

KI-Systeme und (europäische) Regulierung:

Leitplanken für die rechtssichere Beschaffung
und Nutzung von KI

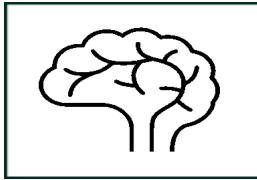
Varinia Iber | Dr. Fabian Bader

Warum KI für öffentliche Stellen rechtlich besonders relevant ist

- **KI ist bereits faktisch im Einsatz – oft schneller als die Regulierung**
 - Automatisierung von Verwaltungsprozessen
 - Entscheidungsunterstützung (z.B. Sozialleistungen)
 - Einsatz von Standard-KI (ChatGPT, Copilot) im Arbeitsalltag
- **KI im rechtlichen Kontext:**



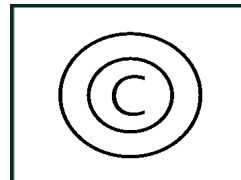
Vergaberecht



KI-Verordnung



DSGVO



Urheberrecht



Vertragsrecht

Teil 1: KI-Verordnung, Vertragsrecht, Urheberrecht und Datenschutz

KI in der öffentlichen Verwaltung: Zwei Realitäten

Klassische KI

- projektbasiert
- vergabegesteuert

vs.

Standard-KI (ChatGPT & Co.)

- SaaS-Modelle
- geringe Implementierungshürde
- oft: ad hoc Nutzung

Gleiche gesetzliche Grundlagen:

- ❖ AI Act
- ❖ DSGVO
- ❖ Vertragsrecht
- ❖ Urheberrecht



Grundlagen der KI-Regulierung

- **Liegt eine KI-System vor ? → Problem: „versteckte“ KI in IT-Produkten**
- **Welche Risikoklasse?**
 - **Verbotene KI-Praktiken** → Nutzungsverbot
 - **Hochrisiko-KI-Systeme** → volle Betreiberpflichten; ggf. Anbieterpflichten
 - **Bestimmte KI-Systeme** → Transparenzpflichten (Art. 50 KI-VO)
 - **sonstige KI-Systeme** → Schulungspflicht (Art. 4 KI-VO)
- **Welche Rolle: Anbieter vs. Betreiber ?**
 - Regelfall: Behörde = Betreiber (Art. 26 KI-VO)
 - Risiko:“Role shift“ zum Anbieter bei:
 - wesentlichen Änderungen des KI-Systems
 - eigenem Training/“Fine-Tuning“
 - Vermarktung unter eigenem Namen

KI-Verordnung als Ordnungsrahmen

Klassische KI-Beschaffung:

- (un)klare Rollenverteilung:
 - Hersteller ist Anbieter
 - Öffentliche Stelle ist Betreiber
 - ➔ aber: Gefahr des „role shift“
- Hochrisiko-KI wahrscheinlicher
 - ➔ umfangreiche Betreiberpflichten

Standard-KI

- klare Rollenverteilung
 - GPAI-Hersteller ist Anbieter (Art. 52 ff. KI-VO)
 - Öffentliche Stelle ist Betreiber
- grundsätzlich keine Hochrisiko-Einstufung
 - ➔ Aber: Nutzungskontext entscheidend
- in der Regel: Schulungspflicht und ggf. Transparenzpflichten

Kernproblem: *Abhängigkeit von Anbieter-Compliance, bei Standard-KI ohne echte Prüf- und Einflussmöglichkeit*

Datenschutz (DSGVO) im Vergleich

Klassische KI:

- klare Zwecke und definierte Datenflüsse
- Löschung und Kontrolle technisch umsetzbar
- AV-Vertrag regelmäßig möglich (bei Cloud-Lösungen)

Standard-KI

- Problem: Eingabedaten (Prompts)
- häufig keine tragfähige Rechtsgrundlage
- Drittstaatentransfer / Cloud-Intransparenz
- unklare Rollen (controller vs. processor)
- fehlende Löschkontrolle



Standard-KI = höchstes DSGVO-Risiko durch Kontrollverlust bei Dateneingabe



AV-Vertrag als Lösung? Problem: Nutzung von Eingabedaten zu Trainings-/Verbesserungszwecken

Urheberrechte: Haftungsdimension

Das Urheberrecht betrifft zwei Ebenen:

Training der Modelle

- öffentliche Stellen sind meist nicht selbst trainierend → Risiko liegt beim Anbieter
- Wenn doch: Rechtmäßigkeit der Nutzung von Trainingsdaten sicherstellen
- vertragliche Absicherung -> Freistellung

Nutzung/Verwertung von Outputs

- Öffentliche Stellen sind verantwortlich für Nutzer
→ Risiko liegt bei öffentlicher Stelle
- mögliche Rechtsverletzungen
- keine Schutzfähigkeit eigener Inhalte

Praxisproblem bei Standard-KI: kaum Einfluss auf Trainingsdaten + AGB der Anbieter meist ohne echte Absicherung

IT-Vertragsrechtliche Besonderheiten

- **KI ist kein „normales IT-Produkt“**, da KI probabilistisch, nicht deterministisch funktioniert. Durch die Funktionsweise entstehen **neue Regelungsfelder**
- Zentrale Vertragsinhalte sind
 - Zweckbindung & Einsatzgrenzen
 - Qualitätsmetriken für probabilistische Systeme
 - Trainingsdaten: Datenkategorien & Datenflüsse, Rechteinhaberschaft
 - Rechte an Output
 - Transparenzpflichten (Dokumentation des Systems / Änderungsmanagement (Model Updates))
 - Compliance (KI-Verordnung, Datenschutz)
 - Haftung & Freistellung
- **EU Modal Contractual Clauses als Standard** (modular, Differenzierung: High-Risk vs. Non-High-Risk)

Steuerung durch Vertrag

Klassische KI:

- maßgeschneiderte Verträge
 - klare Leistungsinhalte
 - Compliance-Klauseln (KI-VO, Datenschutz, Urheberrecht) möglich

Standard-KI

- Nutzung über AGB
- Risiken:
 - keine Verhandlungsmacht
 - keine Transparenz
 - keine Kontrollrechte

Fazit & Handlungsempfehlung

Klassische KI = komplex, aber steuerbar

VS.

Standard-KI = einfach, aber rechtlich riskanter


Was bedeutet das für öffentliche Stellen?

- **zentrale Beschaffung** statt Einzeltools
- **klare interne Nutzungsrichtlinien** für Standard-KI
- **vertragliche Absicherung** (wo möglich)
 - Ausschluss der Nutzung von Eingabedaten zu Training und Modellverbesserung
 - Abschluss AV-Vertrag
- **Schulung** der Mitarbeiter (Art. 4 KI-VO)

Fazit: *Nicht die KI ist das Risiko – sondern ihre ungesteuerte Nutzung.*

Teil 2: Vergaberechtliche Gestaltung der KI-Beschaffung

Leistungsbeschreibung u. Ausschreibungsbedingungen

- **Bedarfsanalyse** und **Risikobewertung**
 - **Klassifizierung** der KI-Anwendung: Hochrisiko vs. Nicht-Hochrisiko
 - Rolle Auftraggeber definieren: **Anbieter** oder **Betreiber** iSd KI-VO?
- **Verpflichtung** AN zur **KI-VO Konformität**
- **„Funktionale“ Leistungsbeschreibung** wählen
 - Autonomie u. Anpassungsfähigkeit  schwierige Erklärbarkeit der **KI-Funktionsweise**
 - Daher Beschreibung der vom KI-System **zu bewältigenden Aufgabe**
- **Verfahrensart**: Häufig Verhandlungsverfahren mit TWB / Verfahrensart mit Verhandlungsmöglichkeit


Leistungsbeschreibung u. Ausschreibungsbedingungen

- **Lernfähigkeit** von KI-Systemen begünstigt **Vendor Lock-in**
 - KI des AN wird mit Daten des öffentlichen Auftraggebers trainiert (**Wettbewerbsvorteil**)
 - ggf. **Urheberrechte** des AN an den **Trainingsdaten**
 - **Verhinderung** Vendor Lock-In, soweit **zumutbar** (EuGH, Urt. v. 09.01.2025 – C-578/23)
 - Mögliche Lösung: **Rechtssicherung** an **KI-Ergebnissen** und Verpflichtung zur Konservierung und Zurverfügungstellung von **Trainingsdaten**
- Betrachtung des gesamten **Lebenszyklus** der KI
 - Gewährleistung **vergleichbarer Angebote**
 - **Dynamik in Leistungserbringung** (Verhinderung Auftragsänderung, vgl. **132 GWB**)
- Hinweis: KI-VO-Konformität für **vor 02.08.2026 beschaffte Hochrisiko-KI-Systeme bis 02.08.2030**

Eignungskriterien

- Fokus auf **Prozesse** und **Kompetenzen**
- **Referenzen**
 - P!: Aussagekraft mit Blick auf Innovationsgrad begrenzt
 - Präzisierung **Vergleichbarkeitsanforderungen** (z. B. Sicherstellung KI-VO Konformität)
- **Spezifische Zertifizierungen für KI**
 - Aktuell noch Vieles im Fluss bzgl. spezifischer Zertifizierungen
 - ISO 42001-Zertifizierung – **Managementsystem** für künstliche Intelligenz (ethische Überlegungen, Transparenz und kontinuierliches Lernen – ähnlich ISO 27001 für IT-Sicherheit)

Angebotsprüfung und -wertung

- **Verwendung von Teststellungen → Reduzierung Intransparenz von KI**
 - Nicht technische Funktionsweise
 - sondern Leistungsfähigkeit und Funktionalität (vgl. oben)
- **Verifizierend:** Prüfung, ob angebotene Leistung festgelegte **Mindestanforderungen** erfüllt
 - Beschränkung auf Bestbieter zulässig
- **Wertend:** Erfüllung Teststellungsanforderungen als **qualitatives Zuschlagskriterium**
 - Wenn absehbar, dass Leistungsmerkmale unterschiedlich erfüllt
 - zwingende Durchführung mit allen Bietern (Dokumentation!)
 - ggf. Zurverfügungstellung Trainingsdaten durch Auftraggeber
 - Aktueller Leistungsstand als Bezugspunkt  fördert Vergleichbarkeit der Angebote