2026 CAMPUS TAGE

DSN GROUP

Von der Schatten-KI zu einer ganzheitlichen KI-Strategie

KI datenschutzkonform und rechtssicher gestalten

DSN GROUP

Dr. Uwe Schläger
Geschäftsführer DSN Holding GmbH

DSN Group
T +49 (0)421 69 66 32 312
E-Mail uschlaeger@dsn-group.de

www.dsn-group.de

Agenda

1. KI als neue Transformationstechnologie
2. Ist-Situation in Unternehmen
3. Anforderungen der DSGVO
4. Eckpfeiler einer ganzheitlichen KI-Strategie
5. Haftung für Betreiber und Anbieter

DSN GROUP

DSN GROUP

1. KI als Transformations-technologie

KI als neue Transformationstechnologie

- KI ersetzt die algorithmische Logik der Informatik
- sehr kurze Innovations- und Entwicklungszyklen
- Entwicklung hat kaum Grenzen - alles ist möglich
- kaum jemand versteht KI-Technologie
- KI ist kaum kontrollierbar – technisch und gesellschaftlich
- KI wird teuer erkauft – enorm hoher Strom- und Wasserverbrauch

- **mangelnde Transparenz**: Wann wird KI eingesetzt?
- **fehlerhafte Ergebnisse**: Wer haftet für falsche Ergebnisse?
- **unkontrolliertes autonomes Handeln**: Wer stoppt KI-basierte Prozesse?
- **ungeklärter Datenschutz**: Umgang mit personenbezogenen Daten?

2. Ist-Situation in Unternehmen

KI-Anwendungen

- **Office-Tätigkeit** (Text- und Folienerstellung, Übersetzungen)
- **Wissensmanagement** (interne und externe Wissensquellen)
- **Personalverwaltung** (Bewerbermanage-ment, Personalplanung und -entwicklung)
- **Kommunikation mit Kunden per Chatbot**
- **Kundenanalyse** (Profiling, Bonitätsbewertung)
- **Marketing, Vertrieb**
- **Videoüberwachung**
- **Software-Entwicklung (Vibe Coding)**

Ist-Situation in vielen Unternehmen

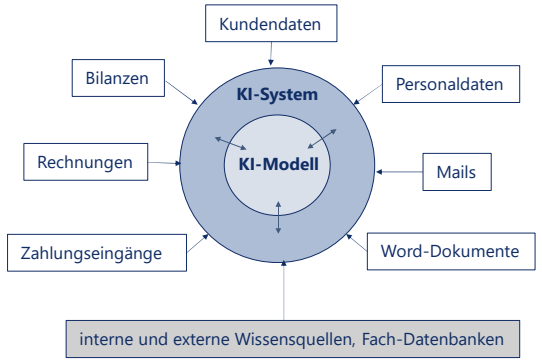
- Datenschutz-Grundverordnung (DSGVO)
- KI-Richtlinie der EU (AI Act)
- § 203 StGB (Ärzte, Anwälte, Steuerberater)
- Haftung gem. BGB (Unternehmen, Hersteller)

Hersteller-getriebene Lösungen	→ ganzheitliche KI-Strategie
Nutzung privater Chatbots, Schatten-KI	→ prozessorientiert statt technikgetrieben
unklare Zuständigkeiten	→ Pilotprojekte, definierte Freigabeprozesse
Unsicherheit bzgl. Datenschutz und Informationssicherheit	→ Trennung von KI-System und -Modell

Fragen zum Stand der KI im Unternehmen

- Wird Chat-GPT oder Claude im Unternehmen genutzt?
- Erfolgt der Zugriff über private Accounts?
- Wird KI zur Optimierung von Geschäftsprozessen genutzt?
- Wird KI für Vibe Coding genutzt?
- Existiert im Unternehmen eine KI-Strategie?
- Existiert im Unternehmen eine KI-Richtlinie?

KI-Architektur: KI-Modell / KI-System



Art. 3 Nr. 63 KI-VO

KI-Modell

1. … ist ein Modell, das mit einer **großen Datenmenge** unter umfassender Selbstüberwachung trainiert wird,
2. das eine erhebliche **allgemeine Verwendbarkeit** aufweist,
3. das in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens, ein **breites Spektrum unterschiedlicher Aufgaben kompetent** zu erfüllen
4. und das in eine **Vielzahl nachgelagerter Systeme oder Anwendungen** integriert werden kann.
5. Ein KI-Modell ist ohne KI-System **nicht** nutzbar.

Bild KI-generiert

Art. 3 Nr. 1 KI-VO | ErwG 12

KI-System

1. … ist **ein maschinengestütztes** System, das für einen **autonomen Betrieb** ausgelegt ist,
2. das nach seiner Einführung **anpassungsfähig** sein kann.
3. Ein wesentliches Merkmal von KI-Systemen ist ihre Fähigkeit, abzuleiten.
4. Die Fähigkeit abzuleiten, **geht über die einfache Datenverarbeitung hinaus**, indem Lern-, Schlussfolgerungs- und Modellierungsprozesse ermöglicht werden.
5. Ein KI-System benötigt **zwingend** ein KI-Modell.

3. Anforderungen der DSGVO

Anforderungen der DSGVO

- Rechtmäßigkeitsprüfung, Zweckbindung der Datenverarbeitung
- angemessenes Datenschutzniveau
- Verträge zur Auftragsverarbeitung
- Verbot von automatisierten Einzelfallentscheidungen
- Umsetzung von Betroffenenrechten
- Dokumentation der KI-Systeme und KI-Modelle

Art. 6 Abs. 1 DSGVO

Rechtmäßigkeit

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

Zweckbindung lässt sich nur garantieren, wenn Daten nicht zur Optimierung des Sprachmodells verwendet werden. Dies muss in dem AV-Vertrag mit den Herstellern der KI-Systeme und KI-Modelle geregelt werden.

Angemessenes Datenschutzniveau

Art. 46 DSGVO

Open AI

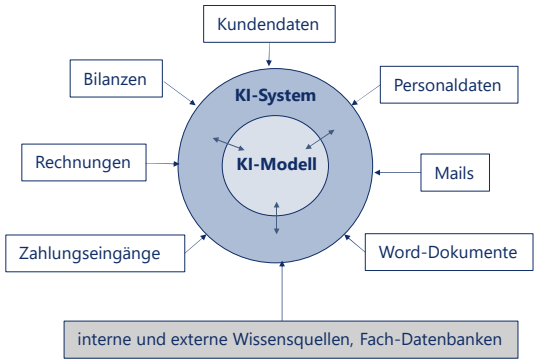
- Zertifizierung nach EU-US Data Privacy Framework
- zusätzlich Abschluss von Standardvertragsklauseln
- OpenAI Ireland Limited seit Februar 2024 als verantwortliche Stelle

Antropic

- keine Zertifizierung nach EU-US Data Privacy Framework
- lediglich Abschluss von Standardvertragsklauseln
- kein Hosting der KI-Modelle in der EU

KI-Modelle von Open AI und Antropic können auch über Microsoft, Amazon oder Google genutzt werden. Die Dienste heißen Azure OpenAI Services, Azure AI Foundry, AWS Bedrock, Vertex AI (Google)

KI-Architektur, Datenimport



KI-Modell:
- Vorschlag: Azure OpenAI Service
- Microsoft verfügt über C5-Testat
- Microsoft ermöglicht Verpflichtung auf ärztliche Schweigepflicht (§ 203 StGB) (Professional Secrecy Amendment)
- durch Aktivierung der Kunden-Lockbox erhält Microsoft nur nach Freigabe Zugriff auf Kundendaten
- Daten dürfen nicht zur Optimierung des KI-Modells genutzt werden.

KI-System:
- EU-Dienstleister übernimmt die Transaktion mit dem Sprachmodell
- und ermöglicht die Anbindung interner Wissensquellen
- Daten dürfen nicht zur Optimierung des KI-Systems genutzt werden.

Art. 22 DSGVO

Automatisierte Einzelfallentscheidungen

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.

Art. 12 – 23 DSGVO

Umsetzung von Betroffenenrechten

Betroffenenrechte, insbesondere **Auskunftsrechte**, das Recht auf Berichtigung unrichtiger Daten oder das Recht auf Datenlöschung können gegenüber dem **Betreiber des KI-Systems** nur schwer umgesetzt werden.

Der Betreiber kann dies nur in Zusammenarbeit mit dem **Anbieter des KI-Systems** realisieren (AV-Vertrag!)

Greifen Betroffenenrechte überhaupt gegenüber dem **Anbieter des KI-Modells**?

4. KI-Strategie

Eckpfeiler einer ganzheitlichen KI-Strategie

AI Act- und DSGVO-Konformität	**Prozessoptimierung statt Technikzentrierung**	**KI-Transformation als Management-Aufgabe, kein IT-Projekt**	**KI-Lenkungs-gremium, KI-Beauftragte, Pilotprojekte, KI-Werkstatt**
pilotartige Beschaffung, kürzere Vertragslaufzeiten	**zentraler Freigabeprozess** (Verwaltung zugelassener KI-Systeme und Wissensquellen)	**KI-Kompetenz der Mitarbeiter**	**KI-Richtlinie, Betriebsvereinbarung**

Grundsätze einer KI-Richtlinie

- KI-Systeme dürfen nur von Beschäftigten genutzt werden, die vorab an einer Grundkompetenzschulung teilgenommen haben.
- Es dürfen keine verbotenen KI-Systeme im Sinne von Art. 5 KI-Verordnung eingesetzt werden.
- Die Verarbeitung von Gesundheits- oder Personaldaten ist nur mit Genehmigung der Geschäftsführung zulässig. Hochrisiko-KI-Systeme und unterliegen zusätzlichen Freigabeprozessen.
- KI-Systeme dürfen nicht genutzt werden, um automatisierte Einzelentscheidungen zu treffen, von denen Mitarbeiter oder Kunden betroffen sind.
- KI-Systeme dürfen nicht für private Zwecke verwendet werden.
- KI-basierte Ergebnisse oder Berichte müssen explizit durch gesunden Menschenverstand hinterfragt und auf Qualität gesichert werden.
- KI-basierte Ergebnisse und Dokumente müssen als solche deklariert werden.

Anwendungsspezifische Regelungen

	Datenschutz	Informationssicherheit	Künstliche Intelligenz
übergreifende Regelungen	Datenschutz-Grundverordnung (DSGVO)	ISO 27001, 27017, 27018, NIS2-Richtlinie	KI-Verordnung der EU (AI Act)
Gesundheitswesen	Art. 9 DSGVO §§ 391-393 Sozialgesetzbuch V § 203 Strafgesetzbuch (StGB)	C5-Testate	§ 16, § 26 + Anhang AI Act Medizinprodukte-Durch-führungsgesetz (MPDG) In-vitro-Diagnostika-Richtlinie (IVDR)
Strafverfolgungsbehörden	Justiz- und Inneres-Richtlinie der EU (JI-Richtlinie) §§ 45-84 Bundesdatenschutz-gesetz (BDSG) Landespolizeigesetze	BSI-Grundschutz	Art. 5 Abs. 1 lit. h AI Act Art. 26 Abs. 10 AI Act

5. Haftung von Betreibern und Anbietern

Haftung von Betreibern und Anbietern

Betreiber	Anbieter
Unternehmen haftet für Organisationsverschulden, Auswahlverschulden und mangelhafte Infrastruktur.	Anbieter haftet, wenn Pflichten für Hochrisiko-KI-Systeme nach Art. 16 AI Act nicht umgesetzt sind (u.a. Qualitäts- und Risiko-Management).
Nutzung nicht zugelassener oder offensichtlich ungeeigneter KI-Systeme	Implementierung fehlerhafter Software
mangelhafte Integration der KI-Systeme in Geschäftsprozesse	Designfehler, ungeeignete KI-Modelle und nicht repräsentative Trainingsdaten
fehlende Qualifikation der KI-Anwender (Auswahlverschulden)	fehlende oder ungenügende Warnhinweisen und Gebrauchsanleitungen
Ignorieren von Herstellerhinweisen	

Vielen Dank für Ihre Aufmerksamkeit!

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

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