

Rechtssicher durch den KI-Dschungel:

Der rechtliche Kompass für KI-Einsatz, Tool-Auswahl und Transparenzpflichten

IPAI Heilbronn - *"KI-Zukunft gestalten: Strategie, Recht und Umsetzung für Entscheider"*

11. Juni 2026

ZIRNGIBL

RECHTSANWÄLTE PARTNERSCHAFT MBB



Vier Himmelsrichtungen

= vier rechtliche Themen

...out of many

Nord

Haftung

Ost

IP-Schutz

Süd

Verträge

West

Kennzeichnung

NORD – Haftung

- KI haftet nicht – Sie haften
 - Maßgeblich ist ihr eigenes Verschulden
 - KI ist kein Erfüllungsgehilfe
 - idR vergleichbar mit der Haftung zu Softwarenutzung
- Fünf wesentliche Haftungsebenen
 - Vertraglich
 - Deliktisch
 - Produkthaftung
 - Urheberrecht
 - DSGVO

OST – IP-Schutz

- KI-Output ist gemeinfrei
 - Kein Urheberrecht – Wettbewerber darf es übernehmen
 - Schutz nur bei substantieller menschlicher Nachbearbeitung
- Persönlichkeitsrecht
 - KI-Stimmnachahmung/Stimmklon verletzt APR
 - Biometrische Daten → Art. 9 DSGVO: Einwilligung erforderlich

SÜD – Verträge

- Urheberrechtsschutz sichern
 - Dokumentationspflicht
 - Mindestbearbeitungstiefe
 - Human in the Loop
 - Besonderheiten bei SW-Entwicklung
- **Mit fehlendem Schutz umgehen**
 - Vertraulichkeit statt Rechteübertragung – auch für gemeinfreien Output
- **Compliance und Input-Schutz**
 - Zulässige Tools
 - kein Input von Betriebsgeheimnissen , kein Training mit Kundendaten
- **Auftrags- oder projektspezifische Besonderheiten:** z.B. spezifische Haftungsklauseln, Datenschutz

WEST – Kennzeichnung Art. 50 KI-VO: Die Rollen

- Zweck und Geltung
 - Schutz vor Täuschung und Identitätsbetrug – gilt unabhängig von der Risikoklasse des KI-Systems
 - Anwendbar ab 2.8.2026 – Umsetzung jetzt!
- Anbieter (Abs. 1) – Chatbot-Kennzeichnung
 - Nutzer muss wissen, dass er mit KI interagiert (Ausnahme: Offensichtlichkeit)
 - Achtung: eigener Marketing-Chatbot → Ihr Unternehmen idR Anbieter – auch bei API-Anbindung.
- Anbieter (Abs. 2) – OpenAI, Adobe, Midjourney
 - Maschinenlesbare Markierung – unsichtbar für Menschen, Ihr Kunde sieht das nicht
- Betreiber (Abs. 4) – rgm. Ihr Unternehmen! Kennzeichnungspflicht nur in zwei Fällen:
 - Deepfake: sichtbare Offenlegung – z.B. Stimm-Klon, KI-Influencer, „KI-Models“
 - Text zu öffentlichem Interesse – Ausnahmen: menschliche Letztkontrolle, redaktionelle Verantwortung; rgm. nicht Werbetexte (Vorsicht bei Gesundheit, Verbraucherschutz, Nachhaltigkeit!)

WEST – Art. 50 KI-VO: Praxis Marketing & Werbung

- Wann liegt ein Deepfake vor? (Art. 3 Nr. 60 KI-VO)
 - Wirklichkeitsbezug entscheidend: Halten die angesprochenen Verkehrskreise den Inhalt für echt? (objektiver Maßstab)
 - (+) KI-Klon eines prominenten Influencers im Werbespot – (–) sprechende Mäuse im Käse-Spot: offensichtlich fiktional (COM-Guidelines)
- Umsetzung der Offenlegung (Abs. 5): klar, eindeutig, barrierefrei – ab erster Interaktion
 - Sichtbares Wasserzeichen, Texthinweis („KI-generiert“), Content-Credentials-Icon (cr)
 - Nicht ausreichend: Hinweis nur in AGB oder Metadaten, unklare Begriffe („Assistent“)
- Praxisfall: KI-generierter LinkedIn-Artikel
 - Gesellschaftlicher Diskurs = öffentliches Interesse → Art. 50 Abs. 4 S. 2 greift
 - Ausnahme redaktionelle Kontrolle: für Einzelpersonen idR (–), sog. Medienprivileg → Offenlegung erforderlich
- Rechtsfolgen bei Verstößen
 - Bußgeld bis 15 Mio. € bzw. 3 % des weltweiten Jahresumsatzes (Art. 99 Abs. 4 lit. g KI-VO)
 - UWG-Risiko: Abmahnungen durch Wettbewerber und Verbände – Sonderfall „AI Washing“

„Darf ich das Tool überhaupt nutzen?“

- These: Die Spielregeln sind nicht neu – KI-Tool = Cloud-Software
 - US-Anbieter, Drittlandtransfer, AVV, TOMs, Geheimnisschutz –bekannt aus M365, SaaS & Co.
 - Wer Daten auf SharePoint ablegt, hat die Grundsatzfragen längst beantwortet
- Aber: Unterschiede zum klassischen SaaS
 - Black Box: Trainingsnutzung und Datenflüsse schwerer nachvollziehbar als reine Datenablage
 - Risiko verlagert sich zur Eingabe: nicht korrigierbar
 - Konnektoren (z.B. M365): Vollzugriff statt punktueller Freigabe – kaum zu orchestrieren
- Verschärfte Maßstäbe im Einzelfall
 - Berufsgeheimnisträger (§ 203 StGB)
 - Geschäftsgeheimnisse (GeschGehG)

Toolauswahl: Vom AVV bis zur Datensouveränität

- **Vertragliches Fundament: AVV/DPA**
 - AVV/DPA abschließen – idR nur bei Bezahl- und Enterprise-Modellen; Vorsicht bei Gratisversionen (Training!)
 - DPAs genau lesen: z.B. Anthropic-DPA erfasst zumindest aktuell keine besonderen Kategorien (Art. 9 DSGVO: z.B. Gesundheitsdaten) – „Special categories: None“
- **Konfiguration: Schutzniveau aktiv erhöhen**
 - Trainingsnutzung deaktivieren/verifizieren, Aufbewahrungsfristen minimieren, Zero Data Retention, EU-Datenresidenz
 - Konnektoren-Rechte minimieren, Memory-/Sharing-Funktionen prüfen, SSO/Rollen, Audit-Logs
 - Geheimnisschutz: sorgfältige Konfiguration = „angemessene Geheimhaltungsmaßnahme“ (§ 2 GeschGehG)
- **Organisation: steuern statt hoffen**
 - Nutzungsrichtlinie und Schulung (KI-Kompetenz, Art. 4 KI-VO): Welche Daten dürfen hinein?
- **Wenn das zu unsicher ist: souveräne Alternativen**
 - Hyperscaler: AWS Bedrock, Vertex AI, Azure – EU-Region, kein Training; AWS European Sovereign Cloud (1/2026); aber: EU-Region ≠ Souveränität (CLOUD Act)
 - DE/EU-Stack –STACKIT (Schwarz Digits),T-Systems, IONOS

Vielen Dank!

ZIRNGIBL

RECHTSANWÄLTE PARTNERSCHAFT MBB

München

Karlstraße 23
80333 München
+49 (89) 290 50-0
munich@zirngibl.de

Berlin

Kurfürstendamm 194
10707 Berlin
+49 (30) 880 331-0
berlin@zirngibl.de

Frankfurt

Bethmannstraße 8
60311 Frankfurt am Main
+49 (69) 589 99 58-0
frankfurt@zirngibl.de

