VIDEO

Nachricht von Ella | Without Consent



VIDEO

Fazit aus Ellas Nachricht

Identitätsdiebstahl
Deepfakes
Verletzte Persönlichkeitsrechte

= Schadenspotenzial für Personen

Wie wirken wir dagegen?

Datenschutz

Wie verwenden wir KI ohne den Datenschutz zu vernachlässigen?





machCon

REFERENT

Christian Herbst

machCon GmbH

IT & Compliance

Smart. Effizient. Sicher.



Übersicht Situation

Datenschutzkonforme Nutzung von KI

ÜBERBLICK

Künstliche Intelligenz

KI =

zukunftsweisende Technologie

- Logisches Denken
- Lernen
- Planen
- Kreativität

Machine Learning (Teil der KI)

- Erkennt Zusammenhänge zwischen Daten
- Generiert neue Ergebnisse



ÜBERBLICK

Künstliche Intelligenz

CHANCEN

- Automatisierung
- Effizienzsteigerung
- Geringerer Personalbedarf / Personalkosten
- Geringere Prozesskosten
- Kostenreduktion
- Vorhersagen von Trends und Entwicklungen
- Globale Zusammenarbeit durch die Eliminierung von Sprachbarrieren
- Innovation und Produktentwicklung durch Markttrend-Analysen und Brainstorming
- Wettbewerbsvorteil durch die schnellere Entwicklung von innovativen Lösungen und günstigere Preise durch die Weitergabe der Kosteneinsparungen

RISIKEN

- Arbeitsplatzverluste
- Hohe Investitionen (Technologie, Schulungen, Infrastruktur)
- Abhängigkeit von Technologie
- Image-Schäden durch falsche Entscheidungen der KI
- Finanzielle Schäden durch falsche Entscheidungen der KI
- Risiko das Anti-Diskriminierungs-Gesetz zu verletzen
- Risiko die DSGVO-Richtlinien zu verletzen

ÜBERBLICK

Urheberrechtliche Grundlagen / Unklare Rechtslage

WER IST DER URHEBER DER KI-GENERIERTEN WERKE?

Das generierte Werk könnte dem geschützten Original ähneln und dem KI-Anwender unbeabsichtigte Konsequenzen bringen.

Derzeit eine Grauzone.

KÖNNEN KI-GENERIERTE WERKE URHEBERRECHTLICH GESCHÜTZT WERDEN?

Das Urheberrecht soll nur menschliche Werke schützen, was die Herausforderung bei KI-generierten Werken darstellt.

Erstellung menschlich + maschinell könnte es urheberrechtlich geschützt werden.

KANN DIE KI SELBST URHEBER DES GENERIERTEN WERKS SEIN?

Grundsätzlich Nein.

AGBs der KI-Anbieter:

- Kommerzielle Nutzung der Werke oft erlaubt
- Urheberrechtliche Prüfung durch den Anwender

Klagen gegen ausländische KI-Anbieter sind schwierig und gerichtlich zu entscheiden.

WIE KÖNNEN KI-GENERIERTE WERKE GENUTZT WERDEN?

Prüfen der generierten Werke auf Urheberrechtsverletzungen

Normalerweise unbedenklich:

Emails, Gebrauchstexte, Eventsabläufe, interne Anweisungen

ÜBERBLICK

Urheberrechtliche Grundlagen

WER HAFTET, SOLLTE EIN URHEBERRECHT DURCH DIE NUTZUNG VON KI-GENERIERTEN INHALTEN VERLETZT WERDEN?

Der Nutzer.

Gerichtsentscheidungen können zu hohen Kosten für den Nutzer führen, ebenso eine potenzielle Rückrufaktion und Schadenersatz.

WIE SIEHT DIE ZUKÜNFTIGE RECHTSLAGE AUS?

Einführung des EU-"AI Act", um bisherige Grauzonen zu klären.

Für KI-Anbieter gilt:

- Über Verwendung von urheberrechtlich geschützten Trainingsdaten informieren
- Verbot des Generierens rechtswidriger Inhalte

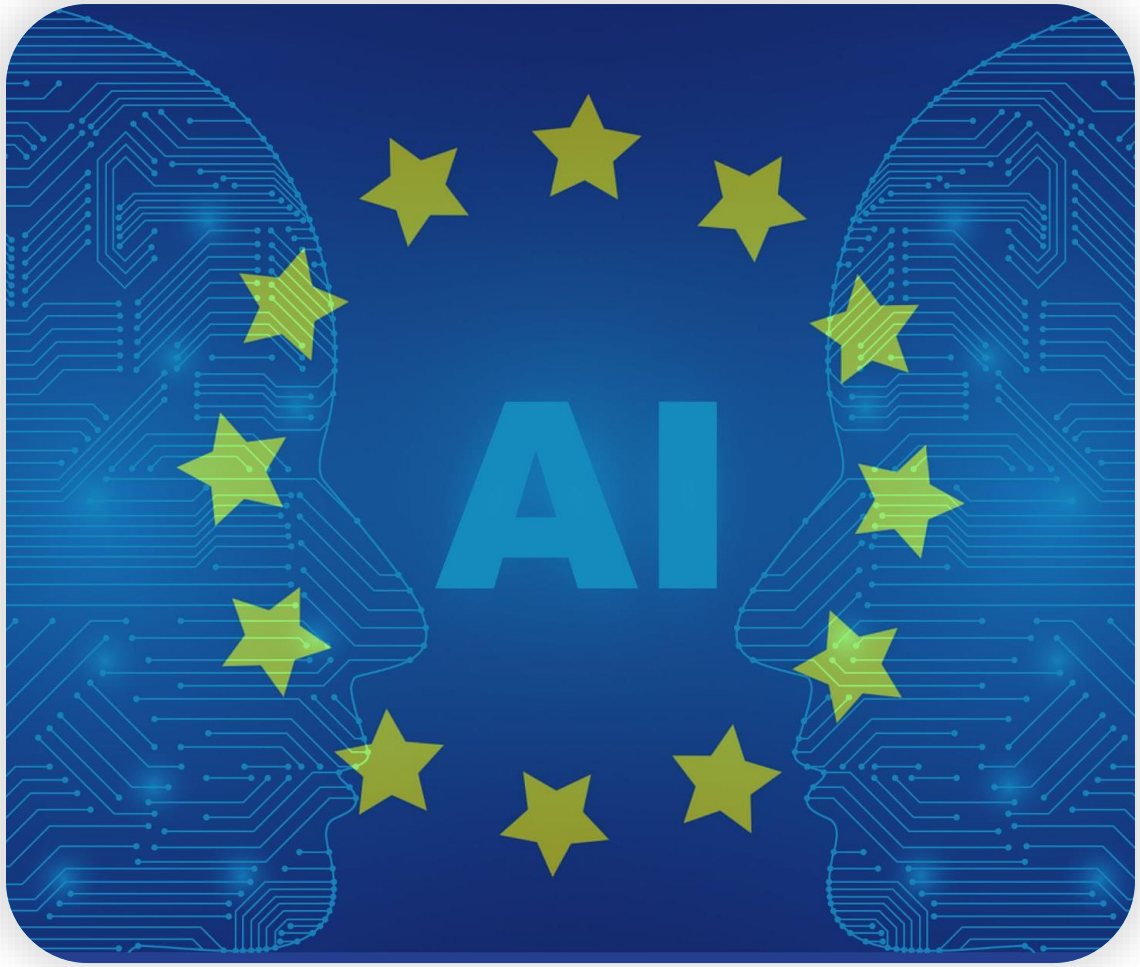


FRISCH VOM EUROPÄISCHEN PARLAMENT VERABSCHIEDET

Der europäische AI Act (KI-Verordnung)

ANBIETER, EINFÜHRER, HÄNDLER UND BETREIBER VON KI-SYSTEMEN MÜSSEN DIVERSE AUFLAGEN ERFÜLLEN:

- Der AI Act verfolgt einen risikobasierten Ansatz
- KI-Systeme werden nach ihrem Risiko bewertet/reguliert
  - unannehmbares Risiko (verbotene KI-Praktiken)
    - Social Scoring & kognitive Verhaltensmanipulation
  - hohes Risiko (Hochrisiko-KI-Systeme)
    - KRITIS Verwaltung & Kreditwürdigkeitsprüfung
  - begrenztes Risiko (KI-Systeme, die für die Interaktion mit natürlichen Personen bestimmt sind)
  - minimales und/oder kein Risiko (alle anderen KI-Systeme)
- Es werden empfindliche Bußgelder für Verstöße gegen die Regelungen bzgl. verbotener KI-Praktiken verhängt
- Ausnahmen im Geltungsbereich bestehen (beispielsweise nationale Sicherheit / militärische Verteidigung)



ÜBERBLICK

Datenschutzproblematik bei der Nutzung von KI

WEITERGABE VON PERSONENBEZOGENEN DATEN AN KI

Die Weitergabe von personenbezogenen Daten erfolgt…

… beim Eingeben von Prompts ohne Anonymisierung

… beim Hochladen von Dateien, die personenbezogene Daten beinhalten

Achtung!

Eingegebene/hochgeladene Daten könnten zu Trainingsdaten werden.

=>> Risiko der Weitergabe der Daten an Dritte besteht.

Das ist ein Datenschutzverstoß!



ÜBERBLICK

Datenschutzproblematik bei der Nutzung von KI

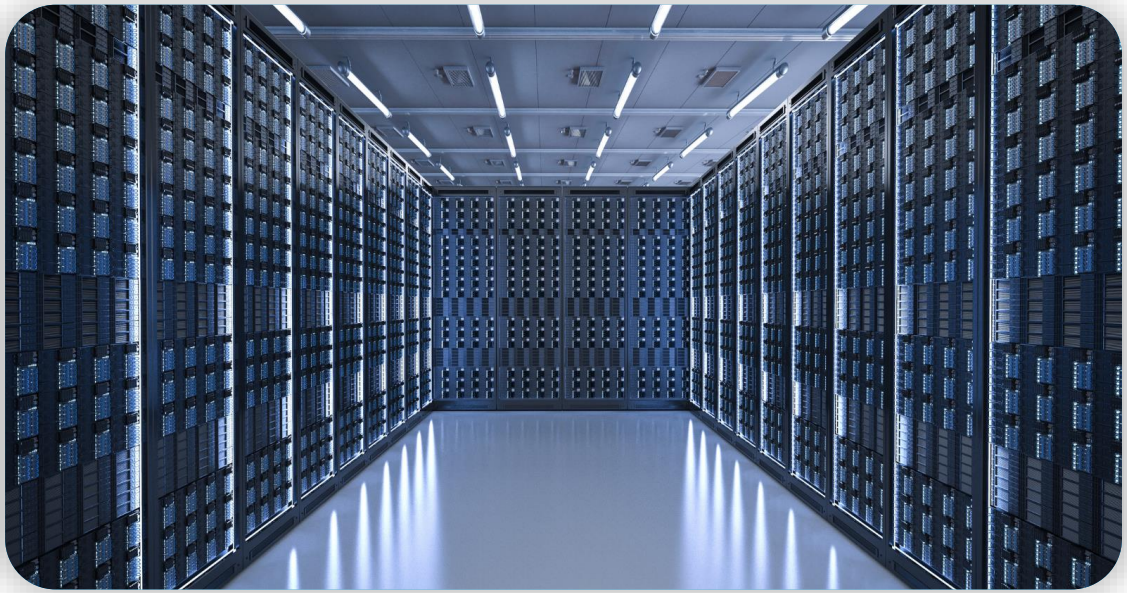
GOOGLE HOME UND AMAZON ECHO

Google Home und Amazon Echo können Gespräche ohne Aufforderung aufzeichnen.

- Schwierigkeiten bei Datenschutzfolgenabschätzungen aufgrund vieler Einflussfaktoren
- Unnachvollziehbare Entscheidungen durch den Algorithmus

SERVER IN DEN USA

Problematisch, da die Datenschutzrichtlinien dort lockerer sind



REGELUNGEN

DSGVO muss eingehalten werden!
Verstöße:
Es drohen hohe Geldstrafen bis zu 20 Millionen Euro oder 4% des weltweiten Umsatzes eines Unternehmens / Konzerns

CHECKLISTE

Datenschutzkonforme Nutzung von KI

Beispielsweise bei Large Language Models (Chat GPT)

- Sicherstellung einer rechtmäßigen Verarbeitung der Daten/Ergebnisse
- Daten nur anonymisiert eingeben
- Abschließen eines Auftragsverarbeitungsvertrags mit dem KI-Anbieter
- Überprüfen von Umformulierung der generierten Texte
- Datenschutzfolgenabschätzung (DSFA) & Transfer Impact Assessment (TIA)
- Richtlinien zur Nutzung von LLMs im Arbeitsvertrag oder einer Verpflichtungserklärung
- Ergänzung Datenschutzerklärung & Verzeichnis für Verarbeitungstätigkeiten (VVT)
- Beachtung der Informationspflichten aus Art. 13 & 14 DSGVO
- Protokollierung eingegebener Daten
- Vermeiden eines Einsatzes von vollautomatischen Entscheidungen basierend auf KI



ÜBERBLICK

Datenschutz bei Machine Learning

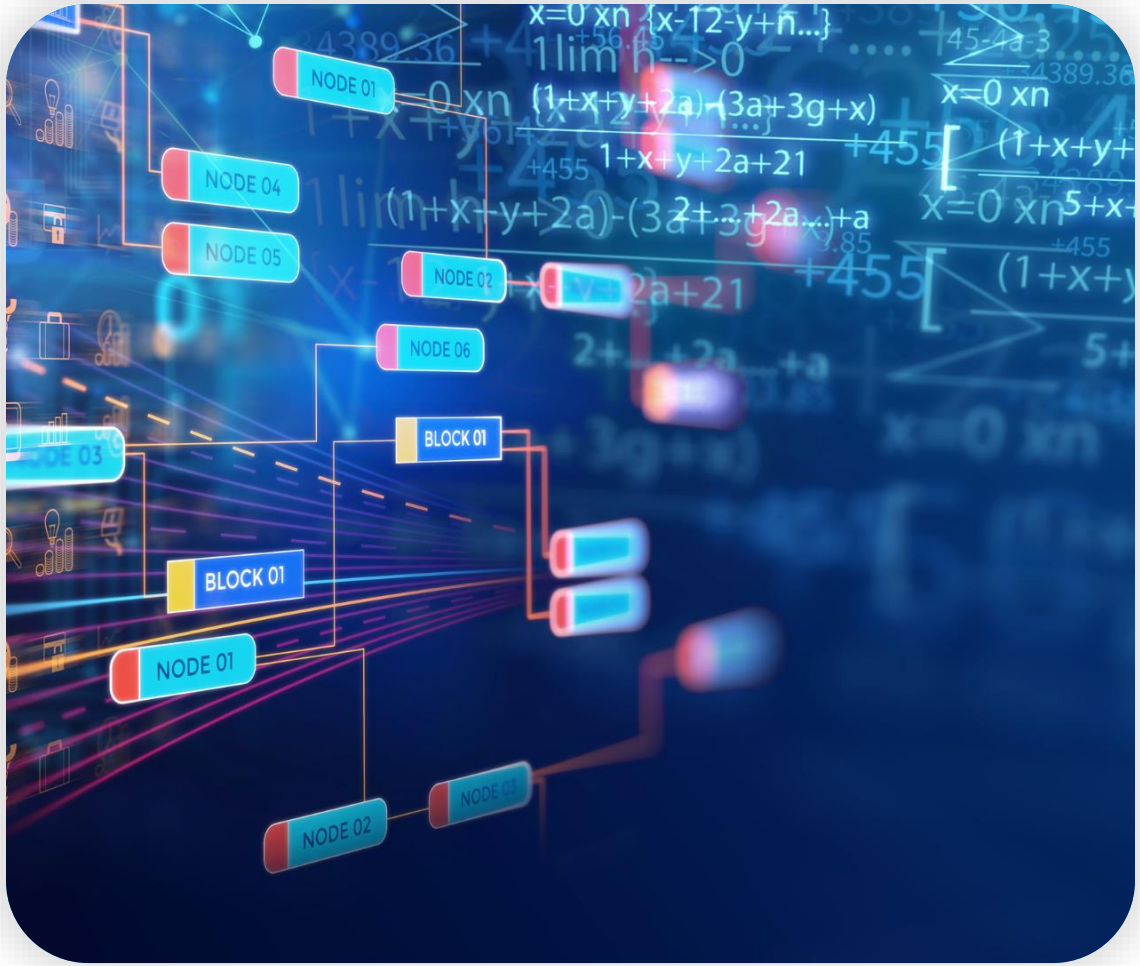
WEITERGABE VON DATEN AN EIN MACHINE LEARNING MODELL

Machine Learning ist eine Unterkategorie von KI.

= Lernen aus eigenen Ergebnissen und neuen Trainingsdaten.

- Vertrauenswürdiger Umgang muss für KI-Anbieter und Anwender gegeben sein, sollte mit nicht anonymisierten Daten gearbeitet werden

- Daten müssen vertraulich, integritätsgeschützt und verfügbar sein, und Datenschutzrichtlinien sind einzuhalten.



ÜBERBLICK

Datenschutz bei Machine Learning

CROWDSOURCING

- Google Maps zeigt Verkehrsprobleme an, indem es Standortdaten und Bewegungen erfasst
- Crowdsourcing ist datenschutzrechtlich für die Erkennung von Datenlecks und Risikoanalysen unbedenklich

- **Problematik:** Anwendung trifft eigenständige Entscheidungen und verwendet Daten für mehrere Zwecke
- Neue Verwendungszwecke müssen mit dem ursprünglichen Grund übereinstimmen

DIE MENSCHENWÜRDE

Um die Menschenwürde zu schützen, müssen wichtige Entscheidungen von Menschen und nicht von einer KI getroffen werden (Art. 22 DSGVO)



ÜBERBLICK

OpenAI API vs. Microsoft

OpenAI API = Chat GPT

- Behauptung: Sensible Daten ≠ Trainingsdaten
- Abuse Monotoring = Datenspeicherung für 30 Tage
- Deaktivierung der Datenspeicherung NICHT möglich!
- Mögliche EU-Sanktionen wegen vermuteter Verwendung personenbezogener Daten aus dem Internet
- Serverstandort: USA
- „Innovativer“

MICROSOFT

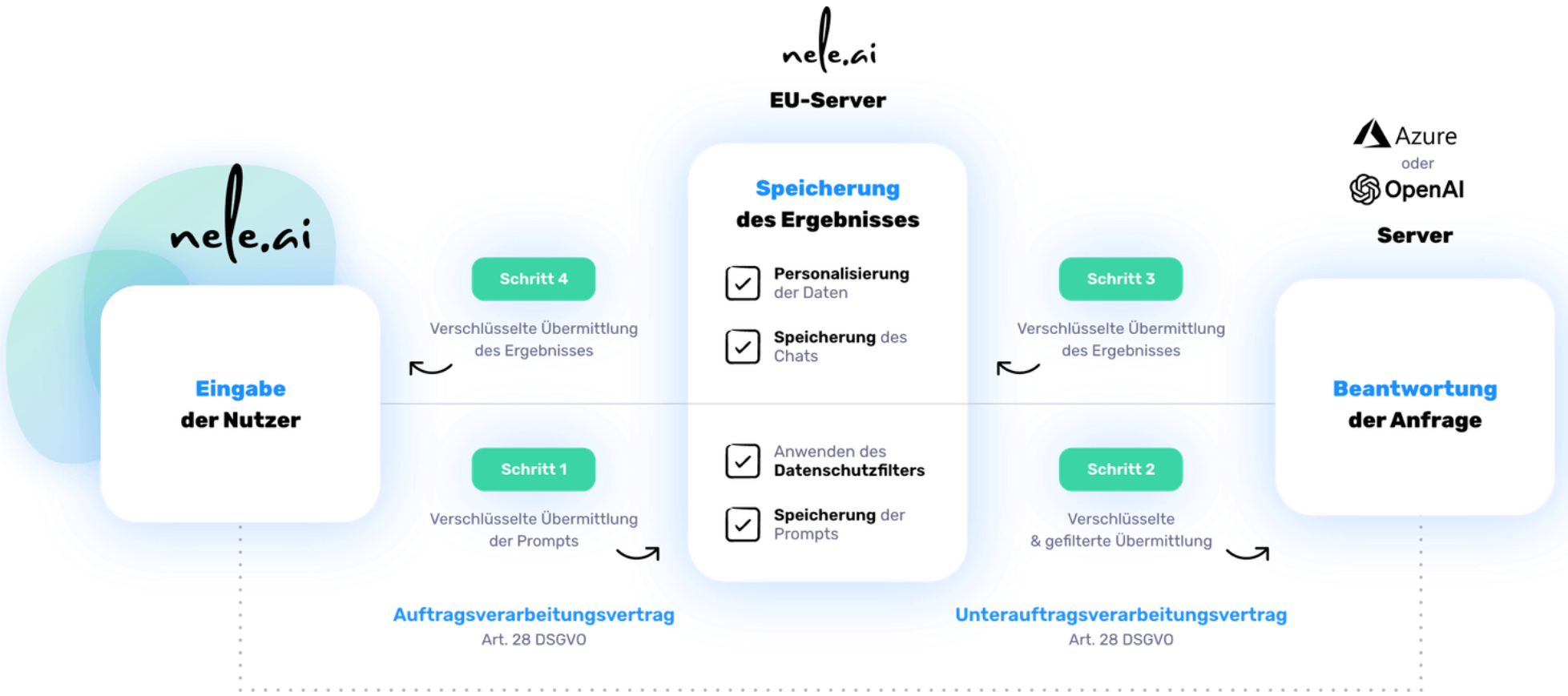
- Behauptung: Sensible Daten ≠ Trainingsdaten
- Abuse Monotoring = Datenspeicherung für 30 Tage
- Deaktivierung der Datenspeicherung nur durch eine genehmigte Sonderanfrage möglich!
- Serverstandort: USA und EU
- „Datenschutzkonformer“

DATENSCHUTZKONFORME ALTERNATIVE: Nele.AI

Nele.AI gibt anonymisierte Daten in ChatGPT und Azure ein. = Optimiert und Unterstützt unter Einhaltung der Datensicherheit, Sensibilisierung und Anonymisierung.

Nele.AI Serverstandort = DE = Beachtung der DSGVO!

Rechtssichere & datenschutzkonforme Plattform „nele.ai“ ermöglicht Paradigmenwechsel



- Sichere und datenschutzkonforme Anwendung
- Sensible Unternehmensdaten werden nicht in der KI gespeichert
- Sparen Sie Zeit bei Ihren täglichen Aufgaben
- Mitarbeiter können KI einfach anwenden
- Nutzen und verwalten Sie eigene Prompts
- Über 200 Prompts für die sofortige Nutzung
- Eine Abrechnung pro Team
- Zahlung per Lastschrift oder Kreditkarte
- KI-Volumen nach Ihrem Bedarf monatlich frei wählbar

VERANTWORTLICHKEITEN

Mögliche Konstellationen von datenschutzrechtlichen Verantwortlichkeiten für die Verarbeitungsprozesse

Alleinverantwortung des KI-Anbieters

Auftragsverarbeitung

Gemeinsame Verantwortlichkeit



Verantwortlichkeit hängt vom Anbieter, Modell Einsatzgebiet ab.

VERANTWORTLICHKEITEN

Was ist zu beachten?

- Klärung der Verantwortung mit dem Anbieter schriftlich (AGBs / Vertrag)
- ChatGPT = Auftragsverarbeiter
- Es ist noch unklar, ob der AVV rechtlich ausreicht
- Modell mit AVV ist sicherer als ohne AVV

IM FALLE EINER DATENSCHUTZVERLETZUNG

- Eingabe nicht anonymisierter personenbezogener Daten in KI-Modellen erfordert Benachrichtigung der Betroffenen
- Einwilligung des Kunden kann nach dem Auftragsverarbeitungsvertrag erforderlich sein
- Datenschutzverletzungen unterliegen der DSGVO und können zu hohen Bußgeldern führen: bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes



FRAGEN & ANTWORTEN

Gibt es noch offene Punkte oder Rückfragen?

STELLEN SIE JETZT IHRE FRAGE

Alternativ haben wir sicherlich im Laufe der Veranstaltung / Pausen noch Zeit für einen Austausch.



SCHLUSSWORT

Herzlichen Dank für Ihre Aufmerksamkeit

VIEL ERFOLG BEI DER UMSETZUNG

Wir hoffen, Ihnen hiermit einen groben Überblick über das aktuelle Spannungsfeld Datenschutz & KI gegeben zu haben.

Wir wünschen Ihnen viel Erfolg bei der Umsetzung Ihrer KI-Initiativen.

