unternehmen, dass Informationen über Personen korrekt sind. Betroffene müssen zudem vollen Zugang zu ebendiesen Informationen und zu ihrer Quelle erhalten. OpenAI scheint das egal zu sein: Das Unternehmen gibt offen zu, falsche Informationen auf ChatGPT nicht korrigieren zu können. Das Unternehmen weiß nicht einmal, woher die Daten stammen oder welche Daten ChatGPT über einzelne Personen speichert. OpenAI ist sich dieses Problems bewusst. Anstatt etwas zu verändern, argumentiert das Unternehmen jedoch einfach, dass *„faktische Genauigkeit in großen Sprachmodellen ein Bereich aktiver Forschung bleibt“*. *noyb* hat nun eine Beschwerde gegen OpenAI eingereicht.

Quelle: https://noyb.eu/de/chatgpt-provides-false-information-about-people-and-openai-cant-correct-it

Datenschutz und KI

Prüfen der KI-Anwendung

Probleme bei Betroffenenrechten:

- **Black-Box-Charakter**: Viele KI-Systeme, insbesondere neuronale Netzwerke, sind schwer nachvollziehbar. Dies erschwert die Auskunft, warum und wie eine Entscheidung getroffen wurde.
- **Training auf personenbezogenen Daten:**Daten, die in den Trainingsdaten enthalten sind, könnten für Berichtigung oder Löschung unzugänglich sein.
- **Große Datenmengen:** KI-Systeme verarbeiten oft riesige Datensätze, was die Identifikation spezifischer personenbezogener Daten erschwert.
- **Automatisierte Entscheidungen:** Entscheidungen basierend auf KI können persönliche Rechte beeinträchtigen, z. B. bei Kreditvergaben oder Bewerbungsprozessen.

Datenschutz und KI

Prüfen der KI-Anwendung

Recht auf Auskunft: Die Funktionsweise der KI ist komplex, und Datenverarbeitungspfade sind schwer zu erklären.

Lösung: Einsatz von Modellen, die Entscheidungen nachvollziehbar und für Laien verständlich machen

Recht auf Berichtigung: Trainingsergebnisse der KI können nicht direkt „korrigiert“ werden, da sie auf aggregierten Daten basieren.

Lösung: Identifizieren und Korrigieren der fehlerhaften Daten in der Trainingsdatenbank. Modell muss nach Korrekturen neu trainiert werden, um veraltete Informationen zu ersetzen.

Recht auf Löschung: Daten, die in Trainingsdaten verwendet wurden, können schwer isoliert und entfernt werden.

Lösung: Einsatz von Methoden, die es ermöglichen, spezifische Daten aus dem Training eines Modells rückwirkend zu löschen. Falls die Daten nicht gezielt entfernt werden können, muss das Modell mit einem bereinigten Datensatz neu trainiert werden.

Datenschutz und KI

Prüfen der KI-Anwendung

Recht auf Einschränkung der Verarbeitung: Laufende Verarbeitung kann schwer gestoppt oder eingeschränkt werden.

Lösung: Implementierung von Mechanismen, die die Verarbeitung personenbezogener Daten dynamisch pausieren können. Daten, die unter Einschränkung stehen, markieren und für das Modell blockieren.

Recht auf Datenübertragbarkeit: Daten müssen in einem strukturierten, gängigen Format bereitgestellt werden, was bei KI-Systemen mit komplexen Datenstrukturen schwierig ist.

Lösung: Entwicklung von Tools, die es ermöglichen, personenbezogene Daten in Formaten wie CSV oder JSON bereitzustellen.

Widerspruchsrecht: Betroffene können der Datenverarbeitung widersprechen, aber KI-Systeme könnten ohne diese Daten nicht funktionieren.

Lösung: Ein nicht-personenbezogenes Modell oder Optionen zur Verarbeitung anonymisierter Daten nutzen.

Datenschutz und KI

Implementierung von KI-Anwendungen

- **Verantwortlichkeiten festlegen und bindend regeln**
  - AV-Vertrag gem. Art. 28 DSGVO
  - Gemeinsame Verantwortlichkeit gem. Art. 26 DSGVO

- **Interne Regelung und Richtlinien**
  - Klare Regelungen, ob und wie KI-Anwendungen im Arbeitsalltag eingesetzt werden dürfen.
  - Klare interne Richtlinien, Arbeitsanweisung erteilen und dokumentieren.
  - Zu welchen Zwecken darf welche KI-Anwendung verwendet werden.
  - Unterlegung mit Beispielen, die erlaubt und die untersagt sind.
  - Ggfs. sind Dienstvereinbarungen abzuschließen.

Richtlinien und Weisungen

- Der richtige Umgang mit KI-Tools ist über Richtlinien und Arbeitsanweisungen zu regeln.
- Wichtige Punkte hierbei sind:
  - Festlegung des Geltungsbereichs der Richtlinie
  - Festlegung der Verantwortlichkeiten
  - Betroffene Beschäftigte/Bereiche
  - Bei neuen KI-Tools Verweis auf Prüf- und Genehmigungsprozess vor Nutzung
  - Verbotene Datenkategorien und Informationswerte, die mittels KI verarbeitet werden dürfen
  - Alternativ: Erlaubte Datenkategorien und Informationswerte, die mittels KI verarbeitet werden dürfen
  - Rechtliche Prüfung der Ergebnisse auf Copyright
  - Ablage der Ergebnisse und Kennzeichnung
  - Prüfung der Einhaltung der Richtlinie
  - Maßnahmen bei Fehlverhalten

Richtlinien und Weisungen

Handlungsleitfaden, Schulung

- Zur Unterstützung der Beschäftigten bei der Nutzung von KI-Anwendungen empfiehlt es sich, dies mit flankierenden Maßnahmen zu untermauern:

  - Transparente Liste der genehmigten KI-Anwendungen
  - Allgemeine Handlungsempfehlungen für die Nutzung der KI-Anwendungen
  - Regelmäßige Sensibilisierungsschulung für den Einsatz von KI-Anwendungen
  - Checklisten

Datenschutz und KI

Implementierung von KI-Anwendungen

- **Risikoanalyse**
  - Im Rahmen der Informationssicherheit ist eine Risikoanalyse durchzuführen.
  - Vor der Verarbeitung von personenbezogenen Daten ist eine generelle Bewertung hinsichtlich der Art, des Umfangs, des Zwecks und der Umstände der Verarbeitung vorzunehmen.
  - Prüfen auf Integrität, Vertraulichkeit, Verfügbarkeit und Belastbarkeit (CIA).

- **Datenschutz-Folgenabschätzung (DSFA)**
  - Wird bei der Risikoanalyse festgestellt, dass voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht, muss eine DSFA gem. Art. 35 DSGVO durchgeführt werden.
  - Sofern die KI-Anwendung durch einen Anbieter bereitgestellt wird, ist der Verantwortliche hier auf die Informationen des Anbieters zur Funktionsweise der KI-Anwendung angewiesen.

4 Risiken kennen

RISIKOMANAGEMENT

Was kann schon schiefgehen?

1. Die Cloud-KI

Szenario: **Nutzung von Cloud-KI-Services ohne angemessene Verträge** ***Risiko:*** **Drittlandtransfers, fehlende Auftragsverarbeitung** ***Bußgeldrisiko:*** **Hoch (2-4% Jahresumsatz)**

2. Trainingsdaten

Szenario: **KI wird mit personenbezogenen Daten ohne Rechtsgrundlage trainiert** ***Risiko:*** **Zweckentfremdung, fehlende Einwilligung** ***Bußgeldrisiko:*** **Mittel bis hoch**

3. Bias

Szenario: **KI diskriminiert bestimmte Personengruppen** ***Risiko:*** **AGG-Verstöße, Reputationsschäden, Klagen** ***Bußgeldrisiko:*** **Mittel + Schadensersatz**

4. Transparenz

Szenario: **Betroffene werden nicht über KI-Nutzung informiert** ***Risiko:*** **Informationspflichtverstöße** ***Bußgeldrisiko:*** **Niedrig bis mittel**

5. Das Auskunftsrecht

Szenario: **Unternehmen können Auskunft über KI-Entscheidungen nicht erteilen** ***Risiko:*** **Betroffenenrechtsverstöße** ***Bußgeldrisiko:*** **Niedrig bis mittel**

Szenario A – Support-LLM im Browser

Support

Kontext: Das Customer-Service-Team kopiert Support-Tickets in ein öffentliches Chat-LLM, um schneller Antwortvorlagen zu erzeugen.

Daten: Kundennamen, E-Mail-Adressen, Bestell-/Seriennummern, Fehlerbeschreibungen; gelegentlich sensible Hinweise (z. B. Gesundheitsbezug im Garantiefall).

Technik/Setup: Web-Zugriff über Standardbrowser; kein Unternehmensaccount; keine AV-Verträge; Prompt-/Output-Logs beim Anbieter.

Standort/Transfer: Rechenzentren außerhalb des EWR möglich; unklare Trainingsnutzung der Eingaben.

Wirkung: Texte fließen (teilweise ungeprüft) in Kundenkommunikation zurück; keine formale Freigabe durch IT/DSB

Szenario B – Eingangsrechnungs-OCR

OCR

Kontext: Team nutzt eine integrierte OCR-SaaS zur Belegerkennung und Vorkontierung in Infor.

Daten: Lieferantenstammdaten (Name, Kontakt), Rechnungsnummern, Beträge, IBAN, USt-ID.

Technik/Setup: EU-Cloud; Business-Plan mit AV-Vertrag; Modelle laut Anbieter mit synthetischen/öffentlichen Daten trainiert; Human-in-the-loop prüft jeden Buchungsvorschlag.

Standort/Transfer: Verarbeitung ausschließlich im EWR; Subprozessoren benannt; Log-Speicherung 12 Monate.

Wirkung: Vorschläge beschleunigen die Buchung, Entscheidung verbleibt beim Menschen.

Szenario C – Bewerber-Ranking & Video-Screening

HR

Kontext: HR setzt ein KI-Tool zur Vorselektion ein: Lebensläufe werden gerankt; zusätzlich analysiert ein Modul kurze Videoantworten. Bottom-30 % werden automatisch abgelehnt.

Daten: Bewerbungsunterlagen (CV, Zeugnisse), Metadaten, ggf. Social-Media-Profile; Video-Clips.

Technik/Setup: Externer Anbieter (Black-Box-Modell); unklare Trainingsdaten; keine interne Dokumentation zur Modelllogik; automatisierte Ablehnung ohne verpflichtende HR-Gegenprüfung.

Standort/Transfer: Anbieter mit globaler Infrastruktur; Vertragswerk liegt im Standard vor; keine spezifische Risikoanalyse.

Wirkung: Automatisierte Vorauswahl mit unmittelbarer Wirkung auf Bewerberchancen; Video-Modul enthält „Emotion/Engagement-Erkennung“.

Risikomanagement

Beispiel Microsoft CoPilot

Grundsatz

Die beabsichtigten Verarbeitungen sind zu identifizieren, damit ebenfalls die Daten, die verarbeitet werden sollen -> CoPilot ist nur ein Mittel der Verarbeitung.

CoPilot dient als (KI-)Assistenz und ist in der Microsoft 365-Suite integriert. Es nutzt hierfür diverse große Sprachmodelle (LLMs).

Es werden dabei nicht nur vortrainierte Modelle (z.B. GPT) genutzt, sondern auch „E-Mails, Chats und Dokumente, für die Benutzer über Zugriffsberechtigungen verfügen.“

Vorteil

Copilot kann direkt auf die in Microsoft 365 gespeicherten Daten eines Unternehmens zugreifen und Antworten liefern, die genau auf das Unternehmen zugeschnitten sind.

Risikomanagement

Beispiel Microsoft CoPilot

Nachteil

Copilot kann direkt auf die in Microsoft 365 gespeicherten Daten eines Unternehmens zugreifen und Antworten liefern, die genau auf das Unternehmen zugeschnitten sind.

Der Datenzugriff erfolgt ohne eigenes Zutun, d.h. die Daten sind teil der Verarbeitung, sobald die entsprechende Berechtigung besteht. Der Nutzer muss selbst keine pbD hochladen.

Es besteht die Gefahr, dass pbD unrechtmäßig verarbeitet und ungewollt verteilt werden. Eine Eingabe im Suchfeld reicht aus.

Risikomanagement

Beispiel Microsoft CoPilot

Empfohlene Maßnahmen

- Identifizieren und Klassifizieren von Informationen.

  Im Rahmen der Klassifizierung werden Dokumente und Informationen in den Dokumenten eingeordnet, je nachdem ob die Information öffentlich, intern, vertraulich oder streng vertraulich ist. Auch der Speicherort wird identifiziert.

- Überprüfen der Rollen und Berechtigungen für den Zugriff der jeweiligen Information.

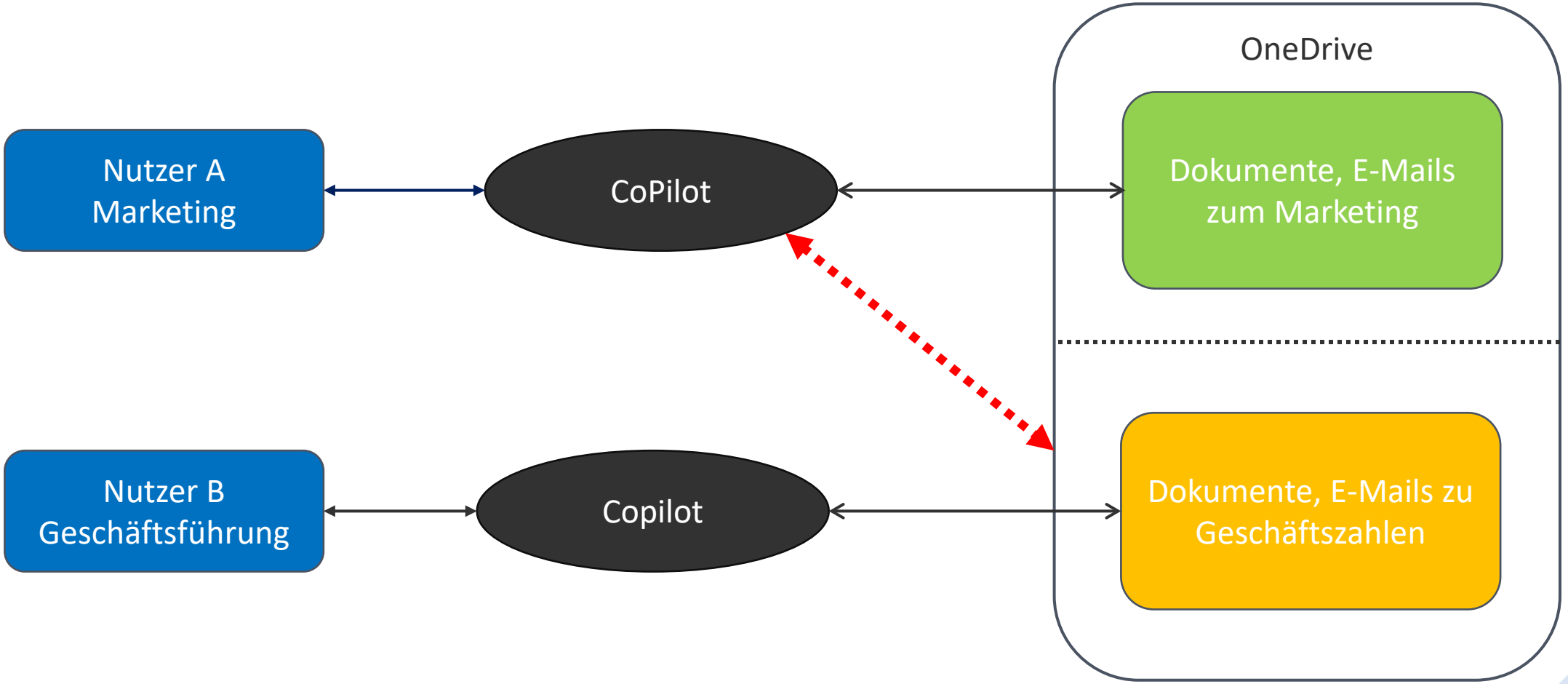
  Folgende Accounttypen sind auszuschließen von Abfragen an CoPilot:

  - Accounts mit Adminrechten
  - Sammelaccounts/Funktionsaccounts

- Risikoanalyse
- Umsetzung der Klassifizierung in Richtlinien und Label

Risikomanagement

Beispiel Microsoft CoPilot



Problemfelder der KI

Lernen ohne Verstehen

Vorurteilsbehaftete Trainingsdaten:
KI-Modelle lernen aus Daten, die gesellschaftliche Vorurteile oder Diskriminierung widerspiegeln können (Historische Daten zur Kreditvergabe, die Frauen oder ethnische Minderheiten benachteiligt haben).

Fehlerhafte Datenrepräsentation:
Wenn bestimmte Gruppen in den Trainingsdaten unterrepräsentiert sind, führt dies zu schlechteren Leistungen des Modells für diese Gruppen (Gesichtserkennungstechnologien, die mit Bildern von hellhäutigen Personen trainiert werden und dunklere Hautfarben schlechter erkennen).

Algorithmische Verzerrungen:
Die mathematischen Modelle selbst können Vorurteile verstärken, wenn sie ungleichmäßige Verteilungen in den Daten nicht korrekt behandeln (Ein KI-System priorisiert Datenpunkte, die häufiger vorkommen, und ignoriert seltene Fälle).

Problemfelder der KI

Lernen ohne Verstehen

5 Haftung und Künstliche Intelligenz

Haftung und Künstliche Intelligenz

aktuell

Haftung nach dem Bürgerlichen Gesetzbuch (BGB):

• Verwenderhaftung: Unternehmen, die KI-generierte Inhalte nutzen, haften für diese Inhalte. Die KI selbst besitzt keine Rechtspersönlichkeit und kann daher nicht haftbar gemacht werden.

• Herstellerhaftung: Eine Haftung des Herstellers kommt in Betracht, wenn die KI nicht die vertraglich zugesicherte Beschaffenheit aufweist oder unzureichende Sicherheitsvorkehrungen getroffen wurden, die zu Schäden führen.

Haftung nach dem Produkthaftungsgesetz (ProdHaftG):

• Derzeit ist unklar, ob KI-Systeme als "Produkte" im Sinne des ProdHaftG gelten. In der Regel wird angenommen, dass für KI keine Haftung nach dem ProdHaftG besteht.

Haftung und Künstliche Intelligenz

Ausblick

Novelle der Produkthaftungsrichtlinie (ProdHaftRL)

Im Oktober 2024 wurde die neue Produkthaftungsrichtlinie verabschiedet. Die Veröffentlichung erfolgte am 18.11.2024. Mitgliedstaaten haben 24 Monate Zeit, diese in nationales Recht umzusetzen.

1. Software als Produkt

Art. 4 Nr. 1 unter „Produkt“ sind auch Elektrizität, digitale Konstruktionsunterlagen, Rohstoffe und **Software** zu verstehen

2. Beweislastumkehr

Art. 9 Nr. 1 der Beklagte verpflichtet ist, unter den in diesem Artikel festgelegten Bedingungen in der Verfügungsgewalt des Beklagten befindliche relevante Beweismittel offenzulegen.

Art. 10 Fehlerhaftigkeit wird vermutet: Der Beklagte unterlässt es, relevante Beweismittel nach Artikel 9 Absatz 1 offenzulegen.

Haftung und Künstliche Intelligenz

Ausblick

Entwurf der KI-Haftungsrichtlinie (September 2022)

- Offenlegungspflicht für Anbieter von Hochrisiko-KI-Systemen (soll dem Phänomen der „Black Box“ bei künstlicher Intelligenz begegnen)
- widerlegliche Kausalitätsvermutung für KI-induzierte Personen- und Sachschäden (Verstoß z.B. gegen KI-VO führt zur Vermutung dessen Kausalität für Schaden)

Studie September 2024

- Die erfassten KI-Systeme sollten laut der Studie präziser und in enger Abstimmung mit der KI-Verordnung definiert werden. Hierzu schlägt die Studie unter anderem vor, neben KI-Systemen auch KI-Modelle mit allgemeinem Verwendungszweck (z.B. GPT-4 von OpenAI) explizit in die KI-Haftungsrichtlinie einzubeziehen.

6 Best Practices

Best Practices für KI-Projekte

So gelingt die Einführung rechtssicher und effizient

COMPLIANCE-ROADMAP

SO MACHEN SIE ES RICHTIG

✅ **1. Datenschutz-Folgenabschätzung (DSFA)**

Praxistipp: **Nutzen Sie die Liste der Datenschutzkonferenz als Orientierung**

✅ **2. Rechtsgrundlage definieren**

Praxistipp: **Dokumentieren Sie die Interessenabwägung ausführlich**

✅ **3. Datenminimierung umsetzen**

Grundsatz: **Nur so viele Daten wie nötig** ***Praxistipp:*** **Anonymisierung/Pseudonymisierung wo möglich**

✅ **4. Transparenz schaffen**

Praxistipp: **Erstellen Sie verständliche "KI-Hinweise" für Betroffene**

✅ **5. Technische Schutzmaßnahmen**

✅ **6. Organisatorische Maßnahmen**

✅ **7. Vertragsmanagement**

✅ **8. Monitoring und Dokumentation**

Takeaways

- **KI und Datenschutz sind kein Widerspruch** - mit der richtigen Herangehensweise
- **Compliance zahlt sich aus** - präventive Maßnahmen sind günstiger als Bußgelder
- **Der AI Act bringt neue Pflichten** - bereiten Sie sich jetzt vor
- **Transparenz schafft Vertrauen** - informieren Sie Ihre Stakeholder proaktiv
- **Kontinuierliche Weiterentwicklung** - KI-Compliance ist ein Prozess, kein Projekt

Noch Fragen?

SACHVERSTÄNDIGENBÜRO MÜLOT GMBH

Datenschutz | Datensicherheit | Forensische Informatik

Risikomanagement | ISO27001

Grüner Weg 80
48268 Greven

Tel.: 02571/5402 0
info@svb-muelot.de

www.svb-muelot.de