h_da

# AI Act vs DS-GVO: Keine Berührungspunkte beim Datenschutz?

**7. Fachtagung Datenschutz im Gesundheitswesen Künstliche Intelligenz im Gesundheitswesen: Und der Patientendatenschutz?**
**März 2025**
**Veranstalter: bitkom, BvD, bvitg, GDD, gmds**

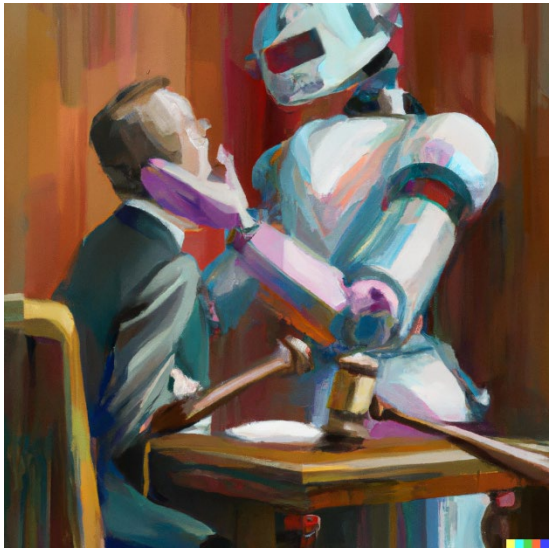
## Gliederung

- Personenbezug in LLMs und GPAIs
- Bleibt die DS-GVO wirklich unberührt von der KI-VO?
- Risikomanagement und Datengovernance
- Zusätzliche Vorgaben für Einwilligungen und Folgeabschätzungen
- Erlaubnistatbestände für die Verarbeitung sensibler Daten zur Beseitigung von Bias?

FAQ und Checklisten sowie Open Access-Publikationen
unter Copilot-recht.de / chatgpt-recht.de

h_da

# Kurzvorstellung



Prof. Dr. Thomas Wilmer

- Gf. Direktor Institut für Informationsrecht der Hochschule Darmstadt
- Leiter der Task-Force „KI und IP“ der Plattform Industrie 4.0 des BMBF und des BMWK
- Co-Ausschussvorsitzender des Fachausschusses „Digitale Wirtschaft und Plattformökonomie“ der DGRI
- Dozent der Fachanwaltsausbildung für das Recht der Informationstechnologie / Bereiche KI und Datenschutz
- Betreiber der Projektwebseite chatgpt-recht.de

*Juristische Sprache, Langeweile, keine Drogen, mentale Gewalt* *Ab 18*

# DSGVO Datenschutzschulung

100% Übereinstimmung **2024** **60 Min** **4K Ultra HD 5.1**


Viele haben von ihr gehört, nur wenige haben sie gelesen. Seit 3 Jahren ist sie unter uns. Du kannst sie nicht verstehen, Du musst sie spüren.

In einer Zeit der Verunsicherung erkundete eine kleine Gruppe verschworener Lehrgangsteilnehmender eine mächtige Regelung, die die Grenzen der Wahrnehmung sprengt. Sie werden ihre Seele restlos leeren und für die Tiefen der DSGVO öffnen. Sie kämpfen gegen die vier Dämonen der Leseunlust, der Ablenkung durch ihr Smartphone, der Unterzuckerung und der Fehlsichtigkeit.

Die Teilnehmenden, die sich dem hingeben, erwartet barmherzige Erleuchtung und eine Teilnahmebescheinigung.

*Prof. Dr. Thomas Wilmer*

*Datenschutzrecht, IT-Recht, Innendekoration*

**Beliebt auf avocado**

# Orientierungshilfen-Navigator KI & Datenschutz (ONKIDA)

Fundstellenübersicht zu zehn zentralen Vorgaben des Datenschutzrechts in aufsichtsbehördlichen Orientierungshilfen zu „Künstlicher Intelligenz“.
Stand Juli 2024. **Die Tabelle als PDF (200 kB)** **Einstiegsvideo (PeerTube)**

**Wobei hilft ONKIDA?** Werden bei KI-Anwendungen personenbezogene Daten verarbeitet, ist die **DS-GVO** anwendbar. Beginnend bei der Frage, wann und an welcher Stelle des Verarbeitungsprozesses man es mit personenbezogenen Daten (pbD) zu tun hat, gibt es zahlreiche weitere datenschutzrechtliche Implikationen. Namentlich, wie Verantwortliche der Maßgabe der Zweckbindung oder Ansprüchen auf Löschung sowie Auskunft bei KI-Systemen nachkommen können – und ab wann sie überhaupt datenschutzrechtlich verantwortlich sind. Zu den datenschutzrechtlichen Fragen, die sich beim Einsatz von KI stellen, gibt es inzwischen zahlreiche Handreichungen von Aufsichtsbehörden, um Verantwortlichen Hilfestellung zu liefern. Dabei zeigt sich ein grundsätzlich sehr einheitliches Bild in der Auslegung, auch wenn im Einzelnen unterschiedliche Schwerpunkte gesetzt werden. ONKIDA gibt hier einen ersten Überblick und versteht sich als Hilfestellung für die Arbeit mit diesen Orientierungshilfen, indem ein schnellerer Zugang zu Einzelaspekten zentraler datenschutzrechtlicher Vorgaben ermöglicht wird.

**Anwendung:** In der linken Spalte (senkrechte Linie) sind zentrale datenschutzrechtliche Vorgaben zu finden („TopTen Datenschutz und KI“), die regelmäßig bei KI-Anwendungen mit pbD eine Rolle spielen. In der obersten Zeile (waagerechte Reihe) findet sich eine Auswahl von Orientierungshilfen verschiedener Aufsichtsbehörden bzw. kooperierender Gremien zu Schnittstellen von DS-GVO und KI, die jeweils verlinkt sind zu den Originaldokumenten. Für jedes Dokument gibt ONKIDA dann in den einzelnen Feldern an, ob und wenn ja an welcher Stelle (Seite, Randnummer) das jeweilige Papier Aussagen zu den Vorgaben in der linken Spalte enthält.

| | **A. EDPS Guidelines on generative AI and the EUDPR (2024, PDF)** *Datenverarbeitung durch EU-Organe* | **B. Report der EDSA Taskforce ChatGPT (2024, PDF)** | **C. DSK: Orientierungshilfe zu KI und Datenschutz (2024, PDF)** | **D. LfDI BW: Rechtsgrundlagen zum Einsatz von KI (2023)** | **E. BayLDA: Checkliste Datenschutzkonforme KI (2024, PDF)** | **F. Hamb Check LLM-b (2023,** |
|---|---|---|---|---|---|---|
| **1. Grundsatz der Datenrichtigkeit** Art. 5 I lit. d) DSGVO | **(+)** S. 15 f. (Art. 4 I lit. d) VO 2018/1725) | **(+)** Rn. 29 ff. sowie im Fragebogen im Annex, S. 11 | **(+/−)** Recht auf Berichtigung Rn. 27, Überprüfung der Richtigkeit der Ergebnisse Rn. 64 f. | **(−)** | **(+/−)** Recht auf Berichtigung, S. 6, 10 | **(+/−)** Üb Richtigke S. 4 |
| **2. Grundsatz der Daten-minimierung** | **(+)** Datenminimierung: S. 14 (Art. 4 I lit. c) VO 2018/1725) | **(+/−)** nur im Rahmen des Fragebogens im Annex, S. 10 | **(+)** Zweckbindung Rn. 1 f. | **(+/−)** Berücksichtigung Datenminimierung bei Art. 6 I | **(+/−)** Zweckbindung nur eher indirekt S. 6, 8, 11 | **(−)** |

| | A. EDPS Guidelines on generative AI and the EUDPR (2024, PDF)↗ *Datenverarbeitung durch EU-Organe* | B. Report der EDSA Taskforce ChatGPT (2024, PDF)↗ | C. DSK: Orientierungshilfe zu KI und Datenschutz (2024, PDF)↗ | D. LfDI BW: Rechtsgrundlagen zum Einsatz von KI (2023) | E. BayLDA: Checkliste Datenschutzkonforme KI (2024, PDF)↗ | F. Ham Chec LLM- (2023 |
|---|---|---|---|---|---|---|
| **3. Personenbezug** Art. 4↗ Nr. 1 DSGVO | | | | | | |
| **4. Rechtsgrundlagen für die Datenverarbeitung** Art. 6↗ I u. 9↗ II DSGVO | VO 2018/1725) | Fragebogen S. 12 f. | auf Positionspapier LfDI BW), Rn. 62 (im Zusammenhang mit sensiblen Daten) | | | Zusamm Persone Zusamm Diskrimi |
| **5. (Mit−)Verantwortlichkeit** Art. 26↗ (und 28↗) DSGVO | **(+)** S. 6 | **(+/−)** Rn. 23 ff. in Zusammenhang mit Fairness-Prinzip, „Abwälzung" der Verantwortlichkeit auf betroffene Personen; im Rahmen des Fragebogens S. 14 | **(+)** Rn. 32 ff. | **(+)** S. 9 ff. | **(+)** S. 9 | **(−)** |
| **6. Transparenzgebot und Informationspflichten** Art. 5↗ I lit. a und 12 ff. DSGVO | **(+)** S. 17 (Art. 14 VO 2018/1725) | **(+)** Rn. 27 f., ebenso im Fragebogen S. 13 | **(+)** Rn. 21 ff. | **(+)** S. 12 (im Zusammenhang mit informierter Einwilligung) | **(+)** Transparenz S. 7 (als Teil des „Datenschutz-Risikomodells") **(+)** Infopflichten S. 5 (Checkliste) | **(−)** |
| **7. Auskunftsanspruch** Art. 15↗ DSGVO **Recht auf Löschung** Art. 17↗ DSGVO | **(+/−)** allgemein Betroffenenrechte S. 22 | **(+)** allgemein Betroffenenrechte Rn. 32 ff. | **(+)** nur Recht auf Löschung Rn. 26, 28 f.; „weitere Betroffenenechte" Rn. 30 | **(+)** nur Recht auf Löschung S. 12 | **(+)** Auskunftsanspruch S. 5, 10 (Checkliste), Recht auf Löschung S. 6, 10 (Checkliste) | **(−)** |
| **8. Automatisierte Entscheidungen und Profiling** Art. 22↗ DSGVO | **(+)** S. 18 (Art. 24 VO 2018/1725) | **(−)** | **(+)** Rn. 12 ff. | **(−)** | **(−)** | **(+)** S. 2 |
| **9. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen** | **(+)** S. 9 (Art. 27 VO 2018/1725) | **(+)** Rn. 7 knappe Bezugnahme; Rn. 35 im Zusammenhang mit | **(+)** Rn. 43 | **(+/−)** S. 7 (Bewertung Personenbezug), S. 18 Fn. 57 (Berücksichtigung bei Art. 6 I | **(+)**, S. 7 (nur ein knapper Satz) | **(−)** |

# KI und Datenschutz: Vorfragen

- KI-Definition: https://ec.europa.eu/newsroom/dae/redirection/document/112455
- Leitlinien zur Definition von KI-Systemen der EU-Kommission, 06.02.25

Datenschutz betrifft

- Tool
- Input
- Output

# KI und Datenschutz: Vorfragen

- Wer ist verantwortliche Stelle? In welcher Verarbeitungsstufe?
  - Anbieter
  - Betreiber
- „derjenige, der allein oder gemeinsam mit anderen über die jeweiligen Zwecke und Mittel entscheidet.“

# Personenbezug: Ausgangslage

- Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
- LLMs (Large Language Models) und GPAIs (General Purpose AI) verarbeiten oft riesige Textmengen, in denen personenbezogene Daten enthalten sein können. Auch indirekt identifizierbare Personen fallen unter den Schutzbereich der DSGVO (ErwG 26 DSGVO).

# Personenbezug: Ausgangslage

- https://datenschutz-hamburg.de/news/hamburger-thesen-zum-personenbezug-in-large-language-models :

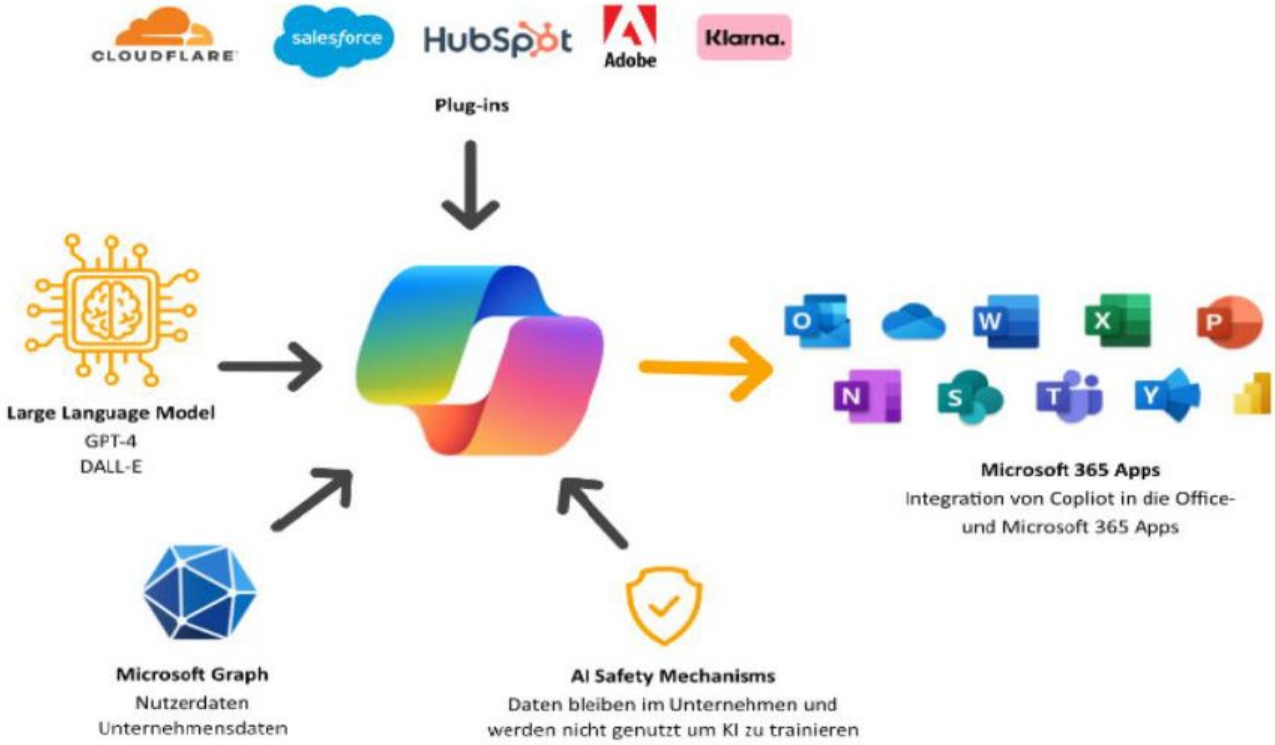
**„Die bloße Speicherung eines LLMs stellt keine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar.** Denn in LLMs werden keine personenbezogenen Daten gespeichert. Soweit in einem LLM-gestützten KI-System personenbezogene Daten verarbeitet werden, müssen die Verarbeitungsvorgänge den Anforderungen der DSGVO entsprechen. Dies gilt insbesondere für den Output eines solchen KI-Systems.

**Mangels Speicherung personenbezogener Daten im LLM können die Betroffenenrechte der DSGVO nicht das Modell selbst zum Gegenstand haben.** Ansprüche auf Auskunft, Löschung oder Berichtigung können sich jedoch zumindest auf Input und Output eines KI-Systems der verantwortlichen Anbieter:in oder Betreiber:in beziehen.

**Das Training von LLMs mit personenbezogenen Daten muss datenschutzkonform erfolgen**. Dabei sind auch die Betroffenenrechte zu beachten. Ein gegebenenfalls datenschutzwidriges Training wirkt sich aber nicht auf die Rechtmäßigkeit des Einsatzes eines solchen Modells in einem KI-System aus.“

h_da

# Personenbezug: Ausgangslage

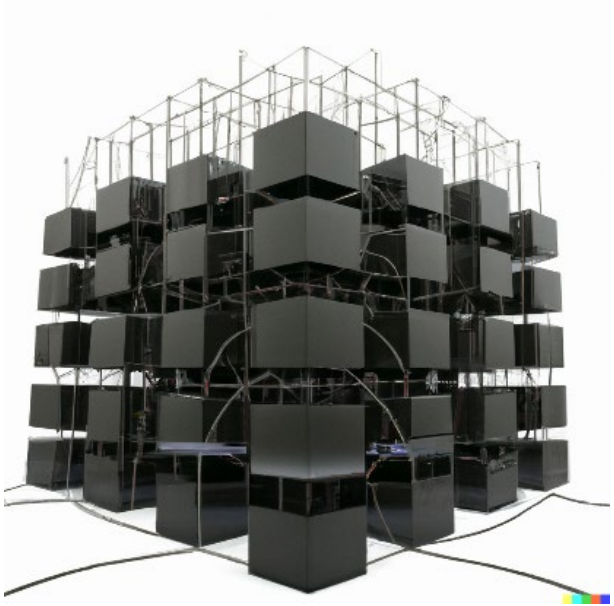


# Personenbezug: Problemstellung

- **Personenbezug** bei Trainingsdaten ist oft schwer erkennbar, insbesondere bei Web-Scraping oder öffentlichen Datensätzen.
- Token selbst sind nicht personenbezogen
- Zentral: Können mit einem Prompt personenbezogene Daten aufgerufen werden?
- Unterschiedliche Risiken in verschiedenen Phasen: Datenerhebung, Training, Nutzungsanpassung
- LLMs/GPAIs generieren auch Inhalte, die unbeabsichtigt personenbezogene Daten enthalten können (sog. "hallucination").

# Verarbeitung: Ausgangslage

- Daten müssen nach Art. 5 DSGVO rechtmäßig verarbeitet werden
  - Privacy by design and by default
  - Erforderlichkeitsgrundsatz
  - Zweckbindung
  - Richtigkeit
- Verbot mit Erlaubnisvorbehalt
  - Rechtsgrundlage ist erforderlich, Artt. 6, 9 DSGVO
    - Einwilligung
    - Vertragserfüllung
    - Gesetz (**KI-VO keine passende Grundlage, ErwGr. 63 KI-VO)**
    - Berechtigte Interessen



# Verarbeitung : Ausgangslage

- Rechtsgrundlage ist erforderlich
  - Gesetz
    - KI-VO íst keine passende Grundlage, ErwGr. 63 KI-VO
    - Ausnahmen:
      - 59 Abs., 1 KI-VO Rechtmäßig für andere Zwecke erhobene personenbezogene Daten dürfen im KI-Reallabor ausschließlich für die Zwecke der Entwicklung, des Trainings und des Testens bestimmter KI-Systeme im Reallabor verarbeitet werden, wenn alle der folgenden Bedingungen erfüllt sind…
      - Art. 10 Abs. 5 BIAS, s.u.

# Verarbeitung : Ausgangslage

- Rechtsgrundlage ist erforderlich
  - Gesetz
    - Digital-Gesetz (DigiG) und Gesundheitsdatennutzungsgesetz (GDNG)
    - European Health Data Space (EHDS): ErwGr. 43 „Zusätzlich zu den Aufgaben, die zur Sicherstellung einer wirksamen Sekundärnutzung von Gesundheitsdaten erforderlich sind, sollte die Stelle für den Zugang zu Gesundheitsdaten darauf hinarbeiten, die Verfügbarkeit zusätzlicher Gesundheitsdatensätze auszuweiten, die Entwicklung von KI im Gesundheitswesen zu unterstützen und die Entwicklung gemeinsamer Standards zu fördern. Sie sollten erprobte Techniken nutzen, die sicherstellen, dass die elektronischen Gesundheitsdaten in einer Weise verarbeitet werden, bei der die Privatsphäre in Bezug auf die Informationen in den Daten, deren Sekundärnutzung erlaubt wird, gewahrt bleibt; dazu gehören auch Techniken zur Pseudonymisierung, Anonymisierung, Generalisierung, Unterdrückung und Randomisierung personenbezogener Daten; Die Stellen für den Zugang zu Gesundheitsdaten können Datensätze so bearbeiten, dass sie die Anforderungen der Datennutzer entsprechend der erteilten Datengenehmigung erfüllen. Dazu gehören auch Vorschriften für die Anonymisierung von Mikrodatensätzen.

# Verarbeitung : Ausgangslage

https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/

„Für die Nutzung von besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO kommen in Zukunft die Regelungen nach Art. 34 der Verordnung über den Europäischen Gesundheitsdatenraum (folgend: EHDS-VO) in Betracht: Danach ist die Weiterverarbeitung (Sekundärnutzung) von elektronisch gespeicherten Gesundheitsdaten u. a.

für Zwecke der im öffentlichen Interesse liegenden öffentlichen und beruflichen Gesundheit (vgl. Art. 34 Abs. 1 Buchst. a EHDS-VO)

**für die Gesundheitsforschung einschließlich der Produktentwicklung, dem Training, der Testung und Evaluierung von algorithmischen und von KI-Systemen** und

zur Verbesserung der Gesundheitsversorgung einschließlich der medizinischen Behandlungen (vgl. Art. 34 Abs. 1 Buchst. h EHDS-VO) vorgesehen.“

**Art. 34 I (g) training, testing and evaluating of algorithms, including in medical devices, AI systems and digital health applications, contributing to the public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices;**

h_da

# Verarbeitung und Personenbezug: Relevanz und Fazit

Besondere Datenschutzprobleme bei KI

- KI-VO erweitert Rechtsgrundlagen nicht wirklich
- Erweiterung um „Gedächtisfunktionen“
- Umsetzung Betroffenenrechte: Auskunft, Löschung, Berichtigung
- Richtigkeit der Daten: Bias bei Personenbezug
- Scoring: Verbot der automatisierten Entscheidung
- Rollen- und Zugriffsmodelle bei GPAI

h_da

# Bleibt die DS-GVO wirklich unberührt von der KI-VO?

**Klarstellung in der KI-VO**

Erwägungsgrund 26 und Art. 2 Abs. 5 KI-VO: Die KI-VO „lässt die Anwendung der DSGVO unberührt".

-> **Keine Verdrängung oder Einschränkung der DSGVO durch die KI-VO**.

**Praktische Wechselwirkungen**

**Datenschutz-Folgenabschätzungen (Art. 35 DSGVO)** überschneiden teilweise sich mit den Risikomanagement-Anforderungen der KI-VO.

**Rechtsgrundlagen (Artt. 6, 9 DSGVO)** sind weiterhin erforderlich, auch wenn die KI-VO ein System als „niedriges Risiko" einstuft.

**Datenminimierung, Zweckbindung** bleiben zwingend, auch wenn die KI-VO flexible Vorgaben zur Datennutzung zulässt (z. B. für Bias-Monitoring).

# Risikomanagement und Datengovernance

## Vorgaben der KI-VO

Risikomanagementsystem (Art. 9 KI-VO): Identifikation, Analyse, Steuerung und Monitoring von Risiken.

Datengovernance (Art. 10 KI-VO): Qualität und Repräsentativität von Trainings-, Validierungs- und Testdaten; Bias-Vermeidung.

## DSGVO-Parallelen

**Art. 24 DSGVO (Verantwortlichkeit)**: Verpflichtung zu wirksamen Datenschutzmaßnahmen (inkl. Governance).

**Art. 32 DSGVO (Sicherheit)**: Technische und organisatorische Maßnahmen.

**Art. 25 DSGVO (Privacy by Design)**: Datenminimierung, Zweckbindung.

# Risikomanagement und Datengovernance

## Konfliktpotenzial

**KI-VO betont die Bedeutung der Trainingsdaten-Qualität** (Breite, Repräsentativität), während die DSGVO Datenminimierung fordert.
**DSGVO legt Fokus auf Zweckbindung**, während die KI-VO breitere Nachnutzungen zu Bias-Kontrollen fordert.

## Fazit

- **Datengovernance wird zum doppelten Pflichtfeld**: DSGVO-konforme Datenverarbeitung und KI-VO-konforme Datenqualität.
- **Risikomanagement wird parallel aus Datenschutz- und KI-Perspektive notwendig.**

# Risikomanagement und Datengovernance

Dazu https://www.lda.bayern.de/de/ki.html

„**KI-Compliance**“ kann durch den Aufbau eine KI-Managementsystems realisiert werden. Dazu kann es sich anbieten, ein gerade bei größeren Unternehmen häufig schon bestehendes Datenschutzmanagementsystem „anzureichern“, mit dem Vorteil, dass die interne Aufbau- und Ablauforganisation nur geringfügig angepasst werden muss.“

h_da

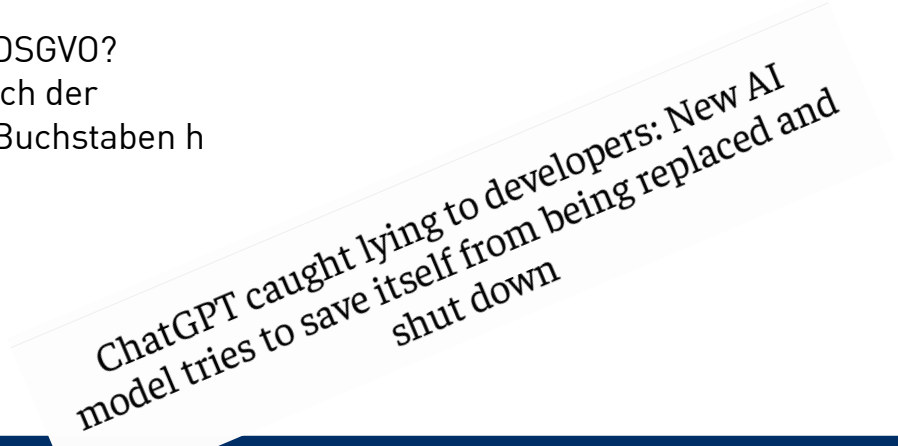
# Risikomanagement und Datengovernance

**Dazu** https://www.lda.bayern.de/de/ki.html

„Die KI-Verordnung sieht den Aufbau von KI-Kompetenz im Unternehmen vor. Die Rolle eines **„KI-Beauftragten“** ist in der KI-VO zwar nicht explizit vorgesehen, mittelbar scheint eine solche Rolle aber in zahlreichen Anforderungen der KI-VO gerade bei größeren Unternehmen geradezu vorausgesetzt. Zu den Aufgaben des betrieblichen Datenschutzbeauftragten gehörten bereits jetzt u.a. die Sensibilisierung und Beratung Verantwortlicher. Damit spricht jedenfalls bei Aufgaben, die nicht mit Entscheidungskompetenzen über die die Nutzung von KI verbunden sind, regelmäßig nichts dagegen, dass ein bereits bestellter DSB, der bereits Expertise für das Unternehmen und KI (aus Datenschutzsicht) mitbringt, auch die Rolle eines solchen KI-Beauftragten als zentraler Ansprechpartner und Koordinator für die KI-Nutzung übernimmt.“

# Risikomanagement und Datengovernance

- KI-unabhängige Datenschutzkonformität des Tools prüfen
- Datenschutzrisiken der Trainingsbasis klären
- Eingabe pbD und Prompts zum „Herausfragen“ von pbD vermeiden
- Pseudonymisierung und Anonymisierung beim Training
- BIAS-Vermeidung: Datenqualität prüfen / Transparenz bei Ausgabe
- Löschpflichten: Ausnahme nach Art. 17 Abs.3 lit c DSGVO? „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;“
- Richtlinien zum Umgang festlegen
- Schulung, Schulung, Schulung



# Zusätzliche Vorgaben für Einwilligungen und Folgeabschätzungen

**Einwilligungen**

DSGVO: Einwilligung nach Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. a DSGVO.

KI-VO:

- Transparenzpflichten (u.a. Art. 50 KI-VO) können dazu führen, dass bestehende Einwilligungen erweitert werden müssen (z. B. zusätzliche Information über KI-Nutzung und mögliche Bias-Risiken).
- Art. 61 KI-VO Sachkundige Einwilligung, Erwgr. 141:
  „Die Einwilligung der Testteilnehmer zur Teilnahme an solchen Tests im Rahmen dieser Verordnung unterscheidet sich von der Einwilligung betroffener Personen in die Verarbeitung ihrer personenbezogenen Daten nach den einschlägigen Datenschutzvorschriften und greift dieser nicht vor.“

# Zusätzliche Vorgaben für Einwilligungen und Folgeabschätzungen

**Folgeabschätzungen**

DSGVO: Datenschutz-Folgenabschätzung (Art. 35 DSGVO).

KI-VO: Konformitätsbewertung und Risikomanagement (Art. 9 ff. KI-VO).

**Zusammenwirken**

**Doppelpflicht**: Unternehmen müssen sowohl DSGVO-Folgenabschätzungen als auch KI-Risikobewertungen durchführen.

**Abgleichbar, aber nicht identisch**: DSGVO fokussiert Datenschutzrisiken, KI-VO System- und Bias-Risiken.

h_da

# Erlaubnistatbestände für die Verarbeitung sensibler Daten zur Beseitigung von Bias?

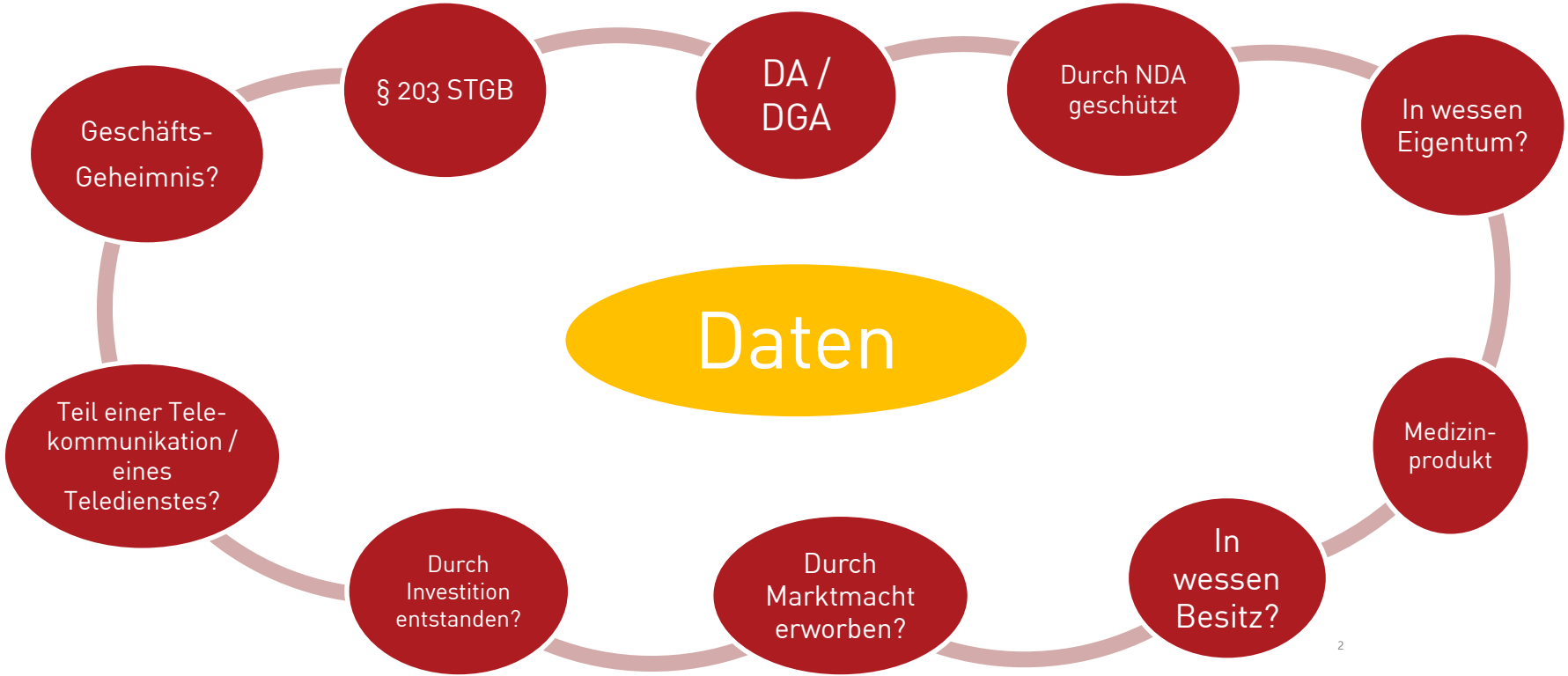
Soweit dies für die Erkennung und Korrektur von **Verzerrungen** im Zusammenhang **mit Hochrisiko-KI-Systemen** im Einklang mit Absatz 2 Buchstaben f und g dieses Artikels **unbedingt erforderlich** ist, dürfen die Anbieter solcher Systeme ausnahmsweise besondere Kategorien personenbezogener Daten verarbeiten, wobei sie angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen müssen. [2]Zusätzlich zu den Bestimmungen der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680 müssen alle folgenden Bedingungen erfüllt sein, damit eine solche Verarbeitung stattfinden kann:

- Die Erkennung und Korrektur von Verzerrungen kann durch die Verarbeitung anderer Daten, einschließlich **synthetischer oder anonymisierter Daten**, nicht effektiv durchgeführt werden;
- die besonderen Kategorien personenbezogener Daten unterliegen technischen Beschränkungen einer Weiterverwendung der personenbezogenen Daten und modernsten Sicherheits- und Datenschutzmaßnahmen, einschließlich **Pseudonymisierung**;
- die besonderen Kategorien personenbezogener Daten unterliegen Maßnahmen, mit denen sichergestellt wird, dass die verarbeiteten personenbezogenen Daten **gesichert, geschützt und Gegenstand angemessener Sicherheitsvorkehrungen** sind, wozu auch strenge Kontrollen des Zugriffs und seine Dokumentation gehören, um Missbrauch zu verhindern und sicherzustellen, dass nur befugte Personen Zugang zu diesen personenbezogenen Daten mit angemessenen Vertraulichkeitspflichten haben;

# Erlaubnistatbestände für die Verarbeitung sensibler Daten zur Beseitigung von Bias?

- die besonderen Kategorien personenbezogener Daten werden **nicht an Dritte** übermittelt oder übertragen, noch haben diese Dritten anderweitigen Zugang zu diesen Daten;
- die besonderen Kategorien personenbezogener Daten werden **gelöscht**, sobald die Verzerrung korrigiert wurde oder das Ende der Speicherfrist für die personenbezogenen Daten erreicht ist, je nachdem, was zuerst eintritt;
- die **Aufzeichnungen über Verarbeitungstätigkeiten** gemäß den Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680 enthalten die Gründe, warum die Verarbeitung besonderer Kategorien personenbezogener Daten für die Erkennung und Korrektur von Verzerrungen unbedingt erforderlich war und warum dieses Ziel mit der Verarbeitung anderer Daten nicht erreicht werden konnte.

# Daten über DSGVO / KI-VO hinaus



# h_da Quellen

Quellen und weitere Informationen:


- Wilmer, KI-Verordnung: Datenschutzrechtliche Herausforderungen, BVD-News 01/24, S. S. 6
- Wilmer, Rechtliche Rahmenbedingungen für KI-Systeme , Tatup 2021, 56, https://doi.org/10.14512/tatup.30.3.56
- Wilmer, Europäisches Daten-Lizenzrecht im Umbruch , NJW-Spezial 2022, S. 2-4, https://neuheiten.beck.de/llm-special/67043655.
- Wilmer, Rechtsfragen bei ChatGPT & Co. Einsatz und Nutzung nach aktuellem und künftigem Recht, K&R 2023, 233.
- Wilmer, Rechtsfragen bei DALL-E & Co. - Schutzfähigkeit der „Promptografie“? K&R 2023, 385
- Gutjahr, Hornung, Krieger, Schaller, Selzer, Spiecker gen. Döhmann, Wilmer: Studie: Fehlende Rechtssicherheit für Big Data und KI
- https://www.athene-center.de/fileadmin/Downloads/Systematic_Privacy_Studie_2023.pdf?_=1699890300
- Wilmer, Herausforderungen der Vertragsgestaltung mithilfe Künstlicher Intelligenz, EuZW 2024, 868
- Wilmer, KI-Recht, Textsammlung, 1.A. 2024
- Wilmer, KI-Recht und Datenschutz, in Jandt/Steidle, Datenschutz im Internet, 2.A. 202

# Empfehlungen

Quellen und weitere Informationen:

- Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI modelsdes EDSA vom 17. Dezember 2024,
- Orientierungshilfe „Künstliche Intelligenz und Datenschutz der DSK vom 06. Mai 2024,
- KI-Checkliste des Bayerischen Landesamts für Datenschutzaufsicht,
- Checkliste zum Einsatz LLM-basierter Chatbots des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit,
- Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

h_da

# Danke für Ihre Aufmerksamkeit!

**Kontakt: thomas.wilmer@h-da.de**