KAPITEL 4

Wer haftet — Compliance als organisatorische Architektur

> *EU AI Act und DSGVO machen Haftung zur Konstruktionsfrage. Wer das ignoriert, baut ein Risiko statt eines KI-Systems. Dieses Kapitel zeigt, wie die Frage Wer haftet so früh gestellt wird, dass die Antwort tragend bleibt — pro Modul, mit Namen, Unterschrift und Versicherungsdeckung.*

Der EU AI Act ist im August 2024 in Kraft getreten. Die meisten Maschinenbau-Hersteller in Bayern und Baden-Württemberg haben sein volles Gewicht noch nicht gespürt — die Übergangsfristen für die meisten Hochrisiko-Kategorien sind in der aktiven Phase oder treten in naher Zukunft in sie ein. Mit ihrem Ablauf werden die Regeln verbindlich, mit Sanktionen bis zu 30 Millionen Euro oder 6 Prozent des globalen Jahresumsatzes, je nachdem, was höher ist.

Die Frage *Wer haftet* gehört zur Konstruktion, und nicht zur juristischen Nachbearbeitung. In den meisten Projekten wird sie zu spät gestellt, an Stellen, wo das Architekturfenster bereits geschlossen ist. Dieses Kapitel beschreibt, wie man die Frage so früh stellt, dass die Antwort tragend bleibt.

EU AI Act in der Praxis: Hochrisiko-Klassifikation, Dokumentationspflichten, verantwortliche Personen

Der Regulierungstext nennt eine konkrete Liste. Für den industriellen DACH-Kontext sind drei Kategorien am relevantesten.

Produktsicherheit. KI-Systeme, die Sicherheitskomponenten von Produkten sind, die unter bestehende EU-Regulierungsregimes fallen — Maschinenrichtlinie (Verordnung 2023/1230), Medizinprodukteverordnung, Aviation Safety Regulation. Wenn ein KI-System die Sicherheit eines Endprodukts in irgendeiner Weise beeinflusst, ist es mit hoher Wahrscheinlichkeit hochriskant.

Kritische Infrastruktur. KI-Systeme zur Steuerung von Wasserversorgung, Energie, Verkehr. Für Industriebetriebe, die Teil kritischer Infrastruktur sind, bedeutet das zusätzliche Auflagen.

Beschäftigung und Personalführung. Systeme zur Rekrutierungsunterstützung, Leistungsbewertung, Aufgabenzuteilung oder zum Monitoring. Jedes KI-System, das Entscheidungen über Mitarbeiter beeinflusst, muss sorgfältig geprüft werden.

Für Hochrisiko-Systeme verlangt der EU AI Act ein Risikomanagement-System vor der Inbetriebnahme, Datenqualitätsmanagement für Trainingssets, technische Dokumentation gemäß Anhang IV, automatische Protokollierung, Transparenz für Endanwender, menschliche Aufsicht — genau hier kommt die 30-Prozent-Schicht zum Tragen — sowie Genauigkeit, Robustheit und Cybersicherheit.

Und entscheidend für den industriellen Kontext: eine klare Definition von *Provider* und *Deployer*. Der Provider entwickelt das System oder bringt es in den Markt. Der Deployer setzt es ein. Beide tragen Pflichten. Zwischen ihnen kann eine vertragliche Zuordnung der Haftung bestehen — der Regulator schaut auf beide Seiten.

Stuart Russell formuliert in *Human Compatible* die allgemeine Regel: Die Verantwortung für ein autonomes System braucht einen institutionellen Träger, bevor das System in den Markt geht. Kate Crawford ergänzt in *Atlas of AI*, dass dieser Träger nie eine rein technische Rolle ist — er ist immer in

eine regulatorische, vertragliche und organisatorische Architektur eingebettet. Der EU AI Act schreibt damit fest, was ohnehin gilt: Zwischen Modell und Markt muss eine benannte Person mit Mandat stehen.

Verantwortungs-Mapping pro Modul: wer unterschreibt was, wann, mit welcher Versicherung

In realen Projekten ist Haftung selten monolithisch. Ein typisches KI-System besteht aus mehreren Komponenten, jede mit eigener Haftungskette.

Modell. Wer ist Provider? Bei einem zugekauften Modell — der Lieferant. Bei einem eigentrainierten — das eigene Haus. Bei einem nachtrainierten Fremdmodell teilt sich die Verantwortung, und die Details hängen vom Lizenzvertrag ab.

Infrastruktur. Wo lebt das Modell? On-premises — eigene Verantwortung für Verfügbarkeit und Sicherheit. In der Cloud — geteilte Verantwortung, wobei die Deployer-Pflicht nach dem EU AI Act dadurch nicht kleiner wird.

Integration. Wer hat das Modell in die Produktivumgebung integriert? Ein externer Integrator? Die eigene IT? Welche Integrationsdokumentation existiert?

Betrieb. Wer führt das System täglich? Das ist der KI-Operator — und er muss in der Compliance-Dokumentation namentlich genannt sein.

Das praktische Werkzeug dafür ist eine Verantwortungsmatrix pro Modul, eine RACI-Variante für KI (Responsible — führt aus, Accountable — verantwortet das Ergebnis, Consulted — wird konsultiert, Informed — wird informiert). Jede Zeile dokumentiert für ein Modul: wer Responsible ist, wer Accountable, wer unterzeichnet und welche Versicherung das Modul abdeckt. Kein bürokratischer Selbstzweck. Die Matrix liefert die Antwort auf die Frage *wer unterschreibt* in dem Moment, in dem etwas schiefgegangen ist. Etwas geht immer schief.

RACI-Matrix für ein KI-System: eine Zeile pro Modul

Modul	R	A	C	I	Versicherung
Modell	Data-Team	CTO	Compliance	CEO	Cyber + E&O
Daten (Training)	Data-Curator	DPO	Legal	CTO	DSGVO-Police
Infrastruktur	IT-Ops	CTO	CISO	CFO	Cyber-Police
Integration	Integrator	Head of IT	QA	CTO	Vendor-SLA
Betrieb	KI-Operator	Process-Owner	Compliance	CEO	D&O + E&O

R — führt aus · A — verantwortet das Ergebnis — eine Rolle pro Zeile
C — wird konsultiert · I — wird informiert

Beispiel einer ausgefüllten RACI-Matrix für ein typisches Hochrisiko-KI-System im industriellen DACH-Kontext. Jedes Modul (jede Zeile) hat genau einen Accountable; die übrigen Rollen folgen der tatsächlichen Kompetenz. Die Spalte „Versicherung" nennt den Policentyp, der Vorfälle im jeweiligen Modul deckt: Cyber + E&O (Errors and Omissions), DSGVO-Police, D&O (Directors and Officers), Vendor-SLA. Ein leeres Feld ist ein struktureller Defekt. Die Norm ISO/IEC 42001 (AI Management System Standard) erweitert die klassische RACI um die Pflicht, die Namen der Rollenträger zu dokumentieren, nicht nur die Positionen.

Schein-Souveränität (Sovereign-Washing): warum „EU-Cloud" selten Haftungsbefreiung bedeutet

Sovereign-Washing ist eine Marketingpraxis, die im DACH-Raum häufiger wird. Cloud-Anbieter bewerben eine *DSGVO-konforme EU-Cloud* oder *souveräne KI* und suggerieren, dass diese Etiketten die Haftungsfrage des Kunden lösen.

Das tun sie nicht.

Die Deployer-Pflicht nach dem EU AI Act ist standortunabhängig. Wer Deployer eines Hochrisiko-KI-Systems ist, trägt Deployer-Pflichten — egal ob das Rechenzentrum in München, Paris oder Dublin steht. *EU-Cloud* heißt, dass Daten innerhalb der EU gespeichert werden. Das kann die DSGVO-Compliance bei Datenübermittlungen erleichtern. Es ändert nichts daran, wer für die Ergebnisse des Systems haftet.

Der Auftragsverarbeitungsvertrag (AVV) mit einem Cloud-Anbieter macht diesen zum Auftragsverarbeiter, der nach Weisung handelt. Geht etwas schief, wendet sich der Regulator zuerst an den Verantwortlichen — also an das eigene Haus. Ein Regress gegen den Anbieter mag bestehen; das ist das Problem des Kunden, nicht das des Regulators.

Ein separates Risiko ist die Verfügbarkeit. *EU-sovereign-Cloud* bedeutet oft, dass die regionale Infrastruktur von einer US-Muttergesellschaft kontrolliert wird. In einem Szenario geopolitischer Spannung oder erweiterter Sanktionen kann diese *souveräne* Cloud unzugänglich werden — aus rechtlichen, nicht aus technischen Gründen.

> *Kein Zertifikat, kein Auftragsverarbeitungsvertrag und kein Marketing-Etikett über „Souveränität“ oder „EU-Konformität“ ersetzt eine eigene Compliance-Architektur mit klar benannten verantwortlichen Personen.*

Werkzeug: einseitiges Verantwortungsdiagramm pro KI-Prozess

Das nützlichste Compliance-Werkzeug in realen Projekten ist kein 200-Seiten-Bericht. Es ist eine A4-Seite, die für jeden KI-Prozess fünf Fragen beantwortet: Klassifikation nach dem EU AI Act, verantwortliche Personen (Provider, Deployer, KI-Operator, Compliance Officer), menschliche Eingriffs-

punkte und Eskalationsschwellen, Dokumentationsverweise, Versicherungsdeckung.

Eine Seite. Nicht weil das Thema einfach wäre — das ist es nicht. Sondern weil ein Verantwortungsdiagramm, das niemand liest, keine Verantwortungsklarheit erzeugt. Eine Seite zwingt zur Entscheidung. Ein 200-Seiten-Bericht erlaubt das Gegenteil.

Verantwortungsdiagramm — ein KI-Prozess, eine Seite

1. Klassifizierung
EU AI Act: hohes Risiko (Art. 6 + Anhang III) / begrenzt / minimal
Begründung · Unterschrift

2. Verantwortliche Personen
Provider: _____ Deployer: _____
KI-Operator: _____ Compliance Officer: _____

3. Menschliche Eingriffspunkte
Eskalationsschwellen · wer die Übersteuerung autorisiert
wer Entscheidungen protokolliert

4. Dokumentation
Anhang IV · Protokolle · Risikomanagement-Akte · Vorfallsregister

5. Versicherungsdeckung
Police · Limits · Ausschlüsse · wer im Vorfall anspruchsberechtigt ist

Struktur des Verantwortungsdiagramms für einen KI-Prozess (ein Workload, ein Produktstrom). Reihenfolge des Ausfüllens: (1) Klassifizierung nach dem EU AI Act — beim Abschluss des Piloten, vor der Entscheidung über den Produktivbetrieb; (2) verantwortliche Personen — in der Planungsphase, vor Entwicklungsbeginn; (3) menschliche Eingriffspunkte — in der Entwurfsphase, vor Training und Integration; (4) Dokumentation — wächst laufend, finalisiert zum Go-live; (5) Versicherungsdeckung — vor dem Go-live. Jeder leere Block wirkt als verdecktes Risiko: Verantwortung existiert strukturell erst, wenn alle Positionen benannte Träger mit ausformuliertem Mandat haben. Adaptiert nach Materialien des EU AI Act Implementation Toolkit (European Commission, Joint Research Centre) und RACI-Schemata der ISO/IEC 42001.

Drei Fragen für den eigenen Kontext

1. **Klassifikation.** Welche der eigenen KI-Prozesse fallen unter Hochrisiko nach dem EU AI Act? Existiert für jeden eine schriftliche Klassifikation mit Begründung — und wer hat sie unterschrieben?

2. **Modul-Mapping.** Existiert eine Verantwortungsmatrix, die für jedes Modul (Modell, Daten, Infrastruktur, Integration, Betrieb) Provider, Deployer und Versicherungsdeckung benennt? Wenn nicht: Welche Module wären besonders kritisch?

3. **Test auf Schein-Souveränität.** Welche Compliance-Behauptungen der eigenen Cloud- oder KI-Lieferanten beruhen auf Marketing-Etiketten und nicht auf vertraglich zugesicherten, prüfbaren Pflichten? Was passiert mit der eigenen Haftung, wenn deren *EU-Cloud* aus rechtlichen Gründen ausfällt?