

KI-Governance Checkliste

In 15-30 Minuten prüfen Sie die wichtigsten Punkte für einen sicheren, nachvollziehbaren und wirtschaftlich sinnvollen KI-Einsatz.

20

CHECKPUNKTE

4

BEREICHE

15-30

MINUTEN REVIEW

● 1) Rechtlich & Compliance



Verantwortlichkeiten definiert

Wer entscheidet, wer prüft, wer gibt frei: Rollen sind klar zugeordnet.



DSGVO-Rechtsgrundlagen geprüft

Zweck, Rechtsgrundlage und Nachweise sind dokumentiert und für Audits auffindbar.



Haftungsrisiken eingeordnet

Kritische Risiken in Prozessen und Kommunikation sind benannt und priorisiert.



Provider-Verträge geprüft

AVV/DPA, Speicherort und Trainingsnutzung durch Anbieter sind eindeutig geklärt.



EU-AI-Act-Relevanz vorgeprüft

Die Risiko-Klasse ist grob eingeordnet und die nächsten Pflichten sind bekannt.

● 2) Daten & Zugriff

☐ **Datenfluss dokumentiert**

Sie wissen, welche Daten intern bleiben und welche Systeme extern eingebunden sind.

☐ **Unerwünschtes Modell-Training ausgeschlossen**

Opt-out/Enterprise-Settings sind aktiv und intern verbindlich kommuniziert.

☐ **Lösch- und Aufbewahrungslogik definiert**

Prompts, Uploads, Logs und Exportdaten haben klare Regeln.

☐ **Zugriffsrechte geregelt**

Rollen, MFA/SSO und API-Key-Handling verbindlich festgelegt.

☐ **Datenklassifizierung umgesetzt**

Vertraulichkeitsstufen definiert und in KI-Nutzung übersetzt.

Praxis-Hinweis: Bei sensiblen Daten sind lokale oder private Deployments meist der robusteste Weg.

● 3) Technik & Betrieb

☐ **Lokale/private Optionen bewertet**

On-Prem/Self-Hosted-Varianten für sensible Daten geprüft.

☐ **API-Sicherheit umgesetzt**

Key-Storage, Rotation, Scopes und Secrets-Handling sauber gelöst.

☐ **Fallbacks vorhanden**

Ausfall-Szenarien dokumentiert, manuelle Alternativen definiert.

☐ **Monitoring aktiv**

Kosten, Nutzung, Latenz und Fehler werden gemessen und bewertet.

☐ **Output-Validierung definiert**

Verbindliche Qualitäts- und Freigaberegeln für kritische Inhalte.

Rote Linie: Keine KI-Kommunikation nach außen ohne klaren Review- und Freigabeprozess.

● 4) Organisation & Adoption

☐ Nutzungsrichtlinien kommuniziert

Klare Do's/Don'ts für Teams sind dokumentiert, freigegeben und aktiv kommuniziert.

☐ Schulungsplan vorhanden

Mitarbeitende werden in Nutzung, Risiken und Qualitätssicherung strukturiert geschult.

☐ Feedback- und Eskalationswege definiert

Fehler, Halluzinationen und Sonderfälle werden strukturiert gemeldet.

☐ Regelmäßige Reviews eingeplant

Nutzwert, Risiken und Änderungen werden in festen Intervallen überprüft.

☐ Verantwortliche Multiplikatoren benannt

Power-User unterstützen Teams in der operativen Anwendung.

Rote Linien

Keine sensiblen Kundendaten ohne Freigabe in öffentliche Tools, keine unklaren Datenflüsse, keine KI-Ausgaben ohne Qualitätskontrolle.

Benjamin Mühlauer - 3C: Content Creation, Coaching & Consulting

E-Mail: info@bm-mail.de | Telefon: +49 152 223 114 72

Hinweis: Diese Checkliste ist Praxis-Orientierung und ersetzt keine Rechtsberatung.