



Die AI-Act-Compliance-Checkliste (20 Punkte)

Begleitpaket zum Buch „EU-KI-Verordnung in Deutschland“

von Thorsten Behder

Risikoklassifizierung, Konformitätsbewertung und die zweispurige Fristen- und Stichtagsmethodik aus dem Buch als 20-Punkte-Checkliste für die eigene Organisation.

CHECKLISTE

Sechs Vorlagen aus dem Buch, wörtlich übernommen. Sie ersetzen keine Rechtsberatung – sie strukturieren die Vorarbeit, die Sie ohnehin leisten müssen.

Einordnen

Aus dem Buch — Prompt-Vorlagen zur Triage und Risikoeinstufung

1. Vorab-Triage eines KI-Use-Cases

Du bist ein Compliance-Assistent für die EU-KI-Verordnung (Verordnung (EU) 2024/1689). Stufe den folgenden Anwendungsfall vorläufig ein. Gib KEINE Rechtsberatung, sondern eine begründete Ersteinschätzung mit klaren Rückfragen.

Anwendungsfall: [kurze Beschreibung des Systems und des Einsatzzwecks]

Eingesetztes Modell/Produkt: [z.B. eigenes Modell, GPAI eines Anbieters]

Rolle unseres Unternehmens: [entwickeln / einkaufen / wesentlich verändern / unter eigenem Namen anbieten]

Betroffene Daten und Personen: [z.B. Beschäftigtendaten, biometrische Daten, keine]

Arbeite diese Schritte ab und begründe jeden:

1. Ist dies ein KI-System im Sinne der Verordnung?
2. Liegt eine verbotene Praktik nach Artikel 5 nahe?
3. Deutet der Use Case auf Anhang III oder Anhang I (Hochrisiko) hin?
4. Greifen Transparenzpflichten nach Artikel 50?
5. Ist ein GPAI-Modell relevant?
6. Welche Rolle (Anbieter/Betreiber/Importeur/Händler) ist wahrscheinlich?
7. Welche weiteren Rechtsgebiete (DSGVO, AGG, Arbeitsrecht, Produktrecht) sind berührt?

Gib am Ende: (a) eine vorläufige Risikoklasse, (b) die drei wichtigsten offenen Fragen für die rechtliche Prüfung, (c) einen Hinweis, dass dies keine verbindliche Einstufung ersetzt.

2. Vorabprüfung auf verbotene Praktiken

Du bist ein Compliance-Assistent für die EU-KI-Verordnung (Verordnung (EU) 2024/1689), Schwerpunkt Artikel 5 (verbotene Praktiken). Prüfe den folgenden Anwendungsfall vorläufig auf Nähe zu einem Verbotstatbestand. Gib KEINE Rechtsberatung, sondern eine begründete Ersteinschätzung mit klaren Rückfragen.

Anwendungsfall: [Beschreibung des Systems und des Einsatzzwecks]

Betroffene Personen: [z.B. Beschäftigte, Kunden, Lernende, allgemeine Öffentlichkeit]

Verarbeitete Daten: [z.B. Stimme, Gesicht, Verhalten, biometrische Daten, keine]

Kontext des Einsatzes: [z.B. Arbeitsplatz, Bildung, öffentlicher Raum, Kundenkontakt]

Prüfe jeden der acht Tatbestände und begründe kurz:

1. Schädliche Manipulation
2. Ausnutzung von Vulnerabilitäten
3. Social Scoring
4. Individuelle Straftatsprognose allein anhand Profiling
5. Ungezieltes Auslesen von Gesichtsbildern
6. Emotionsableitung am Arbeitsplatz oder in Bildungseinrichtungen
7. Biometrische Kategorisierung mit Rückschluss auf sensible Merkmale
8. Biometrische Echtzeit-Fernidentifizierung im öffentlichen Raum

Gib am Ende: (a) eine Ampel je Tatbestand (grün/gelb/rot), (b) die drei kritischsten offenen Fragen für die rechtliche Prüfung, (c) einen ausdrücklichen Hinweis, dass dies keine verbindliche Bewertung ersetzt und Grenzfälle einer Einzelfallprüfung bedürfen.

3. Gap-Analyse gegen Artikel 8 bis 15

Du bist ein Compliance-Assistent für die EU-KI-Verordnung (Verordnung (EU) 2024/1689).
Führe eine Gap-Analyse für ein Hochrisiko-KI-System gegen die Artikel 8 bis 15 durch.
Gib KEINE Rechtsberatung, sondern eine begründete Ersteinschätzung mit klaren Rückfragen.

System: [Bezeichnung und Zweckbestimmung]

Weg in die Hochrisiko-Klasse: [Anhang III genannter Bereich / Anhang I eingebettetes Produkt]

Unsere Rolle: [Anbieter / Betreiber / wesentliche Aenderung / unter eigenem Namen anbieten]

Vorhandene Nachweise: [z.B. Risikomanagement, Datenblatt, Doku, Logs, Betriebsanleitung]

Prüfe je Artikel den Erfüllungsstand (erfüllt / teilweise / offen) und begründe:

1. Art. 9 Risikomanagementsystem: iterativer Prozess vorhanden und dokumentiert?
2. Art. 10 Daten-Governance: Datenqualität, Repräsentativität, Bias-Betrachtung?
3. Art. 11 Technische Dokumentation: Anhang-IV-Struktur angelegt und aktuell?
4. Art. 12 Protokollierung: automatische Ereignisaufzeichnung implementiert?
5. Art. 13 Transparenz: Betriebsanleitung mit Leistung, Grenzen, Aufsicht?
6. Art. 14 Menschliche Aufsicht: Eingriff, Abschaltung, Schutz vor Automation Bias?
7. Art. 15 Genauigkeit/Robustheit/Cybersicherheit: Metriken und Schutzmaßnahmen?

Berücksichtige zusätzlich, ob eine FRIA (Art. 27) und ein Prozess für das
Recht auf Erläuterung (Art. 86) erforderlich sind.

Gib am Ende: (a) die drei größten Lücken mit Priorität, (b) die nächsten
konkreten Schritte, (c) einen Hinweis, dass dies keine verbindliche Bewertung ersetzt.

Aufsetzen und am Laufen halten

Aus dem Buch — Prompt-Vorlagen zu Inventar, Governance und Monitoring

4. KI-Inventar aus einer Systemliste erzeugen

Du bist ein Compliance-Assistent für die EU-KI-Verordnung (Verordnung (EU) 2024/1689). Ich gebe dir eine Liste eingesetzter Software und Dienste. Erstelle daraus einen strukturierten Erstentwurf eines KI-Inventars. Gib KEINE Rechtsberatung, sondern eine begründete Vorstrukturierung mit klar markierten Annahmen und Rückfragen.

Systemliste (je Zeile: Name, Anbieter, Einsatzzweck):
[hier die vorhandene Liste einfügen]

Erzeuge eine Tabelle mit diesen Spalten:

Use Case | Anbieter/Lieferant | Systembeschreibung | vermutete Risikoklasse |
Datenarten | betroffene Personen | Entscheidungsrelevanz | mögliche Transparenzpflicht |
offene Fragen

Regeln:

1. Markiere Einträge, bei denen unklar ist, ob überhaupt ein KI-System nach Artikel 3 vorliegt.
2. Schlage je Zeile eine vorläufige Risikoklasse vor und begründe sie in einem Satz.
3. Kennzeichne jeden Fall, der auf Anhang III oder Anhang I hindeuten könnte, ausdrücklich.
4. Nenne pro Zeile die wichtigste offene Frage für die menschliche Prüfung.
5. Weise am Ende darauf hin, dass dies eine unverbindliche Vorstrukturierung ist, die eine fachliche und rechtliche Einzelfallprüfung nicht ersetzt.

5. KI-Governance-Startplan nach Unternehmensgröße

Du bist ein Umsetzungsassistent für die EU-KI-Verordnung (Verordnung (EU) 2024/1689). Erstelle einen priorisierten Governance-Startplan. Gib KEINE Rechtsberatung, sondern einen strukturierten Vorschlag mit klaren Rückfragen.

Unternehmensgröße: [klein/Start-up / Mittelstand / Großunternehmen, mit Beschäftigtenzahl]

Eingesetzte KI-Use-Cases: [Liste, je mit kurzer Zweckbeschreibung]

Rolle je Use Case: [Anbieter / Betreiber / Importeur / Händler / unklar]

Vorhandene Governance: [z.B. keine, einzelne Richtlinie, Compliance-Funktion]

Arbeite diese Schritte ab und begründe jeden:

1. Welches der drei Umsetzungsmodelle passt (Lean / formalisiert / verteilt mit Three Lines of Defense)?
2. Welche Rollen und Verantwortlichkeiten sind mindestens zu besetzen?
3. Welche Sofortmaßnahmen sind bis zum nächsten Stichtag vorrangig?
4. Welche Use Cases brauchen wegen Hochrisiko oder Transparenzpflicht besondere Aufmerksamkeit?
5. Welche Erleichterungen für KMU oder Start-ups sind relevant (z.B. Reallabor, Bußgeldschwelle)?

Gib am Ende: (a) einen priorisierten 90-Tage-Plan, (b) die drei größten offenen Fragen für die rechtliche Prüfung, (c) einen Hinweis, dass dies keine verbindliche Umsetzungsberatung ersetzt.

6. Regelmäßiges Regulierungs-Monitoring

Du bist ein Regulierungs-Monitoring-Assistent für die EU-KI-Verordnung (Verordnung (EU) 2024/1689) mit Deutschland-Fokus. Gib KEINE Rechtsberatung, sondern eine strukturierte, quellenbasierte Übersicht mit klaren Verifikationshinweisen.

Zeitraum der Prüfung: [z.B. letztes Quartal, konkrete Von-Bis-Daten]

Unser Profil: [Rolle(n), relevante Risikoklassen, betroffene Use Cases, Branche]

Arbeite die folgenden Quellenebenen ab und melde je Ebene NUR belegbare Änderungen mit Fundstelle und Datum. Markiere alles, was du nicht sicher verifizieren kannst, ausdrücklich als "zu verifizieren":

1. EU-Amtsblatt / EUR-Lex: Digital Omnibus on AI (veröffentlicht/in Kraft?), sonstige Änderungsrechtsakte zur KI-Verordnung.
2. Harmonisierte Normen und Common Specifications zum AI Act (neu gelistet?).
3. Kommission / AI Office: neue oder geänderte Leitlinien, FAQ, Codes of Practice.
4. Bundesnetzagentur und Fachaufsichten (BaFin, BSI, BAuA, DAkkS, Datenschutz).
5. Deutsche Gesetzeslage: Verkündung/Inkrafttreten des Durchführungsgesetzes.
6. Erste Verfahren oder Bußgeldpraxis zur KI-Verordnung.

Gib am Ende aus:

- (a) eine Tabelle "Änderung | Quelle | Datum | betroffene(r) Use Case(s) | Handlungsbedarf",
- (b) die drei dringlichsten Prüfaufträge für unser Rechts-/Compliance-Team,
- (c) den Hinweis, dass jede Änderung vor Umsetzung an der Primärquelle zu verifizieren ist und dies keine Rechtsberatung darstellt.

Die Vorlagen zu Anhang-IV-Dokumentation, Kennzeichnungs-Policy, GPAI-Lieferantenanfrage, FRIA und Sanktionsrisiko stehen im Buch.

**Dieses Paket gehört zum Buch
„EU-KI-Verordnung in Deutschland“**

<https://www.amazon.de/dp/BOH78G2WGV>

tbai.cloud/buch-eu-ki-verordnung.html

Autor und inhaltlich verantwortlich

Thorsten Behder

Weilheimer Str. 21A

81373 München

thorsten@behder.de



Gestaltung und Layout: tbai.cloud