# Die 4 Säulen einer sicheren & wirksamen KI-Einführung

\*\*Neukunden-Dossier\*\* · Stand: 2025-09-25

## Executive Summary

- \*\*Pragmatisch\*\*: Wir starten dort, wo Sie heute stehen – mit klar priorisierten Quick Wins und einem realistischen Maßnahmenplan.

- \*\*Rechtssicher\*\*: DSGVO-konform, EU AI Act-ready – mit dokumentierter Governance, Rollen und Prozessen.

- \*\*Sicher\*\*: Schutz vor Datenabfluss, Prompt-Leaks, Schatten-IT und Modellrisiken – inklusive Richtlinien & Schulungen.

- \*\*Wirtschaftlich\*\*: Fokus auf Effizienz, Qualität und messbaren Nutzen – von Automatisierung bis Wissensmanagement.

- \*\*Förderfähig\*\*: Wir prüfen passende Förderprogramme und übernehmen auf Wunsch die Antragsskizze.

## Die 4 Säulen Ihrer KI-Readiness

### 1) Governance & Compliance

\*\*Ziel:\*\* Rechtssichere, nachvollziehbare und auditierbare KI-Nutzung im Unternehmen.

\*\*Quick-Check:\*\*

- Gibt es eine \*\*KI-Richtlinie\*\* (Policies) und klare \*\*Rollen & Verantwortlichkeiten\*\*?

- Ist dokumentiert, \*\*welche Daten\*\* in welche \*\*KI-Tools\*\* fließen (inkl. Auftragsverarbeitung, TOMs)?

- Sind \*\*Risikoklassen\*\* (EU AI Act) bewertet und \*\*Folgenabschätzungen\*\* (z. B. DSFA) durchgeführt?

- Gibt es \*\*Protokollierung\*\*, \*\*Versionierung\*\* und \*\*Freigabeprozesse\*\*?

\*\*Typische Risiken:\*\* Schatten-IT, intransparente Datenflüsse, ungeklärte Rechtsgrundlagen, fehlende Dokumentation.

\*\*Ihre Maßnahmen / Deliverables:\*\*

- KI-Richtlinie & \*\*Responsible-AI-Prinzipien\*\* (inkl. Daten- & Prompt-Richtlinie)

- \*\*Register\*\* für KI-Anwendungen und Datenflüsse

- \*\*Vorlagen\*\*: DPIA/DSFA, Einwilligungen, TOMs, Auftragsverarbeitung

- \*\*Compliance-Check\*\* EU AI Act / DSGVO (inkl. Gap-Analyse & Prioritäten)

### 2) Sicherheit & Risiko-Management

\*\*Ziel:\*\* Risiken minimieren, Vorfälle vermeiden, Resilienz erhöhen.

\*\*Quick-Check:\*\*

- Gibt es Schutz vor \*\*Datenabfluss\*\* (z. B. PII, Kundendaten) und \*\*Prompt-Leaks\*\*?

- \*\*Modell- & Toolbewertung\*\*: Anbieter-Risiken, Logging, Residency, Exportkontrolle?

- \*\*Red Teaming / Abuse Testing\*\* etabliert?

- Notfallpläne (\*\*Incident Response\*\*), Monitoring & Audits vorhanden?

\*\*Typische Risiken:\*\* Jailbreaks, Prompt-Injection, Data Leakage, fehlerhafte Ausgaben (Halluzination), Supply-Chain-Risiken.

\*\*Ihre Maßnahmen / Deliverables:\*\*

- \*\*Threat-Modeling\*\* für KI-Use-Cases

- \*\*Sicherheits-Checkliste\*\* (z. B. für Chatbots, Agenten, Retrieval, Automationen)

- \*\*Musterprozesse\*\* für Vorfallmanagement und Retrospektiven

- \*\*Awareness-Training\*\* inkl. Fallbeispielen und Do/Don’t-Poster

### 3) Nutzen & Prozesse (Use Cases & Operating Model)

\*\*Ziel:\*\* Schneller, messbarer Mehrwert – mit sauberem Betriebsmodell.

\*\*Quick-Check:\*\*

- Welche \*\*Prozesse\*\* eignen sich für \*\*Automatisierung\*\* (z. B. Text, Bild, Audio, Daten)?

- Gibt es ein \*\*Priorisierungsraster\*\* (Impact vs. Aufwand, Risiko vs. Reife)?

- \*\*Eval & QA\*\*: Wie stellen Sie Qualität, Nachvollziehbarkeit und kontinuierliche Verbesserung sicher?

- \*\*Toolchain\*\*: Passende Systemauswahl, Integrationen und Rechtekonzepte?

\*\*Typische Hürden:\*\* Ideenfriedhof ohne Umsetzung, Insel-Lösungen, fehlende Metriken.

\*\*Ihre Maßnahmen / Deliverables:\*\*

- \*\*Use-Case-Backlog\*\* inkl. Wirtschaftlichkeitsrechnung (ROI/TCO)

- \*\*Umsetzungsfahrplan\*\*: Pilot → Rollout → Betrieb

- \*\*Quality-Gates\*\*: Prompts, Tests, Evals, Human-in-the-Loop

- \*\*Vorlagen\*\*: Briefings, Prompt-Libraries, Review-Checklisten

### 4) Befähigung & Kultur (Enablement & Change)

\*\*Ziel:\*\* Teams, die sicher, souverän und kreativ mit KI arbeiten.

\*\*Quick-Check:\*\*

- \*\*Rollenprofile\*\* (z. B. Prompt-Specialist, KI-Owner, Data Steward) definiert?

- \*\*Trainingspfade\*\* und Lernformate vorhanden?

- \*\*Kommunikation\*\*: Transparenz, Feedback, Erfolgsgeschichten?

- \*\*Ethik & Leitplanken\*\* alltagsnah verankert?

\*\*Ihre Maßnahmen / Deliverables:\*\*

- \*\*Schulungen & Mikro-Learnings\*\* (rollenbasiert)

- \*\*Onboarding-Paket\*\* für neue Tools (How-to, Fail-safes, Beispiele)

- \*\*Kommunikations-Kit\*\* (Townhall-Folien, FAQ, Poster)

- \*\*Change-Plan\*\* mit Meilensteinen & KPIs

## Methode & Ergebnisdokumente

1. \*\*KI-Readiness-Check (online)\*\* – strukturierter Fragebogen mit Score.

2. \*\*Kick-off & Discovery\*\* (½–1 Tag) – Prioritäten, Risiken, Datenflüsse.

3. \*\*Audit & Proofs\*\* – Richtlinien, Prozesse, Use Cases, Sicherheit.

4. \*\*Maßnahmenplan\*\* – Quick Wins (30–60 Tage) + Roadmap (6–12 Monate).

5. \*\*Abschluss & „Gamechanger“-Idee\*\* – eine visionäre Empfehlung für den nächsten großen Sprung.

\*\*Sie erhalten:\*\* Readiness-Report (PDF), Governance-Paket (Vorlagen), Sicherheits-Checklisten, Use-Case-Backlog, Roadmap, Trainingskonzept.

## Förderungen (optional)

Wir prüfen passende Programme (z. B. für Digitalisierung/Innovation) und unterstützen bei \*\*Antragsskizze\*\* und \*\*Projektstruktur\*\*. Details sind regional und zeitlich unterschiedlich – wir beraten transparent und aktuell.

## Beispiel: Start in 6 Wochen

- \*\*Woche 1:\*\* Kick-off, Fragebogen, Datenfluss-Sichtung

- \*\*Woche 2–3:\*\* Governance & Security Baseline, Quick-Wins live

- \*\*Woche 4–5:\*\* Use-Case-Pilots mit Eval & QA

- \*\*Woche 6:\*\* Maßnahmenplan, Trainings, „Gamechanger“

## Häufige Fragen (FAQ)

\*\*Brauchen wir sofort eine große Plattform?\*\* Nein. Starten Sie klein mit klaren Policies und zwei bis drei gut gewählten Use Cases.

\*\*Wie vermeiden wir Fehlentscheidungen?\*\* Mit einem strukturierten Priorisierungsraster und Quality-Gates.

\*\*Ist das datenschutzkonform?\*\* Ja – mit korrekter Rechtsgrundlage, Verträgen, TOMs, und dokumentierten Verfahren.

\*\*Wie nehmen wir das Team mit?\*\* Rollenspezifische Trainings, klare Kommunikation und leichtgewichtige Leitplanken.

## Nächste Schritte

1. 30‑minütiges \*\*Erstgespräch\*\* (kostenfrei)

2. \*\*Readiness-Check\*\* (online)

3. \*\*Kick-off\*\* mit Prioritäten-Workshop

\*\*Kontakt:\*\*

\*\*Wolf Hohl – Zertifiziertes KI-Management\*\*

Web: ki-sicherheit.jetzt · ki-foerderung.jetzt

E-Mail: kontakt@ki-sicherheit.jetzt