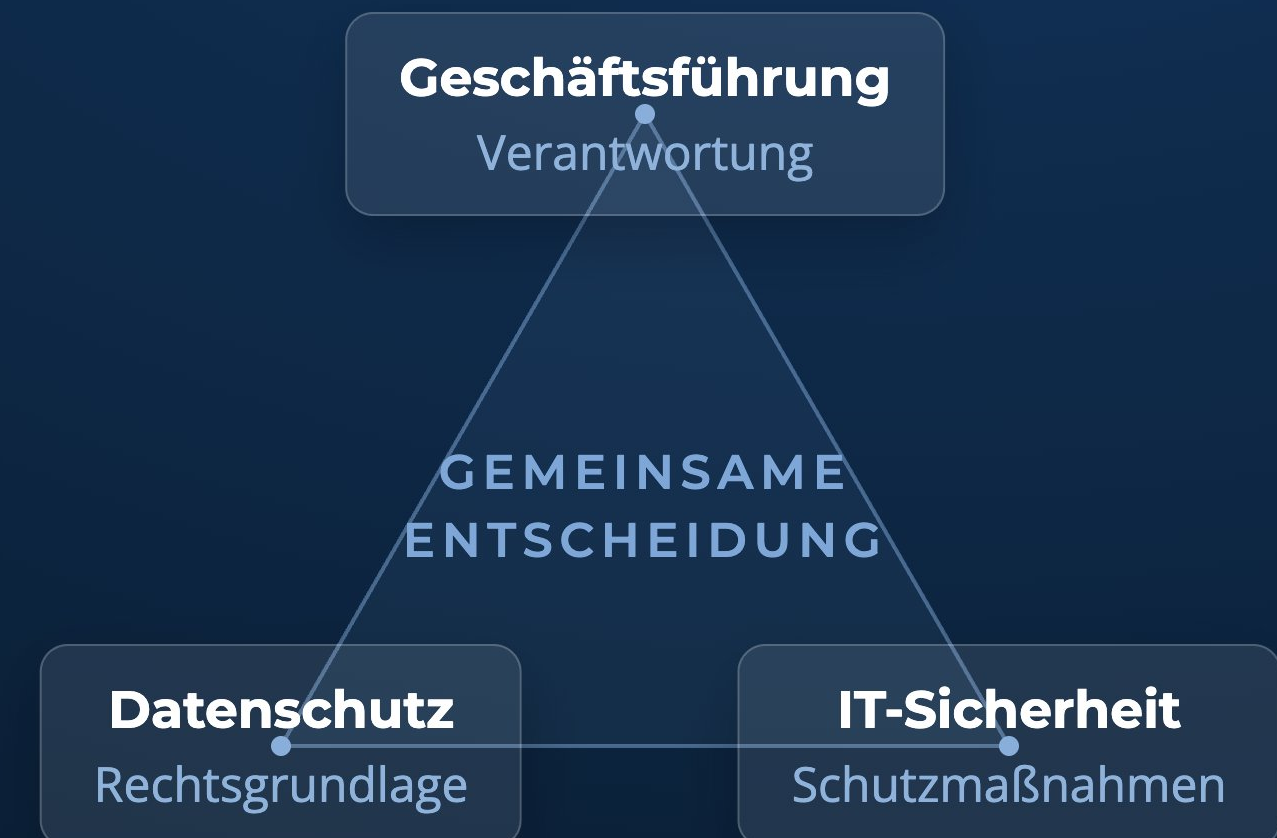


Datenschutz & Governance bei KI-Projekten

KI-Projekte sind Führungsaufgabe — nicht nur ein IT-Thema.

- KI verarbeitet Kunden-, Mitarbeiter-, Vertrags- und Betriebsdaten.
- Datenschutz, Sicherheit und Fachbereich entscheiden gemeinsam.
- Ohne Governance: Schatten-KI, Datenabfluss, Haftungsrisiken.



Die DSGVO bleibt die Basis

02

Der EU AI Act ersetzt den Datenschutz nicht — er kommt zusätzlich hinzu.

- Zweckbindung, Datenminimierung, Rechtsgrundlage und Transparenz gelten weiter.
- KI-Modelle mit personenbezogenen Trainingsdaten sind nicht automatisch anonym.
- Besonders kritisch: Kunden-, Mitarbeiter-, Gesundheits- und Bewerberdaten.

Quelle: EDPB Opinion 28/2024; EU AI Act.

04 Interne Richtlinien
Freigaben, Rollen, Nutzungsregeln



03 EU AI Act
Risikobasierte Pflichten



02 IT-Sicherheit
Zugriff, Verschlüsselung, Protokolle



01 DSGVO — Fundament
Rechtsgrundlage jeder Verarbeitung

Der AI Act verändert die Projektprüfung

Unternehmen müssen risikobasiert bewerten, welche KI sie einsetzen.

- Verbotene KI-Praktiken gelten bereits seit Februar 2025.
- Pflichten für General-Purpose- und Hochrisiko-KI greifen stufenweise.
- Mittelständler sind selten Anbieter — meist „Deployer“ von KI-Systemen.

Quelle: Europäische Kommission, AI Act Framework.

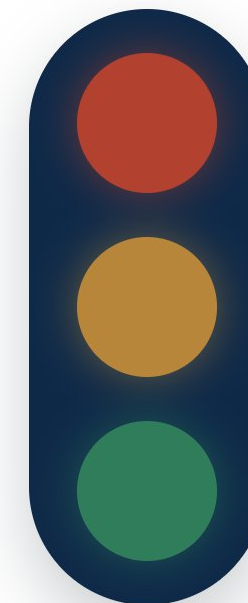


Welche Daten dürfen in die KI?

Nicht jede Information gehört in Prompts, Trainingsdaten oder Wissensdatenbanken.

- Vor der Nutzung: klare Datenklassen definieren.
- Verträge, Personalakten und Betriebsgeheimnisse gesondert behandeln.
- Standardregel: so wenig personenbezogene Daten wie möglich.

Quelle: BfDI & DSK — Datenschutzprüfung vor KI-Einsatz.



Rot — Personenbezogen & vertraulich

Nur mit Rechtsgrundlage und Prüfung

Gelb — Interne Fachdaten

Nur in freigegebenen, sicheren Systemen

Grün — Öffentliche Inhalte

Weitgehend unkritisch nutzbar

Schatten-KI ist das größte Praxisrisiko

Ohne sichere Lösung nutzen Mitarbeiter oft ungeprüfte Tools.

- Typisch: Chatbots für Kundentexte, Bewerbungen, Verträge, Protokolle.
- Risiko: vertrauliche Inhalte verlassen unkontrolliert das Unternehmen.
- Lösung: erlaubte Tools, verbotene Daten und Freigabewege festlegen.

SICHERE KI-NUTZUNG — RAHMENWERK

- ✓ **Erlaubte Tools**
Freigegebene, geprüfte Anwendungen
- ✓ **Erlaubte Datenarten**
Klare Grenzen nach Datenampel
- ✓ **Freigabeprozess**
Wer gibt neue Anwendungsfälle frei?
- ✓ **Protokollierung**
Nachvollziehbarkeit der Nutzung
- ✓ **Schulung**
Mitarbeiter sicher befähigen

Wer darf was mit welcher KI tun?

KI braucht Rollen, Berechtigungen und nachvollziehbare Entscheidungen.

Rolle	Verantwortung	Strategie	Auswahl	Betrieb	Kontrolle
Geschäftsführung	Leitplanken & Risikobereitschaft	A	A	I	I
Fachbereich	Zweck, Nutzen & fachliche Richtigkeit	C	R	A	R
IT	Sicherheit & Datenverarbeitung	C	R	R	C
Datenschutz	Zulässigkeit, Verträge & Rechte	C	C	C	A
Einkauf	Beschaffung & Anbietersteuerung	I	R	I	I

Anbieterprüfung ist Pflicht, nicht Formalie



Der Anbieter entscheidet über Datenschutz, Verfügbarkeit und Haftung mit.

- Prüfen: Serverstandort, Auftragsverarbeitung, Subunternehmer, Trainingsnutzung.
- Prüfen: Logging, Löschkonzept, Exportfähigkeit, Berechtigungen.
- Bei sensiblen Daten: EU-Hosting, private Instanzen oder lokale KI.

LIEFERANTEN-SCORECARD Bewertung 1-5

Datenschutz
Standort, AVV, Trainingsnutzung ○ ○ ○ ○ ○

Sicherheit
Logging, Verschlüsselung, Rechte ○ ○ ○ ○ ○

Vertrag
AVV, Haftung, SLA ○ ○ ○ ○ ○

Betrieb
Verfügbarkeit, Support, Löschung ○ ○ ○ ○ ○

Exit
Export, Migration, Datenrückgabe ○ ○ ○ ○ ○

Human Oversight bleibt entscheidend

**KI darf Entscheidungen vorbereiten —
kritische Entscheidungen nicht unkontrolliert
treffen.**

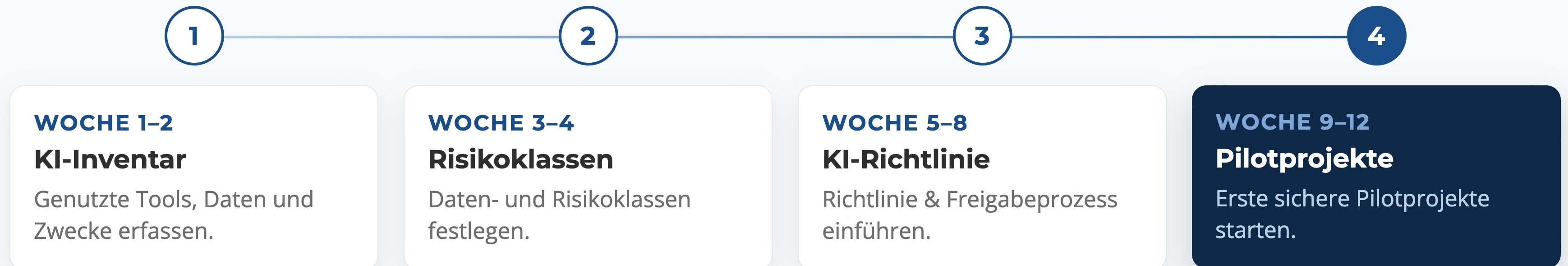
- Relevant bei Personal, Kundenbewertung, Kredit, Compliance, Medizin, Sicherheit.
- Fachliche Kontrolle fest im Prozess verankern.
- Ergebnisse bleiben prüfbar, korrigierbar und dokumentierbar.

Quelle: AI Act — menschliche Aufsicht, Monitoring, Protokollierung bei Hochrisiko-KI.



Empfohlener 90-Tage-Fahrplan

Gute KI-Governance lässt sich pragmatisch starten.



Datenschutz & Governance bremsen KI nicht — sie machen KI einsatzfähig.

WEG A — STATUS QUO

Ungesteuerte Toolnutzung zulassen

Schatten-KI, unkontrollierter Datenabfluss und Haftungsrisiken.

VS

WEG B — EMPFEHLUNG

Kontrollierte KI-Fähigkeit aufbauen

Sofortmaßnahme: KI-Richtlinie, Toolfreigabe und Datenampel — produktive Nutzung bei reduziertem Risiko.

NÄCHSTER SCHRITT

KrambergAI KI-Governance-Check durchführen und Maßnahmen priorisieren.



KrambergAI
krambergai.com