

KI sicher einsetzen

KI-Governance für Kommunen



KI sicher einsetzen

Fahrplan

- Zwischen Begeisterung und Stillstand**
- Wenn Motivation auf fehlende Regeln trifft**
- Welche Regeln für KI gelten**
- Was kommt zuerst – Technik, Recht oder Organisation**

Ein kleiner Blick zurück

Digitalagentur Sachsen & KI 2025/26

100 Beratungen, Impulse und Weiterbildungen

180 Use Cases in Workshops an der HSF entwickelt

Wöchentliche KI-Sprechstunde für KMU

KI-Podcast »Promptgenau« – Praxisnahes Wissen rund um KI

Community of Practice KI – Austausch und Vernetzung für die sächsische Verwaltung

Studien



Zwischen Begeisterung und Stillstand



Zwischen Begeisterung und Stillstand

Vom persönlichen Werkzeug zur organisationalen Aufgabe

Individuell: Generative KI ist seit ~3,5 Jahren ein echter Gamechanger

Organisational: strukturelle Trägheit, fehlende KI-Strategie und KI-Governance, Führung ohne KI-Erfahrung, Messbarkeitsproblem, kulturelle Spaltung

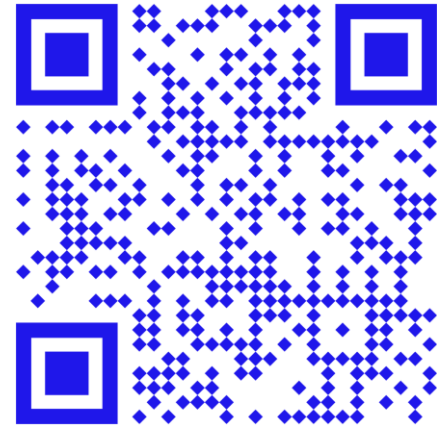
In der Verwaltung: regulatorisches Paradoxon - Herausforderungen hoch zwei

Zwischen Begeisterung und Stillstand

Vom persönlichen Werkzeug zur organisationalen Aufgabe

Haben Sie generative KI bereits ausprobiert? Also Chatbots wie ChatGPT, Mistral, Gemini ...

Link: <https://claper.sbarco.de/e/kissg>



Zwischen Begeisterung und Stillstand

Vom persönlichen Werkzeug zur organisationalen Aufgabe

Haben Sie generative KI bereits im beruflichen Kontext genutzt?

Zwischen Begeisterung und Stillstand

Vom persönlichen Werkzeug zur organisationalen Aufgabe

Macht Ihnen die Arbeit mit KI-Tools Spaß?

Zwischen Begeisterung und Stillstand

Vom persönlichen Werkzeug zur organisationalen Aufgabe

Dürfen Sie die KI-Tools offiziell im beruflichen Kontext einsetzen?

Wenn Motivation auf fehlende Regeln trifft



Wenn Motivation auf fehlende Regeln trifft

Schatten-KI

- **Schatten-KI** entsteht nicht aus böser Absicht, sondern weil Organisationen nichts bereitstellen.
- **kostenfreie Modelle** bezahlt man mit den eingegebenen Daten. Das ist heikel.
- **Licht:** Beschäftigte mit hoher intrinsischer Motivation sind eine Chance!

Wenn Motivation auf fehlende Regeln trifft

Zwischenfazit

Nichtstun ist das größte Risiko.

KI ist nicht aufzuhalten – und wir wollen das auch gar nicht.
Schatten-KI ist bereits Realität. Wer nicht gestaltet, wird gestaltet.

Welche Regeln für KI gelten



EU-Daten-Gesetzgebung im Überblick

Wichtige Rechtsakte für Daten, KI und digitale Infrastruktur | Stand 2026

Die EU-Datenregulierung besteht aus mehreren Bausteinen: Datenschutz, Datennutzung, KI-Regulierung und Cybersicherheit.

1 DSGVO Datenschutz



- Schutz personenbezogener Daten
- Rechtsgrundlagen, Betroffenenrechte, Rechenschaftspflicht
- Gilt seit 25.05.2018

2 AI Act KI-Regulierung



- Risikobasierte Regeln für KI-Systeme
- Pflichten für Anbieter, Betreiber und GPAI
- Stufenweise Anwendung seit 2025

3 Data Act Datennutzung



- Zugang zu und Nutzung von Produkt- und IoT-Daten
- Datenweitergabe, Cloud-Wechsel, B2B/B2G
- Anwendbar seit 12.09.2025

4 Data Governance Act (DGA) Datenteilung



- Datenmittlungsdienste und Datenaltruismus
- Weiterverwendung geschützter öffentlicher Daten
- Anwendbar seit 24.09.2023

5 Open Data Directive Öffentliche Daten



- Weiterverwendung von Informationen des öffentlichen Sektors
- High-Value Datasets und offene Schnittstellen
- Vor allem für den öffentlichen Sektor relevant

6 NIS2 Cybersicherheit



- Sicherheitsanforderungen und Meldepflichten
- Governance, Risikomanagement, Vorfallmeldungen
- Umsetzungsfrist 18.10.2024 - Umsetzung in DE verzögert sich

7 ePrivacy-Richtlinie Kommunikation



- Regeln für elektronische Kommunikation und Cookies
- Schutz der Vertraulichkeit von Kommunikationsdaten
- Ergänzt die DSGVO im Kommunikationsbereich

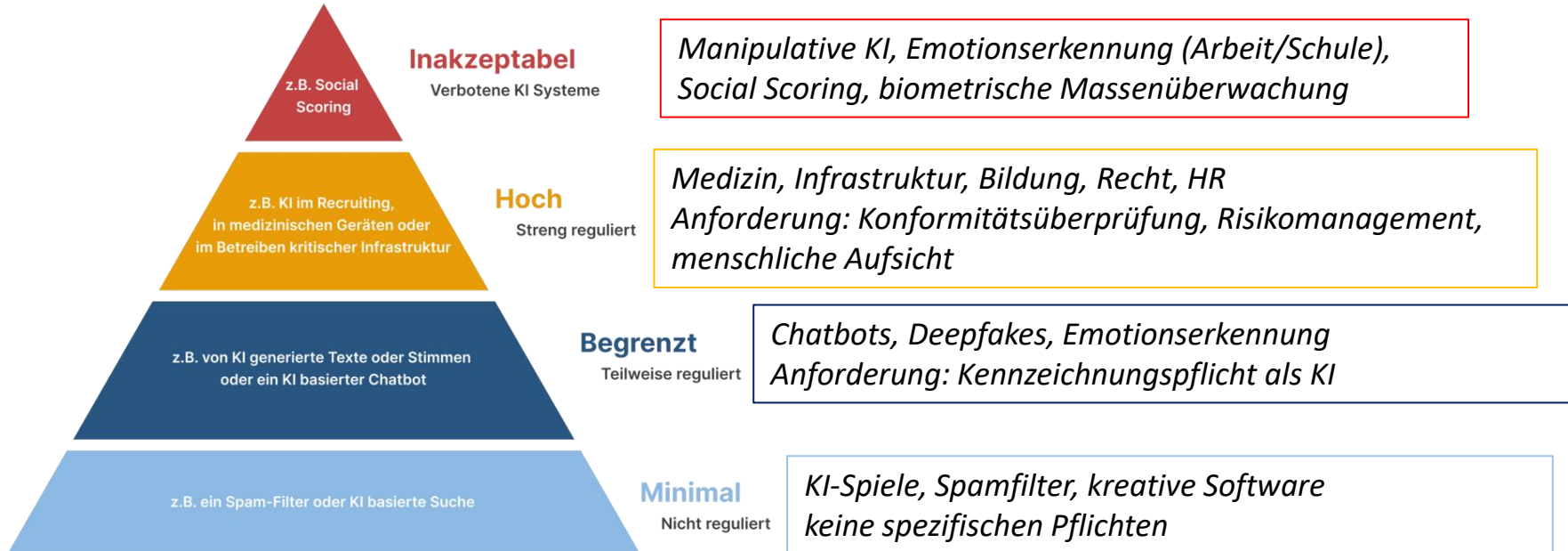


Zusammenspiel

- ✓ DSGVO schützt personenbezogene Daten.
- ✓ Data Act und DGA regeln Zugang, Teilen und Nutzung von Daten.
- ✓ Der AI Act steuert den Einsatz von KI-Systemen.
- ✓ NIS2 schützt Systeme, Prozesse und digitale Infrastruktur.

EU AI Act (KI-VO)

Risikopyramide



Quelle: <https://www.digitalhub-ai.de/>

EU AI Act (KI-VO)

Risikopyramide (KI-Systeme aus der Risikoklasse „hoch“)

1 Biometrische Identifikation



- Identifikation & Kategorisierung natürlicher Personen

2 Kritische Infrastrukturen



- Betrieb digitaler Infrastrukturen
- Energie, Wasser, Verkehr

3 Bildung und Ausbildung



- Bewertung, Beurteilung, Überwachung
- Bildung & berufliche Ausbildung

4 Beschäftigung & Personal



- Einstellung, Beförderung, Beendigung von Arbeitsverhältnissen
- Schichtpläne & Aufgabenzuteilung

5 Zugang zu Dienstleistungen



- Kreditwürdigkeit & wesentliche Dienste
- Finanzen, Versicherung, Notfall, öff. Leistungen

6 Strafverfolgung



- Polizeiliche & strafrechtliche Zwecke
- Risikobewertung, Vorhersage von Straftaten

7 Migration & Grenzkontrolle



- Asylverfahren & Grenzmanagement
- Prüfung von Visa- & Asylanträgen

8 Rechtspflege & Demokratie



- Gerichtsverfahren & demokratische Prozesse
- Urteilsfindung, Wahrheitsermittlung

EU AI Act (KI-VO)

Art. 26 – Pflichten der Betreiber von Hochrisiko-KI-Systemen

1 Technische & organisatorische Maßnahmen



Einsatz gemäß Betriebsanleitung sicherstellen

2 Menschliche Aufsicht



Kompetente, befugte Personen müssen Aufsicht übernehmen (Kompetenzpflicht)

4 Eingabedaten



Relevant & repräsentativ für den Zweck

5 Betriebsüberwachung & Meldepflichten



Laufende Überwachung des Betriebs; Vorfälle melden; Nutzung ggf. aussetzen

6 Protokolle aufbewahren



Automatische Logs ≥ 6 Monate

7 Arbeitnehmer informieren



Vor Einsatz am Arbeitsplatz

8 Registrierung



EU-Stellen: Eintrag in EU-Datenbank (Art. 71)

9 DSGVO-Folgenabschätzung



Anbieter-Infos (Art. 13) für DSFA (Art. 35)

10 Biometrische Fernidentifizierung



Bspw. Gesichtserkennung; Genehmigung ≤ 48 h; Jahresberichte

11 Information Betroffener



Über KI-Entscheidungen informieren

12 Behördenkooperation

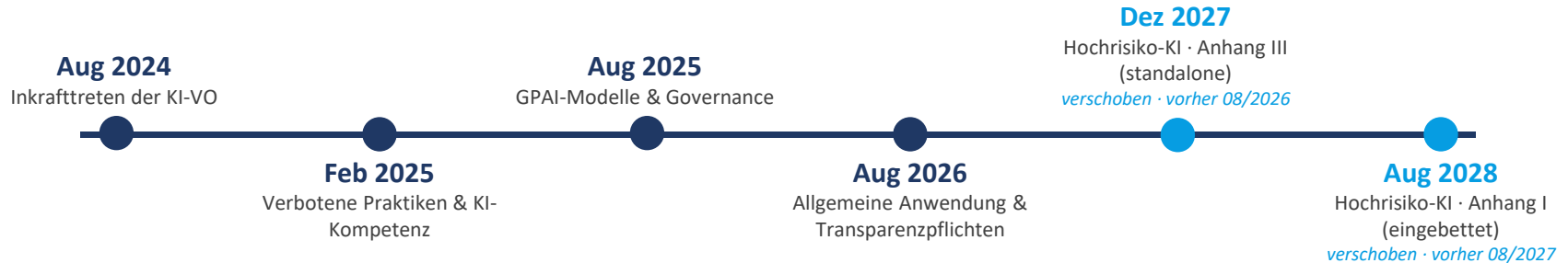


Mit zuständigen Behörden zusammenarbeiten

EU AI Act (KI-VO)

Digital Omnibus: Fristen

Gestaffelte Anwendung des AI-Acts (KI-Verordnung)



Digital Omnibus (Einigung 07.05.2026): Hochrisiko-Pflichten verschoben — **Anhang III → 02.12.2027**, **Anhang I → 02.08.2028**. Transparenz- & KI-Kompetenzpflichten gelten unverändert ab 08/2026.

Was kommt zuerst – Technik, Recht oder Organisation



Was kommt zuerst – Technik, Recht oder Organisation

Was Sie sofort tun können

1

Arbeitsgruppe bilden, Rollen besetzen, Mandat klären:

Zentrale Akteure wie Personalrat, Datenschutz, Informationssicherheit frühzeitig einbinden.



2

Bestandsaufnahme:

Welche KI-Anwendungen gibt es bereits in der Organisation? Wo wird KI informell genutzt?



3

Erste KI-Richtlinie entwerfen:

Auch als einfache Ein-Seiten-Version.



Was kommt zuerst – Technik, Recht oder Organisation

Was Sie als Nächstes angehen

4

Überblick über regulatorische Anforderungen erarbeiten:

EU-AI-Act, DSGVO etc. – Was betrifft uns?



5

Ethische Leitprinzipien:

Für die eigene Organisation diskutieren und formulieren.



6

Erste Risikobewertung:

Bestehende KI-Anwendungen prüfen und bewerten.



Was kommt zuerst – Technik, Recht oder Organisation

Was nachhaltig trägt

7

KI-Kompetenzen der Beschäftigten:

Welche Kompetenzen werden benötigt? Wie werden diese erlangt?



8

KI-Register:

Modelle, Daten, Zweck, Risiko, Verantwortlichkeiten etc. systematisch erfassen.



9

Austauschformate:

Hausleitung und Beschäftigte regelmäßig up-to-date halten.




KI sicher einsetzen

Fazit

Fangen Sie an.

Nicht unbedingt perfekt und nicht vollständig – aber anfangen! Nicht verbotsorientiert, sondern innovationsgeleitet.

Vielen Dank für Ihr Interesse!

 Thomas Schindler

 Digitalagentur Sachsen

 Kontakt: info@digitalagentur.sachsen.de

 <https://www.digitalagentur.sachsen.de/digitale-transformation.html>

