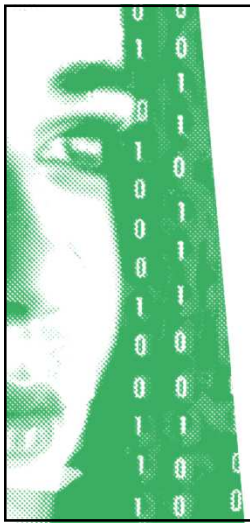
2024 CAMPUS TAGE

# KI trifft auf Datenschutz Digitalstrategien



DSN Akademie

## Künstliche Intelligenz – datenschutzkonform gestalten

**Dr. Uwe Schläger, Geschäftsführer DSN Holding GmbH**

**www.dsn-group.de**

## Agenda

DSN GROUP

1. Große Sprachmodelle und KI-Anwendungen
2. Rechtsgrundlagen von KI-Anwendungen
3. Training von KI-Systemen und -Modellen
4. Auftragsverarbeitung / gemeins. Verantwortung
5. Umsetzung von Betroffenenrechten
6. Automatisierte Einzelfallentscheidungen
7. AI Act als komplexes Regelwerk
8. KI-Strategie / KI-Richtlinie

## Definition von KI-Systemen

DSN GROUP

„KI-Systeme grenzen sich von Systemen ab, „die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen. **Ein wesentliches Merkmal von KI-Systemen ist ihre Fähigkeit, abzuleiten.** Diese Fähigkeit bezieht sich auf den Prozess der Erzeugung von Ausgaben, wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen … sowie auf die Fähigkeit von KI-Systemen, Modelle oder Algorithmen oder beides aus Eingaben oder Daten abzuleiten. Zu den Techniken, die während der Gestaltung eines KI-Systems das Ableiten ermöglichen, gehören Ansätze für maschinelles Lernen … sowie logik- und wissensgestützte Konzepte … **Die Fähigkeit eines KI-Systems, abzuleiten, geht über die einfache Datenverarbeitung hinaus, indem Lern-, Schlussfolgerungs- und Modellierungsprozesse ermöglicht werden**."

Erwägungsgrund 12 AI Act

## Große Sprachmodelle

Große Sprachmodelle (LLM) verwenden **tiefgreifende Lernmodelle**, die mit großen Datenmengen trainiert werden, und lernen hierdurch Muster und Verbindungen (Parameter) zwischen Wörtern und Phrasen.

Anzahl der Parameter bekannter Sprachmodelle:
- GPT-4: 1 Billion Parameter
- LLaMA 3: 70 Milliarden Parameter
- Gemini: 1,6 Billionen Parameter

Große Sprachmodelle (LLM) arbeiten nicht **deterministisch**, sondern **heuristisch**, d.h. auf eine Anfrage wird ein Satz generiert, der mit hoher Wahrscheinlichkeit die Anfrage am besten beantwortet.

## Große Sprachmodelle – Anwendungen

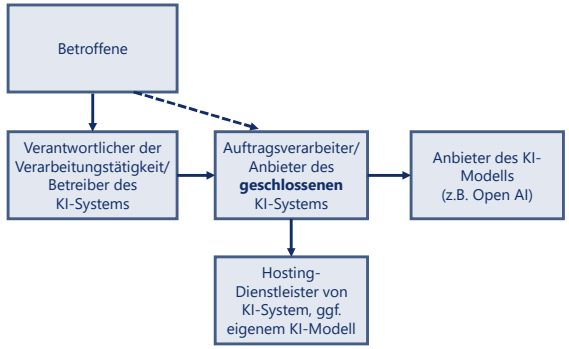
Anwendungsmöglichkeiten von LLM in Unternehmen:
- Texterstellung, Übersetzung von Texten
- Marketing: Bildgenerierung statt Stockfotos
- Authentisierung per biometrischer Gesichtserkennung
- Code-Generierung/Programmierung
- **Bewerberauswahl**
- Unternehmensinternes Wissensmanagement
- Gesundheitswesen: Diagnostik, Befundung, Bilderkennung, Berichterstellung
- Call-Center: Stimmungsanalyse von Kunden

## KI-basierte Bewerberauswahl

„Die KI-Technologie ermöglicht es, Bewerbungen objektiv anhand vordefinierter Kriterien zu bewerten und diejenigen herauszufiltern, die am besten zu den Anforderungen der Stelle passen. Dadurch wird die menschliche Voreingenommenheit minimiert und eine fairere Bewerberauswahl gewährleistet." (Rocken Jobs)

„Die Künstliche Intelligenz in der Personalabteilung durchforstet Lebensläufe und analysiert Videodaten. Sie findet den Perfect Fit und zieht Rückschlüsse auf die Persönlichkeit der Bewerber." (Computerwoche)

## Akteure von KI-Systemen (DSGVO, AI Act)




## Rechtmäßigkeit von KI-Anwendungen

Als Rechtsgrundlage der Datenverarbeitung kommen in Betracht:

- **Vertrag** mit Betroffenem
- **Einwilligung** des Betroffenen
- **Berechtigtes Interesse** des Verantwortlichen der KI-Anwendung keine ausreichende Rechtsgrundlage, da schutzwürdige Interessen des Betroffenen dem in aller Regel entgegenstehen

Problem: **Zweckbindung** lässt sich schwer garantieren!

Art. 6 Abs. 1 DSGVO

## Training von KI-Systemen/KI-Modellen

Sofern das Training von KI-Systemen mit personenbezogenen Daten oder pseudonymisierten Daten erfolgt, liegt eine **zweckfremde** Nutzung der Daten vor, für die eine separate Rechtsgrundlage vorliegen muss.

Das Training mit pseudonymisierten Daten kann rechtskonform über eine **Einwilligung** des Betroffenen erfolgen, die auch vergütet werden kann.

Einwilligungslösung **praxistauglich**, da für das Training bereits 10 % der Datensätze ausreichen.

Sofern keine Rechtsgrundlage existiert, sollte das Training mit **anonymisierten** Daten erfolgen.

## LLM-Betreiber: Auftragsverarbeiter oder gemeinsam Verantwortlicher ?

Sofern KI-Systeme und KI-Modelle mit personenbezogenen Daten optimiert werden, verarbeitet der Anbieter des KI-Systems bzw. des KI-Modells die Daten zu eigenen Zwecken und ist damit **Verantwortlicher**.

Anstelle eines AV-Vertrags muss mit dem Anbieter des KI-Systems bzw. KI-Modells ein Joint-Controller-Vertrag geschlossen werden.

Art. 26, 28 DSGVO

## Umsetzung von Betroffenenrechten

Betroffenenrechte, insbesondere **Auskunftsrechte**, das Recht auf Berichtigung unrichtiger Daten oder das Recht auf Datenlöschung können kaum umgesetzt werden.

Diese Rechte können kaum gegenüber dem **Anbieter** des KI-Systems geltend gemacht werden, da dieser hierzu einfach nicht in der Lage ist.

Auch bei gemeinsamer Verantwortung können Betroffene kaum erkennen, dass ihre Daten durch den Anbieter des KI-Modells inkorrekt verarbeitet werden und wie eine **Berichtigung der Daten** durchgesetzt werden kann.

Gleiches gilt für **Informationspflichten** gemäß Art. 13/14 des Verantwortlichen.

Art. 12 - 23 DSGVO

## Automatisierte Einzelfallentscheidungen

Art. 22 DSGVO

Gemäß Art. 22 DSGVO haben Betroffene das Recht, nicht ausschließlich einer Entscheidung unterworfen zu werden, die auf einer automatisierten Verarbeitung beruht, die den Betroffenen **erheblich** beeinträchtigt.

Dieses Recht ist beim Einsatz von KI-Systemen nur sehr **schwer umsetzbar** und bedarf einer **Qualitäts-sicherung** der Ergebnisse durch den Verantwortlichen der KI-Anwendung.

## AI Act der Europäischen Union

... wurde im März 2024 im EU-Parlament verabschiedet, am 21.5.2024 vom Rat der EU beschlossen, seit **1.8.2024 in Kraft** getreten.

... muss **innerhalb von 2 Jahren** umgesetzt werden; das Verbot bestimmter Systeme gilt bereits ab 2.2.2025.

... gilt für sämtliche Unternehmen in der EU, die KI **anbieten/entwickeln** oder **betreiben**.

... gilt nicht für den **militärischen** und Forschungsbereich.

Als KI-Aufsichtsbehörde ist **Bundesnetzagentur** geplant.

Bei Nicht-Einhaltung drohen **sehr hohe Bußgelder**.

## AI Act: Wesentliche Inhalte

AI Act schreibt vor, dass KI nicht missbraucht werden darf; **Grundrechte** müssen gewahrt werden.

**Transparenzpflicht**: Künstlich erzeugte Inhalte (Audios, Bilder, Videos) müssen als solche gekennzeichnet werden.

**Verbot** von Social Scoring zur gezielten Beeinflussung von Personen, Verfahren zur biometrischen Kategorisierung.

Zahlreiche Pflichten für Betreiber und Anbieter von **Hochrisiko-KI-Systemen**.

**Schulungspflichten** gelten bereits ab 2. Februar 2025 !

*https://www.datenschutz-notizen.de/category/kuenstliche-intelligenz-ki/*

## IT-Strategie / Vorgehensweise


Ausprobieren und Testen

KI-Kompetenz bei Mitarbeitenden und KI-Projektverantwortlichen stärken.

Intensiv mit AI Act beschäftigen: Hohe Anforderungen an Betreiber und Anbieter von Hochrisiko-KI-Systemen

KI-Richtlinie erstellen

KI-Strategie entwickeln

## Inhalt einer KI-Richtlinie

Dokumentation freigegebener KI-Systeme (Whitelist)

Regeln zur Benutzung freigegebener KI-Systeme, u.a.
- Verbot der Nutzung von Personal-/Gesundheitsdaten
- Verbot der privaten Nutzung
- Transparenzpflicht bei KI-gestützter Generierung von Texten, Bilden und Videos
- Menschliche Überprüfung KI-gestützter Ergebnisse

Blacklist von verbotenen KI-Systemen

elearning-Kurs zur Erlangung einer gewissen Grundkompetenz

## Fazit

AI Act und DSGVO anwendbar

Hohe Anforderungen an Betreiber, Anbieter, Einführer und Händler von Hochrisiko-KI-Systemen

Datenschutzfolgeabschätzung erforderlich bei Hochrisiko-KI-Systemen

Training von LLM-Modellen möglichst mit anonymisierten, zumindest mit pseudonymisierten Daten

KI-Strategie entwickeln, KI-Richtlinie erstellen

## Vielen Dank für Ihre Aufmerksamkeit!

Dr. Uwe Schläger
Geschäftsführer DSN Holding GmbH
uschlaeger@dsn-group.de

**https://www.dsn-group.de/dsn-akademie**