



Grundlagen KI in der öffentlichen Verwaltung

Digi-Lunch am 14. Mai 2024

Yvonne Herzog, Sachbearbeiterin beim

Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg

1. Prolog
2. Überblick über die KI-VO
3. Grundfragen KI und Datenschutz
4. Orientierungshilfe der DSK



„KI liefert keine perfekten Ergebnisse, aber gibt jeder und jedem einen blitzschnellen Praktikanten an die Seite, der unermüdlich Dokumente durchackert, lästige Verwaltungsaufgaben erledigt oder im richtigen Tonfall Mails an Auftraggeber verfasst, die ihre Rechnungen noch nicht bezahlt haben.“

[Gregor Schmalzried, brand eins 09/2023, S. 62](#)



Innovation. Chancen. Risiken.

1. Prolog



1936: Turingmaschine

1956: Die Geschichte beginnt: der Begriff „KI“ entsteht

1966: Geburt des ersten Chatbots

1972: KI gelangt in die Medizin

1986: „NETtalk“ spricht

1997: Computer schlägt Schachweltmeister

2011: KI erreicht den Alltag

2018: KI debattiert über Raumfahrt und vereinbart einen Friseurtermin

2022: ChatGPT (GPT-3) kostenfreier Zugang für Öffentlichkeit

2023: u.a. offizielle Version [4.0 von GPT](#) und weitere Sprachmodelle (sog. LLM) treten in die Öffentlichkeit

20xx: Die nahe Zukunft



Innovation. Chancen. Risiken.

2. Überblick über die KI-VO

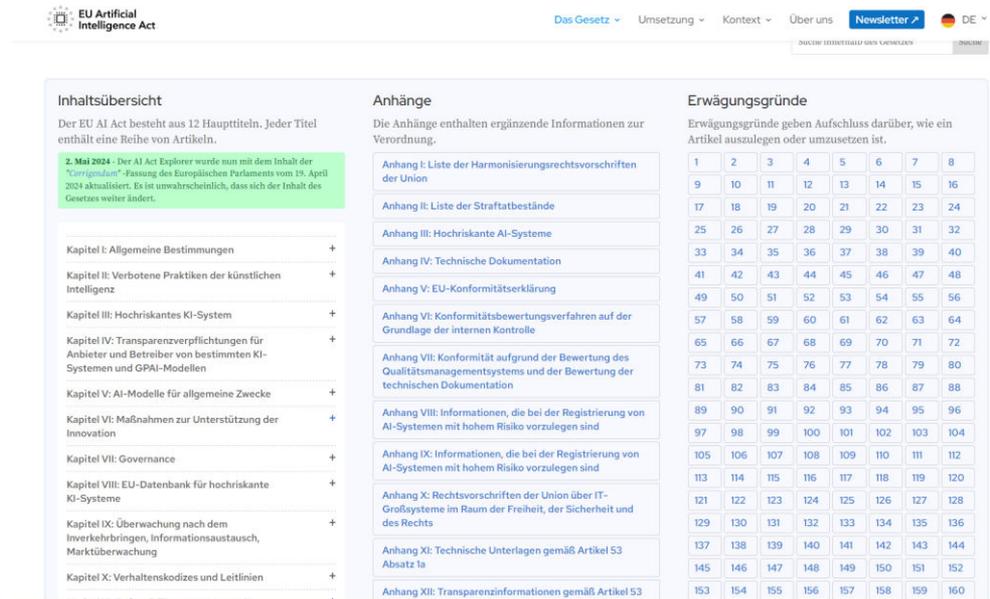
- Dezember 2023 - Europäische Union erzielt nach anhaltenden Trilog-Verhandlungen eine Einigung über die KI-VO
- 13. März 2024 - Beschluss der KI-VO durch das Europäische Parlament mit Korrekturen vom 25. April 2024
- formelle Genehmigung des Rats
- Veröffentlichung im offiziellen Gesetzblatt der Europäischen Union
- gestuftes Wirksamwerden von Normen

Produkthaftungsgesetz

→ guten Überblick bietet: <https://artificialintelligenceact.eu/de/>

- 13 Kapitel mit 113 Artikel
- 180 Erwägungsgründe
- 8 Anhänge
- die aktuelle PDF-Version hat einen Umfang von 460 Seiten
- „Produkthaftungsvorschriften“

<https://artificialintelligenceact.eu/de/ai-act-explorer/>



The screenshot shows the 'EU Artificial Intelligence Act' Explorer interface. It features a top navigation bar with 'Das Gesetz', 'Umsetzung', 'Kontext', 'Über uns', and a 'Newsletter' button. The main content is divided into three columns: 'Inhaltsübersicht', 'Anhänge', and 'Erwägungsgründe'. The 'Inhaltsübersicht' column lists 12 chapters (Kapitel I to XII) with expandable arrows. The 'Anhänge' column lists 12 annexes (Anhang I to XII) with expandable arrows. The 'Erwägungsgründe' column contains a grid of 160 numbered boxes, arranged in 8 rows and 20 columns, representing the grounds for the act.

Inhaltsübersicht
Der EU AI Act besteht aus 12 Haupttiteln. Jeder Titel enthält eine Reihe von Artikeln.

2. Mai 2024 - Der AI Act Explorer wurde nun mit dem Inhalt der "Corrigendum"-Fassung des Europäischen Parlaments vom 19. April 2024 aktualisiert. Es ist unwahrscheinlich, dass sich der Inhalt des Gesetzes weiter ändert.

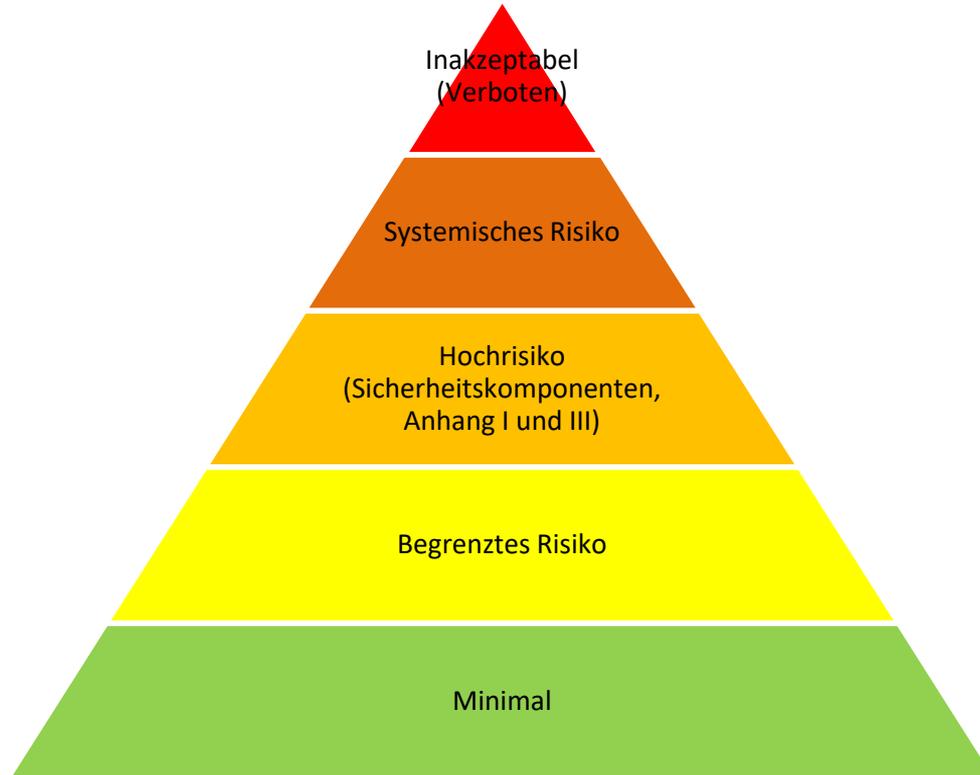
- Kapitel I: Allgemeine Bestimmungen
- Kapitel II: Verbotene Praktiken der künstlichen Intelligenz
- Kapitel III: Hochriskantes KI-System
- Kapitel IV: Transparenzpflichtungen für Anbieter und Betreiber von bestimmten KI-Systemen und GPAI-Modellen
- Kapitel V: AI-Modelle für allgemeine Zwecke
- Kapitel VI: Maßnahmen zur Unterstützung der Innovation
- Kapitel VII: Governance
- Kapitel VIII: EU-Datenbank für hochriskante KI-Systeme
- Kapitel IX: Überwachung nach dem Inverkehrbringen, Informationsaustausch, Marktüberwachung
- Kapitel X: Verhaltenskodizes und Leitlinien

Anhänge
Die Anhänge enthalten ergänzende Informationen zur Verordnung.

- Anhang I: Liste der Harmonisierungsrechtsvorschriften der Union
- Anhang II: Liste der Straftatbestände
- Anhang III: Hochriskante AI-Systeme
- Anhang IV: Technische Dokumentation
- Anhang V: EU-Konformitätserklärung
- Anhang VI: Konformitätsbewertungsverfahren auf der Grundlage der internen Kontrolle
- Anhang VII: Konformität aufgrund der Bewertung des Qualitätsmanagementsystems und der Bewertung der technischen Dokumentation
- Anhang VIII: Informationen, die bei der Registrierung von AI-Systemen mit hohem Risiko vorzulegen sind
- Anhang IX: Informationen, die bei der Registrierung von AI-Systemen mit hohem Risiko vorzulegen sind
- Anhang X: Rechtsvorschriften der Union über IT-Großsysteme im Raum der Freiheit, der Sicherheit und des Rechts
- Anhang XI: Technische Unterlagen gemäß Artikel 53 Absatz 1a
- Anhang XII: Transparenzinformationen gemäß Artikel 53

Erwägungsgründe
Erwägungsgründe geben Aufschluss darüber, wie ein Artikel auszulegen oder umzusetzen ist.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64
65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88
89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104
105	106	107	108	109	110	111	112
113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128
129	130	131	132	133	134	135	136
137	138	139	140	141	142	143	144
145	146	147	148	149	150	151	152
153	154	155	156	157	158	159	160



vollständiges oder teilweises
Verbot

KI mit allgemeinem
Verwendungszweck, zusätzliche
Maßnahmen und Kontrollen

z.B. Ex-ante-
(Selbst)Zulassungsverfahren

Transparenzpflichten,
Risikofolgenabschätzung, Ex-post-
Kontrolle etc

-



Innovation. Chancen. Risiken.

3. Grundfragen KI und Datenschutz

The Elephant in the Room...



Der Landesbeauftragte für den
Datenschutz und die
Informationsfreiheit
Baden-Württemberg



Ein Elefant sitzt in einem Serverraum und versteckt sich hinter Kabeln

Bing Image Creator | 1024 x 1024 jpg | Jetzt erstellt



Teilen



Speichern



Herunterladen



Feedback

Inhaltsnachweise

Mit KI erstellt · 13. November 2023 um 6:55 PM

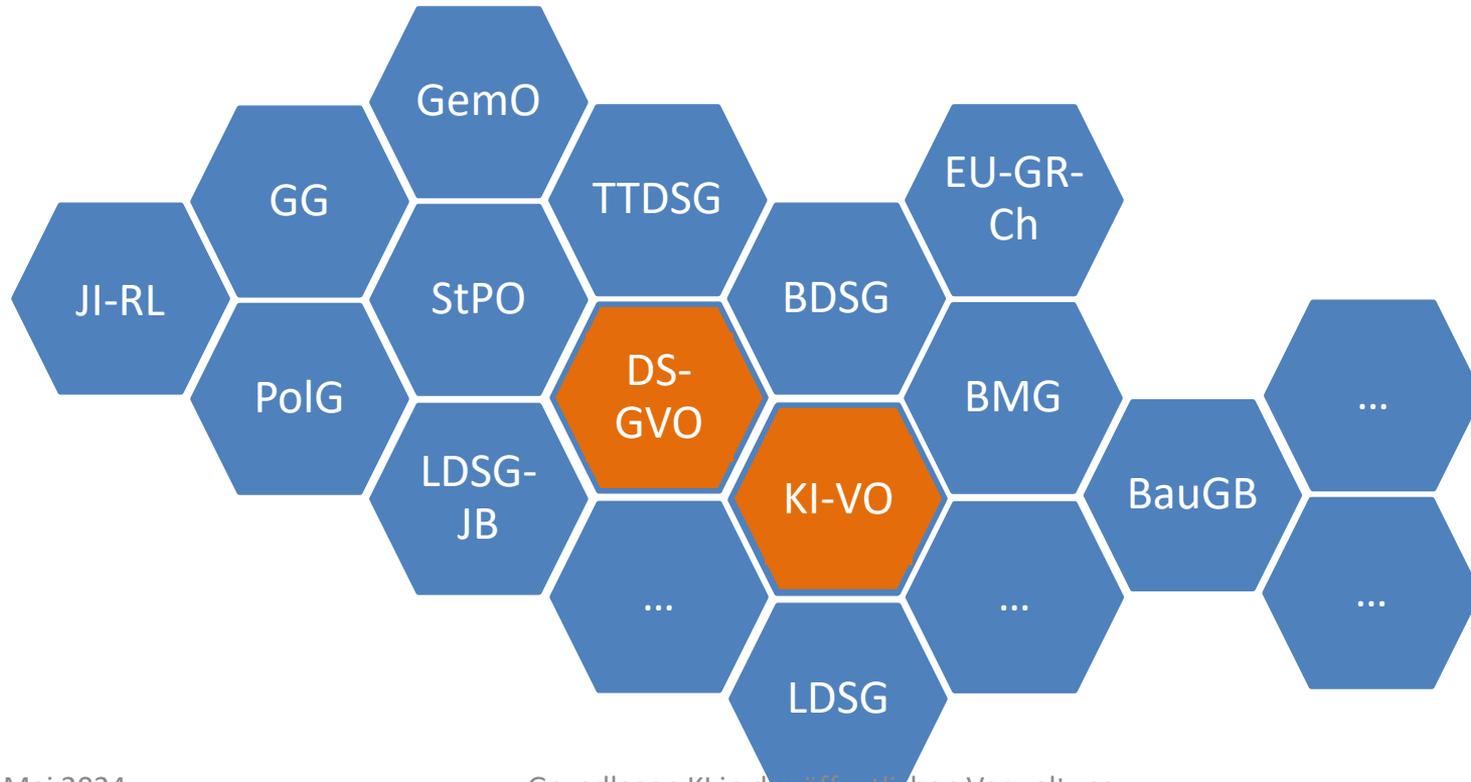


Überblick über Vorschriften



Der Landesbeauftragte für den
Datenschutz und die
Informationsfreiheit
Baden-Württemberg







Innovation. Chancen. Risiken.

3. Orientierungshilfe der DSK

- Überblick über datenschutzrechtliche Kriterien, für die datenschutzkonforme Nutzung von KI-Anwendungen
- Leitfaden, um KI-Anwendungen auszuwählen, zu implementieren und zu nutzen



https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf

greift u.a. folgende Punkte auf:

- a) Bestimmung von **Einsatzfeld** und **Zweck** und deren Rechtmäßigkeit
- b) Datenschutzkonformes Training von KI-Anwendungen
- c) **Rechtsgrundlagen für die Datenverarbeitung**
- d) **keine automatisierte Letztentscheidung**
- e) **geschlossenes oder offenes System**
- f) **Transparenz und Betroffenenrechte**

- **Verantwortlichkeit** festlegen und verbindlich regeln
- **Interne Regelungen** treffen und Beschäftigte sensibilisieren
- Datenschutz-Folgenabschätzung
- Beschäftigte schützen, **betriebliche Accounts** einrichten
- Datenschutz durch **Technikgestaltung** und durch datenschutzfreundliche **Voreinstellungen**
- **Datensicherheit**

- Vorsicht bei Eingabe und Ausgabe personenbezogener Daten
- Besondere Vorsicht bei besonderen Kategorien personenbezogener Daten
- Ergebnisse und Verfahren auf Diskriminierung prüfen

... in Baden-Württemberg



Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Über uns | Datenschutz | Informationsfreiheit | Infothek | Kultur | Bildungszentrum | Kontakt

Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz

Wann und wie dürfen personenbezogene Daten für das Training und die Anwendung von Künstlicher Intelligenz verarbeitet werden?

- Diskussionspapier, Version 1.0 vom 07.11.2023 -

Das Papier als PDF herunterladen (ca. 0,6 MB)

zur Diskussion

Inhalt (ausblenden)

Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz

- I. Ziel und Grenzen dieses Diskussionspapiers
- II. Personenbezogene Daten und der Einsatz von Künstlicher Intelligenz
- III. Phasen der Verarbeitung
 1. Erhebung von Trainingsdaten für Künstliche Intelligenz
 2. Verarbeitung von Daten für das Training von Künstlicher Intelligenz
 3. Bereitstellen von Anwendungen der Künstlichen Intelligenz
 4. Nutzung von Anwendungen der Künstlichen Intelligenz
 5. Nutzung von Ergebnissen der Künstlichen Intelligenz



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



Gliederung des Diskussionspapiers

- I. Einführung: Ziel und Grenzen des Diskussionspapiers
- II. - III. [...]
- IV. Rechtsgrundlagen für öffentliche und nicht-öffentliche Stelle
- V. Rechtsgrundlagen für nicht-öffentliche Stellen

VI. Rechtsgrundlagen für öffentliche Stellen in Baden-Württemberg

1. Öffentliches Interesse oder öffentliche Gewalt, Art. 6 Abs. 1 Buchst. e DS-GVO
2. Dienst- und Arbeitsverhältnisse, § 15 LDSG BW
3. Videoüberwachung öffentlich zugänglicher Räume, § 18 LDSG BW
4. Generalklausel für öffentliche Stellen, § 4 LDSG BW

...in Baden-Württemberg

Öffentliches Interesse oder öffentliche Gewalt, Art. 6 Abs. 1 Buchst. e DS-GVO

- Verarbeitung muss in Ausübung öffentlicher Gewalt oder im öffentlichen Interesse sein.
 - ➔ Voraussetzung ist die Übertragung einer öffentlichen Aufgabe an die verantwortliche Stelle nach dem Unionsrecht oder Recht des Mitgliedstaates.
- Gilt nur in Verbindung mit einer bestimmten Rechtsgrundlage!

- Die Weizenbaumsche Basisfrage...

„Aber wir sollten doch [bei jeder technischen Innovation] die Frage stellen:
Brauchen wir das?“

...ist auch eine datenschutzrechtliche Frage. [Erforderlichkeit]

Wir brauchen:

- Schaffung spezifischer Rechtsgrundlage[n] im [engen] Ausgestaltungskorridor zwischen DSGVO und KI-VO
- Regulatorisches Lernen [ErwG. 139 KI-VO)
- Vorbild Beratungs- und Evaluierungszentrum für Künstliche Intelligenz, BEKI - BEKI @theLänd auch für die kommunale Ebene (?)



← Post



@mikesnosense



im like the opposite of machine learning. human forgetting

[Post übersetzen](#)

6:27 vorm. · 17. Apr. 2024 · **3,4 Mio.** Mal angezeigt

<https://twitter.com/mikesnosense/status/1780453112169607404?s=12&t=YT3O9m3NcPobbjZAU-hoNw>

- <https://artificialintelligenceact.eu/de/das-gesetz/>
- [Orientierungshilfe der DSK zu Künstlicher Intelligenz und Datenschutz- \(DSK Orientierungshilfe\)](#)
- [Positionspapier zu nationalen Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz \(DSK Positionspapier\)](#)
- [Diskussionspapier Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz des LfDI Baden-Württemberg \(LfDI BW - Diskussionspapier\)](#)
- <https://www.lida.bayern.de/de/ki.html> (Checkliste KI BayLDA)
- https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/20231113_Checkliste_LLM_Chatbots_DE.pdf (Hamburger Checkliste zum Einsatz LLM-basierter Chatbots)



Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

herzog@lfdi.bwl.de