

# KI & RECHT: NICHT JEDE REGEL GILT IMMER.

Rechtliche Anforderungen richten sich nach dem konkreten KI-Einsatz – nicht nach dem Hype.

## VOM USE CASE ZUR RECHTSSICHEREN UMSETZUNG

### 1 USE CASE VERSTEHEN



Wo soll KI eingesetzt werden?

Welchen Prozessschritt unterstützt oder ersetzt sie?

### 2 DATEN & PERSONEN



Welche Daten werden verarbeitet?

Sind personenbezogene Daten betroffen?

### 3 RISIKO EINSCHÄTZEN



Welche Auswirkungen hat der Einsatz?

Fehler, Diskriminierung, Sicherheit, Grundrechte?

### 4 ROLLE BESTIMMEN



Sind wir Anbieter, Betreiber oder Nutzer?

Davon hängen viele Pflichten ab.

### 5 ANFORDERUNGEN ABLEITEN



Welche Gesetze, Standards und Pflichten sind relevant?

### 6 UMSETZEN & DOKUMENTIEREN



Maßnahmen umsetzen, verantworten und nachweisen.

Regelmäßig überprüfen und verbessern.

## WELCHE RAHMENWERKE SIND WANN RELEVANT?



### EU AI ACT

Wann relevant?

Bei Entwicklung, Bereitstellung oder Nutzung von KI-Systemen.

Worauf kommt es an?

- Risikoklasse des KI-Systems (minimal, begrenzt, hoch, unzulässig)
- Transparenz & Kennzeichnung
- Daten-Governance
- Human-in-the-Loop
- Dokumentation & Protokollierung
- AI Literacy (Pflicht seit 02.02.2025)



Gestaffelte Anwendung:

ab 02.02.2025 erste Pflichten, vollumfänglich ab 02.08.2026.



### DSGVO

Wann relevant?

Sobald personenbezogene Daten verarbeitet werden.

Worauf kommt es an?

- Rechtsgrundlage
- Zweckbindung & Datenminimierung
- Transparenz & Betroffenenrechte
- Datenschutz-Folgenabschätzung (bei hohem Risiko)
- Auftragsverarbeitung



Sehr häufig in KI-Projekten relevant.



### ISO/IEC 27001

Wann relevant?

Wenn Informationssicherheit strukturiert gemanagt werden soll oder muss.

Worauf kommt es an?

- Risikomanagement für Informationssicherheit
- Zugriffsschutz & Kryptografie
- Betriebssicherheit
- Lieferanten- & Dienstleistermanagement



Wichtig für Nachweise gegenüber Kunden, Partnern & Behörden.



### ISO/IEC 42001

Wann relevant?

Wenn KI im Unternehmen systematisch gesteuert und verantwortungsvoll eingesetzt werden soll.

Worauf kommt es an?

- KI-Governance & Verantwortlichkeiten
- Risiko- & Impact-Management
- Transparenz & Nachvollziehbarkeit
- Messung & kontinuierliche Verbesserung
- Ethische Grundsätze



Hilft, KI-Governance professionell aufzubauen und nachzuweisen.



### NIS2

Wann relevant?

Für Unternehmen in kritischen oder wichtigen Sektoren (18 Sektoren in der EU).

Worauf kommt es an?

- Cybersicherheits-Risikomanagement
- Vorfallmeldung
- Lieferketten-Sicherheit
- Technische & organisatorische Maßnahmen



Relevant, wenn KI in kritischen Umgebungen eingesetzt wird.



### GOLDENE REGEL:

Compliance beginnt nicht mit Angst, sondern mit einem sauber verstandenen Use Case.



### MERKE:

Nicht jede KI ist automatisch „hoch riskant“. Aber jeder KI-Einsatz braucht eine saubere Einordnung.

S · A · I · S  
SUCCESSFUL AI SOLUTIONS

Vom ersten Gedanken bis zum messbaren Mehrwert.