EU AI Act (KI-VO) / Risikoklassen, Transparenz, Governance

A. Normen- & Struktur-Kurzliste

I. Grundnormen & Begriffe

- **Art. 2 KI-VO** – Anwendungsbereich
- **Art. 3 Nr. 1 KI-VO** – KI-System (Ableitung + Output + Umweltwirkung)
- **Art. 3 Nr. 12 KI-VO** – Zweckbestimmung (entscheidend für Risikoklasse)

Wichtig für den Mockup: Ohne Ableitung + Außenwirkung **kein KI-System**, damit **keine unmittelbare Anwendbarkeit**.

II. Risikoklassen

- **Art. 5 KI-VO** – Verbotene KI-Praktiken
- **Art. 6 KI-VO i.V.m. Anhang III** – Hochrisiko-KI
- **Art. 50 KI-VO** – Transparenzpflichten (begrenztes Risiko)
- **Art. 6 Abs. 3 KI-VO** – Systeme mit geringem/minimalem Risiko

3. Governance & Pflichten (nur antizipiert)

- **Art. 9–15 KI-VO** – Systemanforderungen (Hochrisiko)
- **Art. 26 KI-VO** – Betreiberpflichten
- **Art. 27 KI-VO** – Grundrechte-Folgenabschätzung
- **Kapitel VII (Art. 64 ff.)** – Aufsichts- & Governance-Architektur

B. Hintergrundmemo

I. Rolle des EU AI Act im AI Case Sprint

Der EU AI Act ist **keine reine Technikregulierung**, sondern eine **ex-ante Governance- und Organisationsverordnung**, die bereits **vor** Produktivsetzung steuernd wirken soll.

Sprint-Logik: Nicht „Compliance bauen“, sondern **prüfen, ob ein Use Case unter realistischen Annahmen regulatorisch tragfähig wäre**.

II. Kein KI-System im Mockup – aber maßgeblich für das Zielbild

1. Warum der Mockup nicht unter die KI-VO fällt

Nach Art. 3 Nr. 1 KI-VO setzt ein KI-System voraus:

- maschinengestützte Ableitung,
- autonome Funktionsweise,
- Outputs mit Einfluss auf physische oder virtuelle Umgebungen.

Der Mockup:

- trifft keine Entscheidungen,
- erzeugt keine Ableitungen,
- entfaltet keine Wirkung.

Kein KI-System, keine Pflichten (so auch die einhellige Auffassung in der Literatur).

2.Warum der EU AI Act trotzdem zwingend mitzudenken ist

Die **Zweckbestimmung** entscheidet über die Risikoklasse – nicht die technische Raffinesse.

Der Mockup definiert:

- Zweck,
- Rollen,
- Entscheidungslogik.

Damit prägt er **die spätere regulatorische Einordnung**.

III. Risikoklassifizierung im Legal-/Compliance-Kontext

1. Hochrisiko-KI: klare Negativabgrenzung

Hochrisiko liegt nur vor, wenn:

- Einsatz in Anhang-III-Bereichen **oder**
- Sicherheitskomponente regulierter Produkte.

Die Literatur stellt klar:

- **Nicht jede KI im KRITIS-Umfeld ist Hochrisiko-KI**
- Entscheidend ist die **funktionale Nähe zu Grundrechts- oder Sicherheitsrisiken** .

Für Legal/Compliance:

- keine biometrische Identifikation,
- keine Bewertung natürlicher Personen,
- keine operative Steuerung kritischer Infrastruktur.

IdR kein Hochrisiko-System.

2. Typische Einordnung: geringes oder begrenztes Risiko

Rechts- und Compliance-KI fällt regelmäßig unter:

- **Art. 6 Abs. 3 KI-VO** (Vorbereitung menschlicher Entscheidungen)
- oder **Art. 50 KI-VO** (Transparenzpflichten bei Interaktion)

Diese Einordnung wird in mehreren Beiträgen ausdrücklich als **intendierter Anwendungsfall der KI-VO** beschrieben.

IV. Transparenz – der zentrale Steuerungshebel

Die Literatur ist hier ungewöhnlich einhellig: **Transparenz ist der niedrigschwelligste, aber wirkungsmächtigste Pflichtanker der KI-VO** .

1. Transparenz bedeutet nicht „Erklärung des Modells“

Sondern:

- klare Kennzeichnung von KI-Einsatz,
- verständliche Beschreibung der Funktionslogik,
- eindeutige Abgrenzung Mensch / KI.

Transparenz = **Governance-Instrument**, kein Technik-Deep-Dive.

2. Mockup-Implikationen

Der Mockup sollte sichtbar machen:

- „KI-unterstützt“ statt „KI-entscheidet“
- Zweck & Grenzen
- menschliche Letztverantwortung

Damit wird **Art. 50 KI-VO antizipiert**, ohne ihn auszulösen.

V. Governance: eigentlicher Schwerpunkt des EU AI Act

1. KI-VO als Organisationsrecht

Die kritische Literatur hebt hervor: Der AI Act reguliert primär über:

- Dokumentation,
- Selbstzertifizierung,
- Organisations- und Kontrollpflichten und weniger über materiellen Grundrechtsschutz .

Für Unternehmen bedeutet das: **Governance-Versagen ist das eigentliche Risiko**, nicht Technik.

2. Anschlussfähigkeit an bestehende Compliance

Raspé/Flöter zeigen überzeugend:

- KI-Compliance lässt sich **bruchfrei in bestehende CMS integrieren**
- insbesondere entlang **IDW PS 980** (Risiken, Kontrollen, Überwachung) .

Für Trianel:

- Legal/Compliance wird **Governance-Owner**,
- nicht KI-Entwickler.

VI. Leitplanken für den Mockup

Der Mockup sollte **explizit zeigen**:

- Klare Zweckbestimmung (kein Scope-Creep)
- Bewusst niedrige Risikoklasse
- Menschliche Entscheidung immer final
- Transparenz über KI-Einsatz
- Dokumentations- & Prüfpfade
- Keine autonome Außenwirkung

Genau diese Konstellation wird in der Literatur als **„regulatorisch beherrschbar“** beschrieben .

VII. Kurzfazit

- **KI-VO = EU AI Act**
- Der Mockup unterfällt **nicht** der KI-VO, prägt aber die spätere Einordnung.
- Legal-/Compliance-KI ist **regelmäßig kein Hochrisiko-System**, wenn sie:
  - unterstützend,
  - transparent,
  - menschlich kontrolliert bleibt.
- Governance & Zweckklarheit sind die **entscheidenden Stellschrauben**.