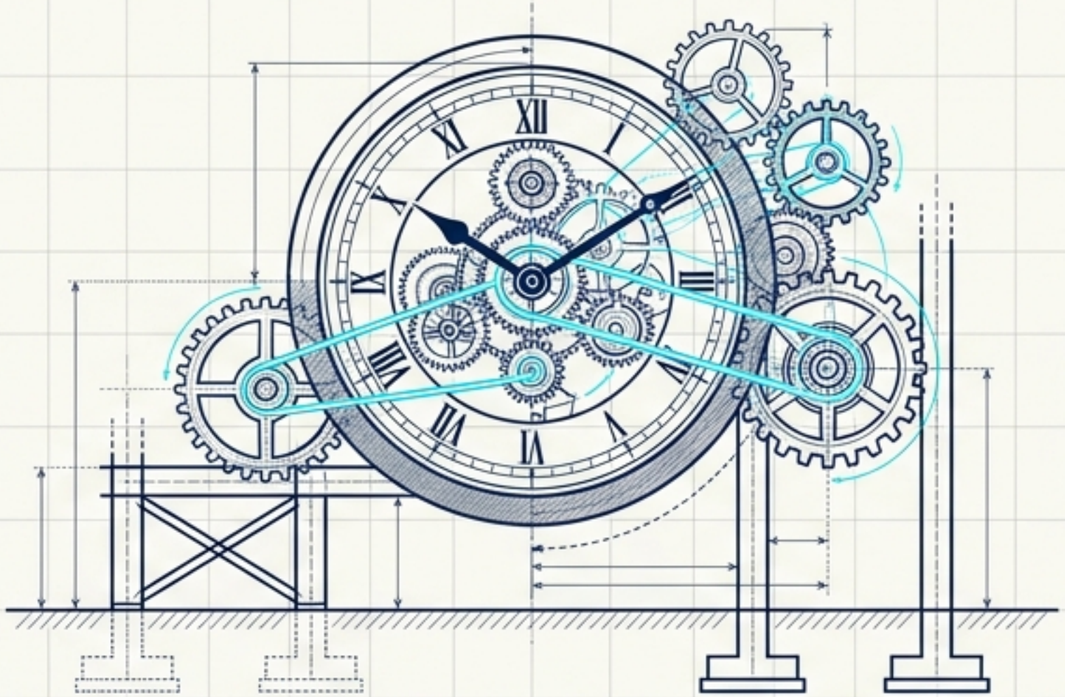
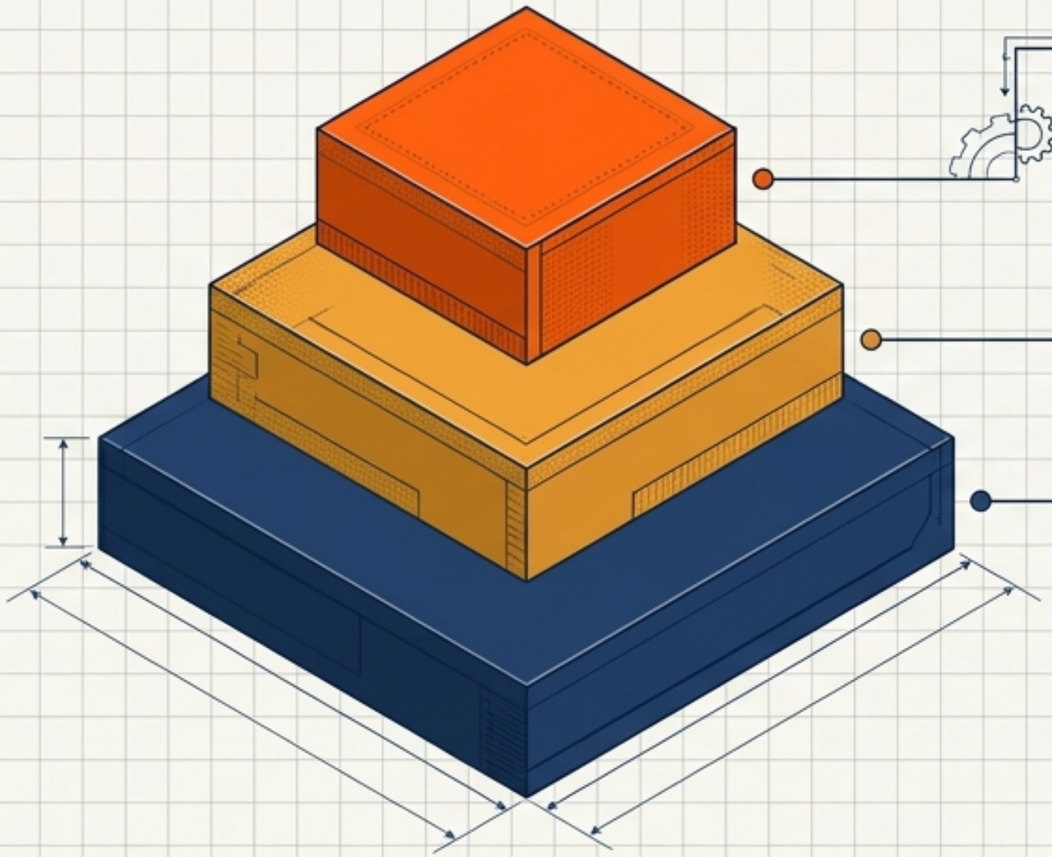
Der trügerische Aufschub

Ein strategischer Blueprint zur Corporate AI Governance nach dem Digital Omnibus Deal 2026



Orientierung für C-Level, Compliance und HR – Wie Sie die verschobenen Fristen des EU AI Acts für den Aufbau echter technologischer Souveränität nutzen.

Die Bußgeld-Kaskade des AI Acts



35 Mio. € oder 7% des Weltjahresumsatzes

Verbotene KI-Praktiken (Art. 5)

- Beispiele: Social Scoring, unzulässige biometrische Praktiken, manipulative KI, neue Nudifier-Verbote.

15 Mio. € oder 3% des Weltjahresumsatzes

Verstoß gegen sonstige Pflichten

- Beispiele: Einsatz von Hochrisiko-KI ohne Risikomanagement, mangelnde Transparenz, fehlerhafte Dokumentation (z.B. in HR-Systemen).

7,5 Mio. € oder 1% des Weltjahresumsatzes

Formelle Verstöße

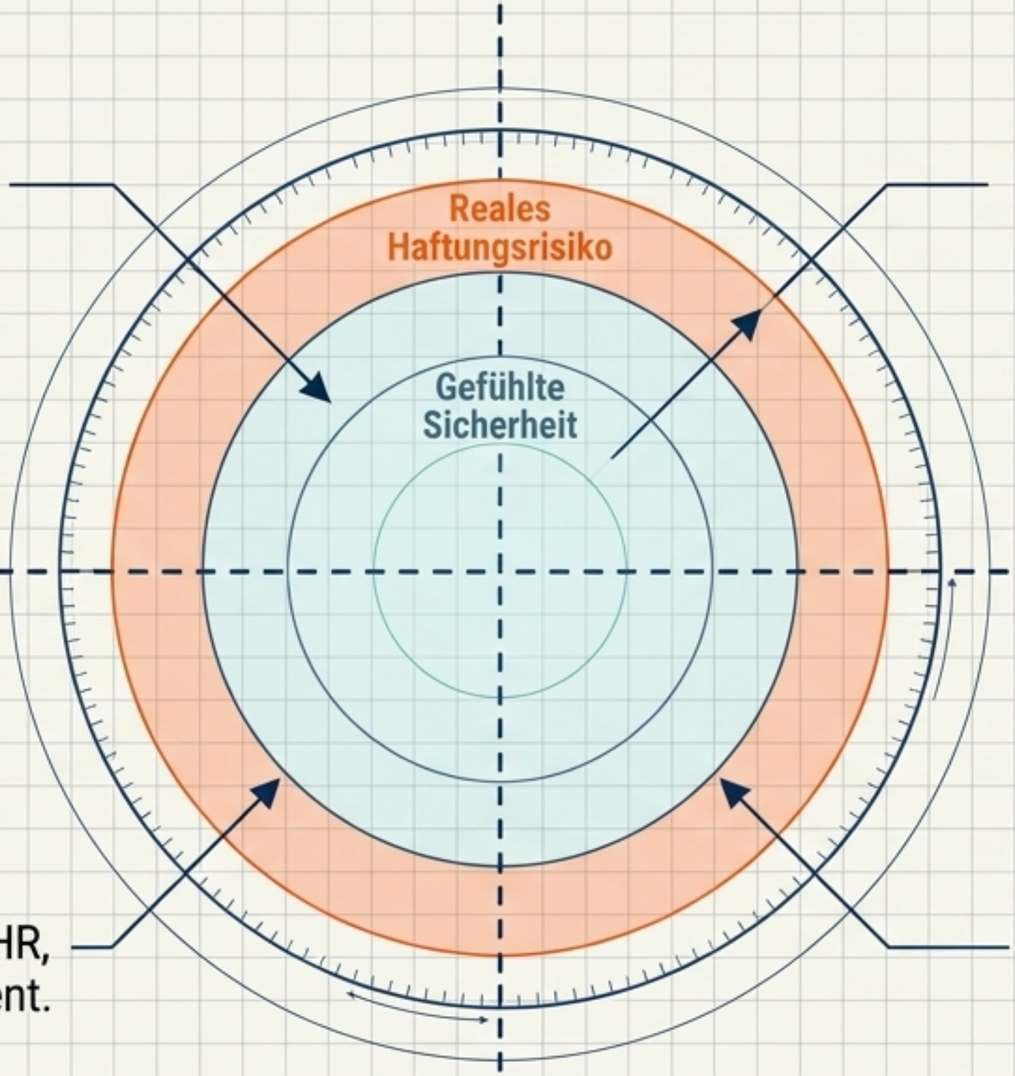
- Beispiele: Falsche, irreführende oder unvollständige Angaben gegenüber den Behörden (Benannte Stellen).

Die KMU-Klausel: Für Start-ups und KMU greifen zwar Begrenzungen, doch Schatten-KI im Unternehmensalltag macht auch kleine Organisationen zu direkten Zielscheiben.

Gefährliche blinde Flecken: Das Risiko-Radar

Mythos: Wir sind zu klein.

Realität: Schatten-KI in KMUs unterliegt den gleichen Transparenz- und Dokumentationspflichten, wenn Kundendaten betroffen sind.



Mythos: Wir nutzen nur ChatGPT.

Realität: Auch allgemeine KI-Nutzung löst sofortige Transparenzpflichten aus (Art. 50).

Mythos: Das ist ein reines IT-Problem.

Realität: Hochrisiko-Systeme (Annex III) betreffen maßgeblich HR, Finanzen und das Top-Management.

Mythos: Wir haben jetzt bis 2027 Zeit.

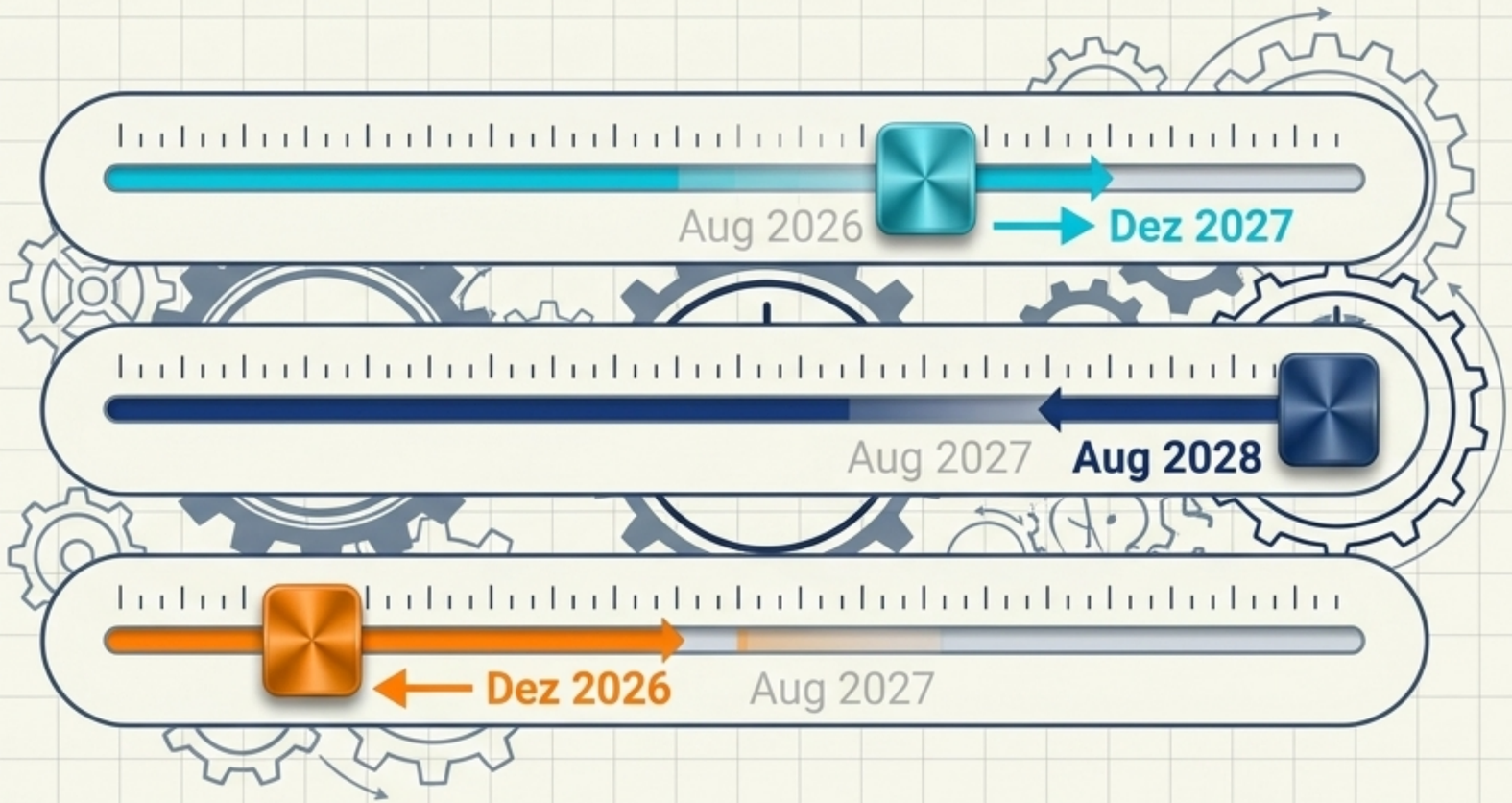
Realität: Die Wasserzeichen-Pflicht und Nudifier-Verbote greifen bereits im Dezember 2026.

Die asymmetrische Fristen-Architektur des Omnibus-Deals

Annex III (Eigenständige Hochrisiko-Systeme, z.B. HR, Biometrie)

Annex I (KI als Sicherheitskomponente in regulierten Produkten)

Transparenz (Art. 50) & **Verbotene KI** (Nudifier)



Die Verschiebung der Hochrisiko-Fristen ist kein regulatorischer Rückzug, sondern eine realpolitische Reparatur: Die benötigten harmonisierten CEN/CENELEC-Normen für Konformitätsbewertungen waren schlicht nicht fertig.

Das Omnibus-Delta:
Was sich für Unternehmen geändert hat

Thema	Ursprünglicher AI Act	Omnibus-Einigung (7. Mai 2026)	Bedeutung für die Praxis
KMU-Erleichterungen	Galt nur für Kleinstunternehmen/KMU	Ausweitung auf Small Mid-Caps (SMCs)	Weniger Dokumentationslast für den klassischen Mittelstand.
Annex I (Produkte)	Alle regulierten Produkte im AI Act	Maschinenbau ausgenommen, MedTech bleibt	Aufspaltung der Industrie-Compliance (Doppelbelastung für Medizinprodukte bleibt).
Art. 5 (Verbotene KI)	Social Scoring, Biometrie	Neues Verbot: Nudifier-Software & KI-CSAM	**Sofortige Anpassungspflicht bis Dez 2026.**
Art. 4 (AI Literacy)	Strenge, überprüfbare Ergebnispflicht	Umgewandelt in eine Bemühenspflicht	Gibt Unternehmen mehr Spielraum bei der internen Schulungsgestaltung.

Die KI-Systemarchitektur nach Risiko-Klassen

Verbotene KI

- **Beispiele:** Nudifier-Apps, Social Scoring, Echtzeit-Biometrie.
- **Deadline:** Bereits in Kraft (bzw. Dez 2026 für Neuaufnahmen).
- **Zentrale Pflicht:** Sofortiger Stopp.

Hochrisiko Annex III (Standalone)

- **Beispiele:** HR-Recruiting-Filter, Kreditscoring.
- **Neue Deadline:** Dez 2027.
- **Zentrale Pflicht:** Konformitätsbewertung, Risikomanagement, Human Oversight.

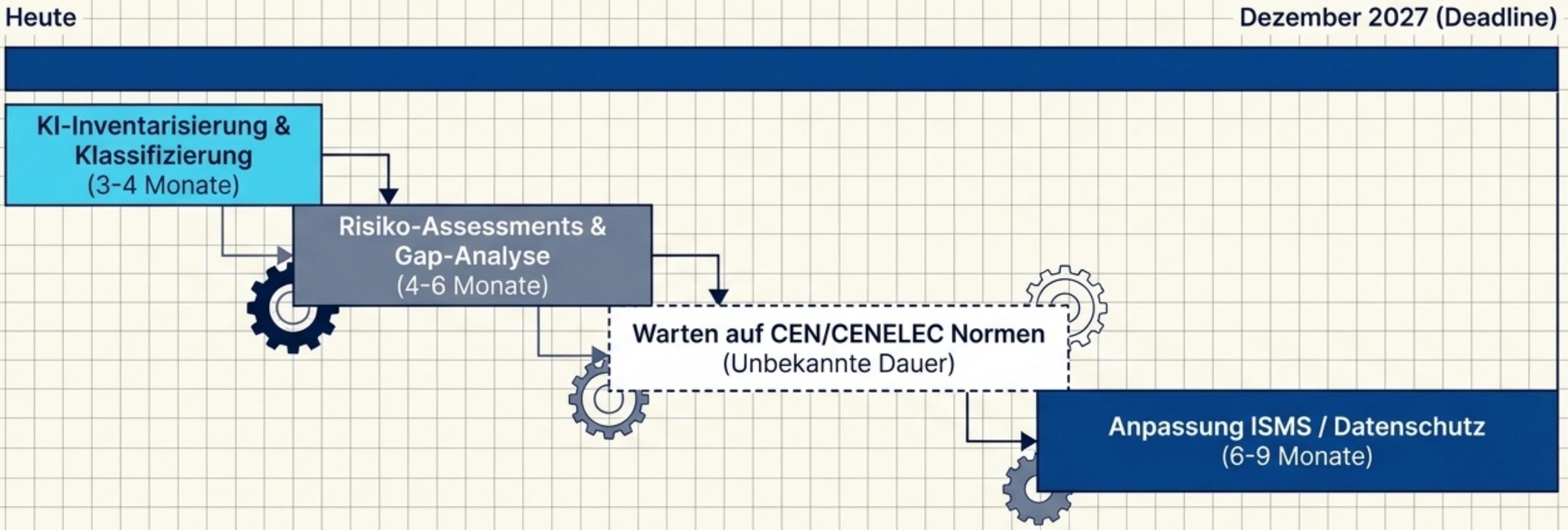
Hochrisiko Annex I (Produkte)

- **Beispiele:** Medizintechnik, Aufzüge (Sicherheitskomponenten).
- **Neue Deadline:** Aug 2028.
- **Zentrale Pflicht:** Integration in bestehende Produktsicherheitsregimes.

Generative KI / GPAI

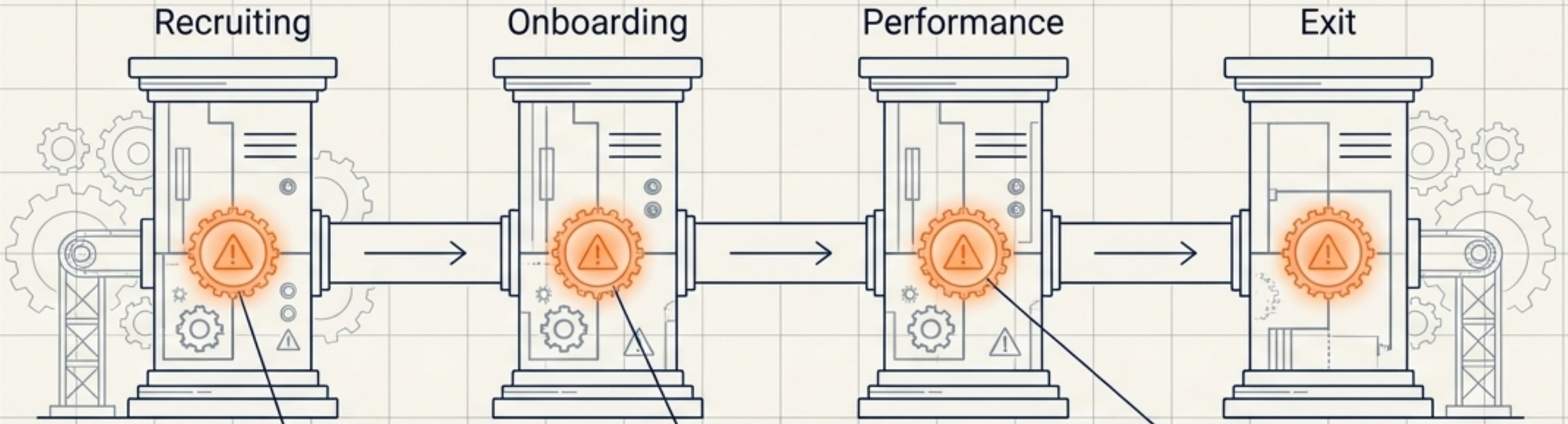
- **Beispiele:** ChatGPT-Nutzung, Bildgeneratoren.
- **Deadline:** Dez 2026 (Transparenz).
- **Zentrale Pflicht:** Wasserzeichen, Code of Practice Einhaltung, System Cards.

Das Snooze-Button-Paradoxon



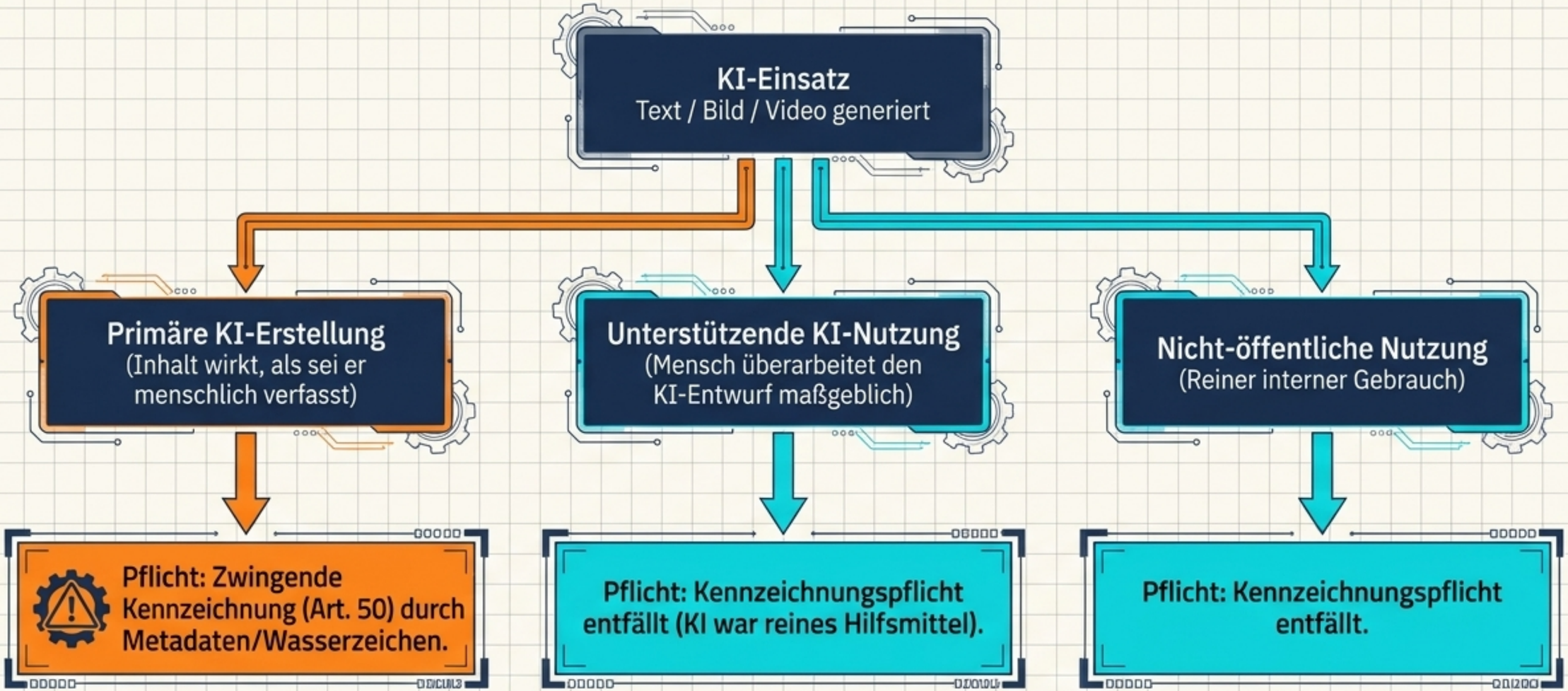
Warnung: Wer bis zur finalen Veröffentlichung der harmonisierten Normen wartet, bevor er interne Governance-Strukturen aufbaut, wird die Konformitätsbewertung bis Dezember 2027 rechnerisch nicht abschließen können.

Der unterschätzte Vektor: Human Resources als Hochrisiko-Zone



HR-Systeme sind das Einfallstor für den AI Act in klassische mittelständische Unternehmen. Auch wer die KI nur einkauft (als Betreiber), haftet für Human Oversight und Datenschutzfolgenabschätzungen.

Transparenzpflicht vorgezogen: Der Content-Lifecycle ab Dez 2026

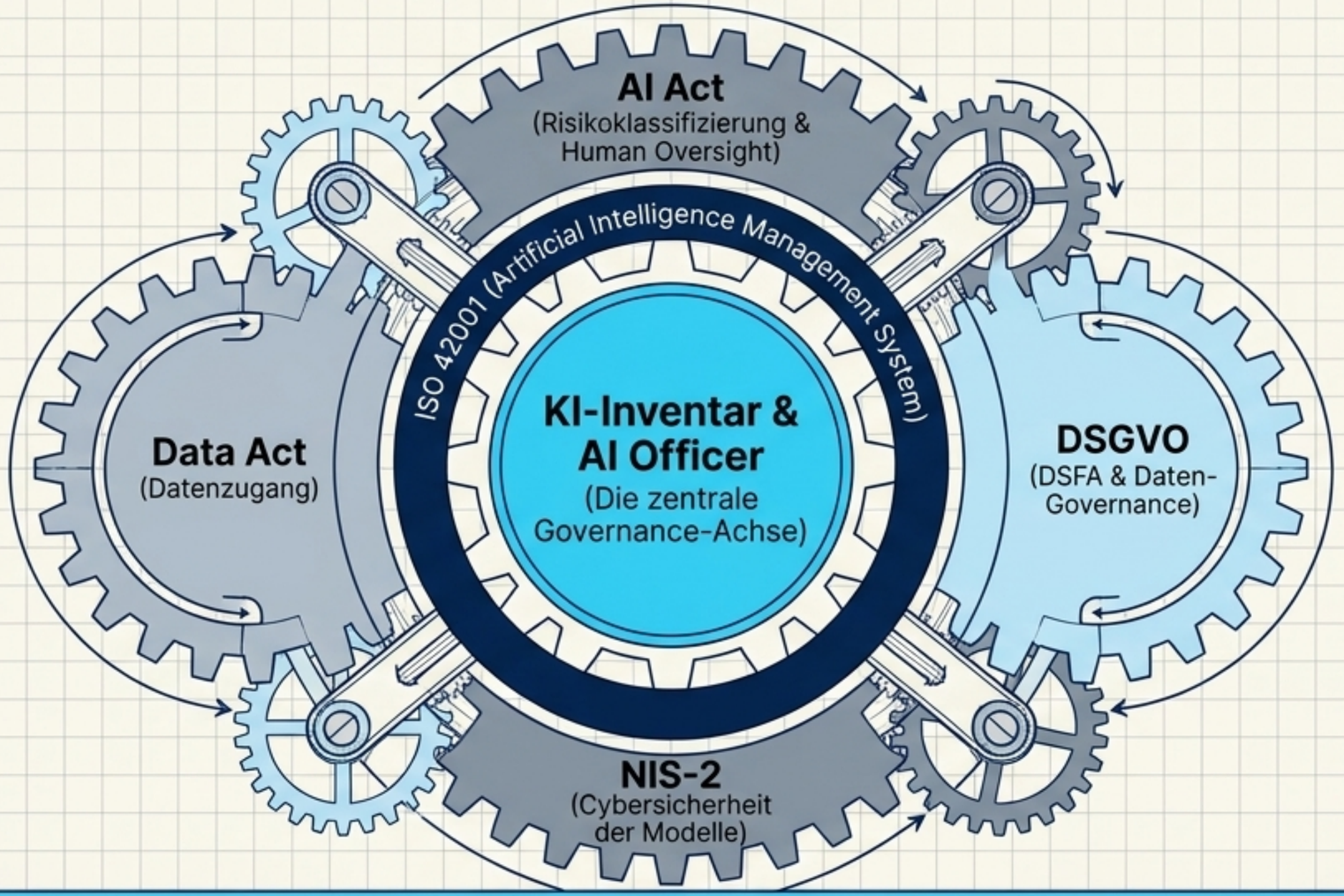


Die Governance-Herausforderung besteht nicht in der Erstellung des Inhalts, sondern im unternehmensweiten Nachweis, an welcher Abzweigung des Diagramms sich der Inhalt befindet.

Das Sandbox-Prinzip: Bias-Korrektur mit sensiblen Daten

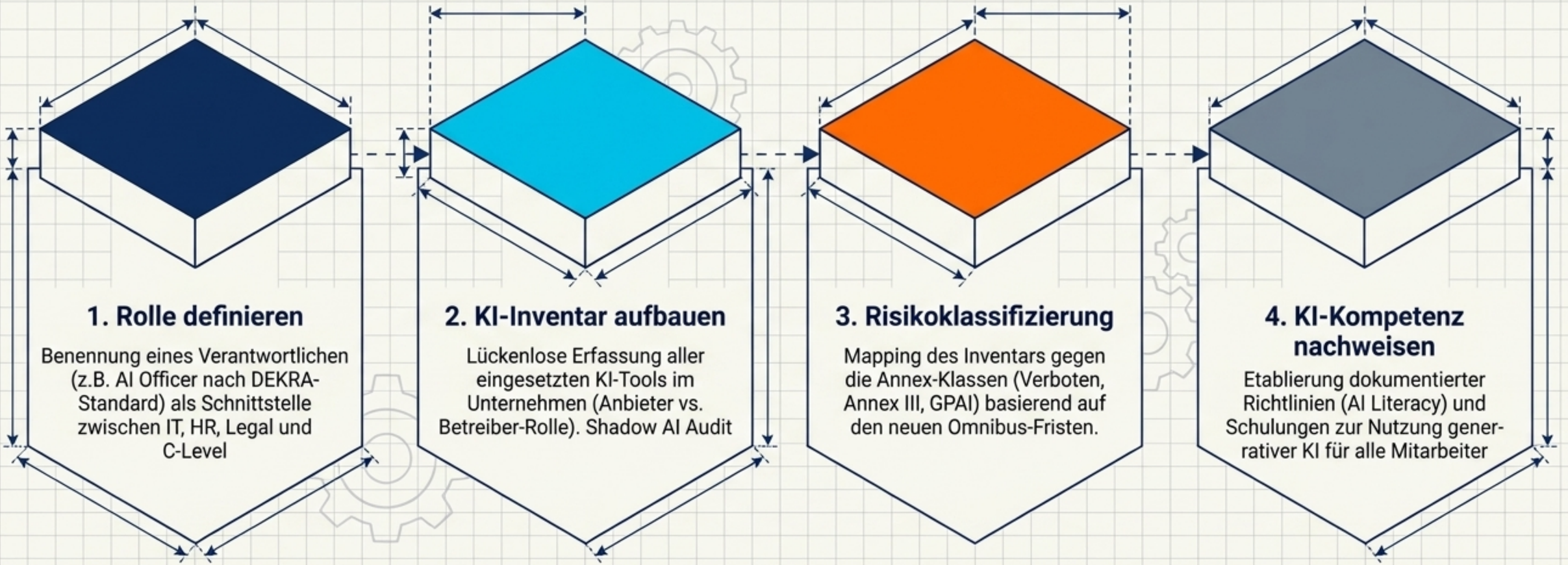
Ein bewusster Kompromiss des Gesetzgebers:
Die strenge Logik der DSGVO wird punktuell gelockert, um diskriminierungsfreie KI-Systeme zu ermöglichen.

Die Synthese: Eine integrierte Corporate KI-Architektur



AI Act Compliance, DSGVO und NIS-2 sind keine getrennten Projekte. Organisatorische Governance (Inventar & Verantwortlichkeiten) schlägt isolierte rechtliche Checklisten.

Der Blueprint zur Implementierung: Nächste Schritte



1. Rolle definieren

Benennung eines Verantwortlichen (z.B. AI Officer nach DEKRA-Standard) als Schnittstelle zwischen IT, HR, Legal und C-Level

2. KI-Inventar aufbauen

Lückenlose Erfassung aller eingesetzten KI-Tools im Unternehmen (Anbieter vs. Betreiber-Rolle). Shadow AI Audit

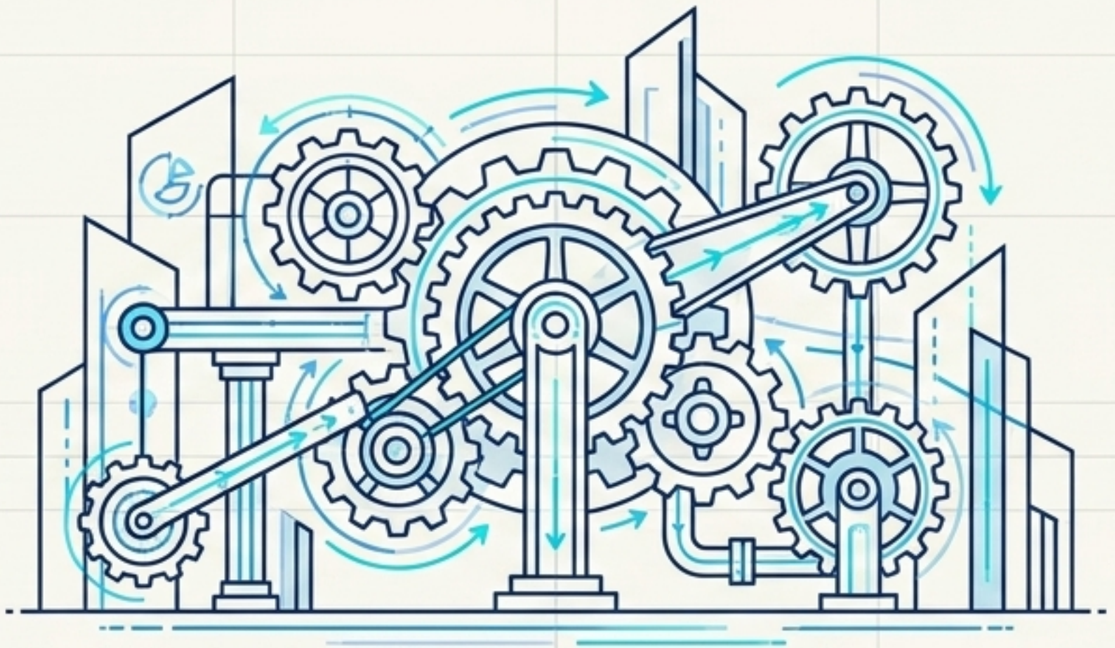
3. Risikoklassifizierung

Mapping des Inventars gegen die Annex-Klassen (Verboten, Annex III, GPAI) basierend auf den neuen Omnibus-Fristen.

4. KI-Kompetenz nachweisen

Etablierung dokumentierter Richtlinien (AI Literacy) und Schulungen zur Nutzung generativer KI für alle Mitarbeiter

Der Aufschub ist kein Stillstand



„Die gewonnene Zeit bis 2027 ist kein regulatorisches Geschenk, sondern eine zwingende Vorbereitungsphase. Wer jetzt eine integrierte Governance-Architektur aufbaut, sichert nicht nur Compliance, sondndern die technologische Souveränität seines Unternehmens.“