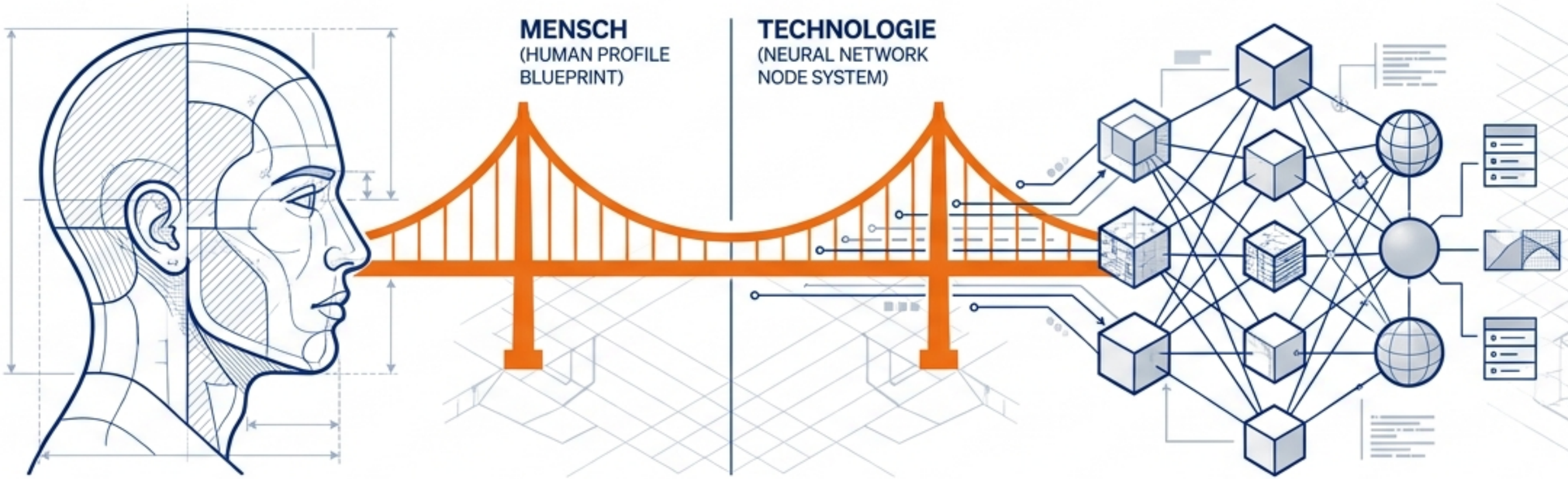
Der EU AI Act: Das Playbook für Unternehmen.

Die strategische Blaupause zur Klassifizierung, Bewertung und Konformität von KI-Systemen.

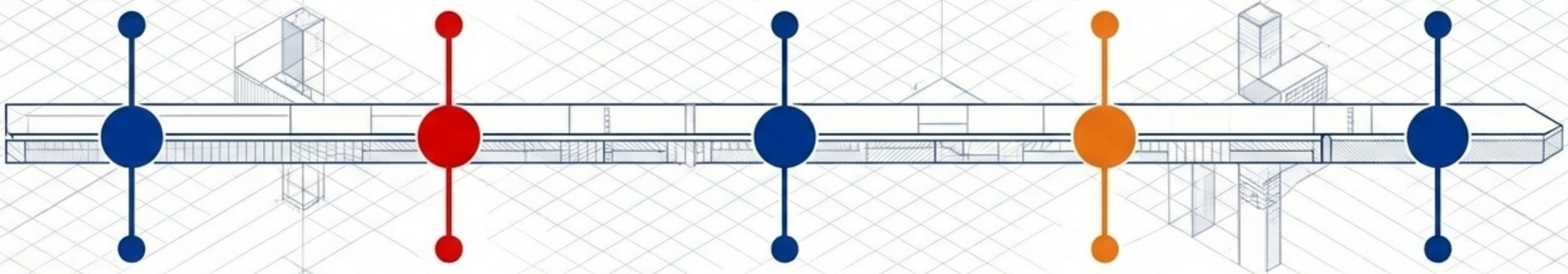
Die Brücke zwischen Mensch und Technologie.



Die EU leistet Pionierarbeit. Der AI Act ist nicht nur Regulierung – er ist der globale Standard, um Vertrauen durch strukturierte Sicherheit zu schaffen.

1. **Sicherheit & Grundrechte:** Schutz vor unannehmbaren Risiken.
2. **Investitionssicherheit:** Klare Spielregeln für Anbieter und Betreiber.
3. **Innovation:** Förderung von vertrauenswürdiger KI im Binnenmarkt.

Die Timeline der Compliance.



Aug 2024

Inkrafttreten (Entry into force).

Feb 2025

Verbotene KI-Praktiken & KI-Kompetenz-Pflicht.

Aug 2025

Regeln für General-Purpose AI (GPAI) & Notified Bodies.

Aug 2026

Vollständige Anwendung (Start der High-Risk Compliance).

Aug 2027

Start für KI als Sicherheits-komponente (Art. 6(1)).

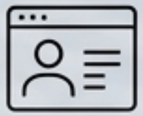
Die Rollenverteilung: Wer trägt die Verantwortung?

Der Anbieter (Provider)

Definition:
Entwickelt ein KI-System/GPAI-Modell oder lässt es entwickeln.

Aktion:
Bringt das System unter eigenem Namen/Marke auf den Markt oder nimmt es in Betrieb.

Pflicht:
Hauptverantwortlich für das Conformity Assessment (CA).



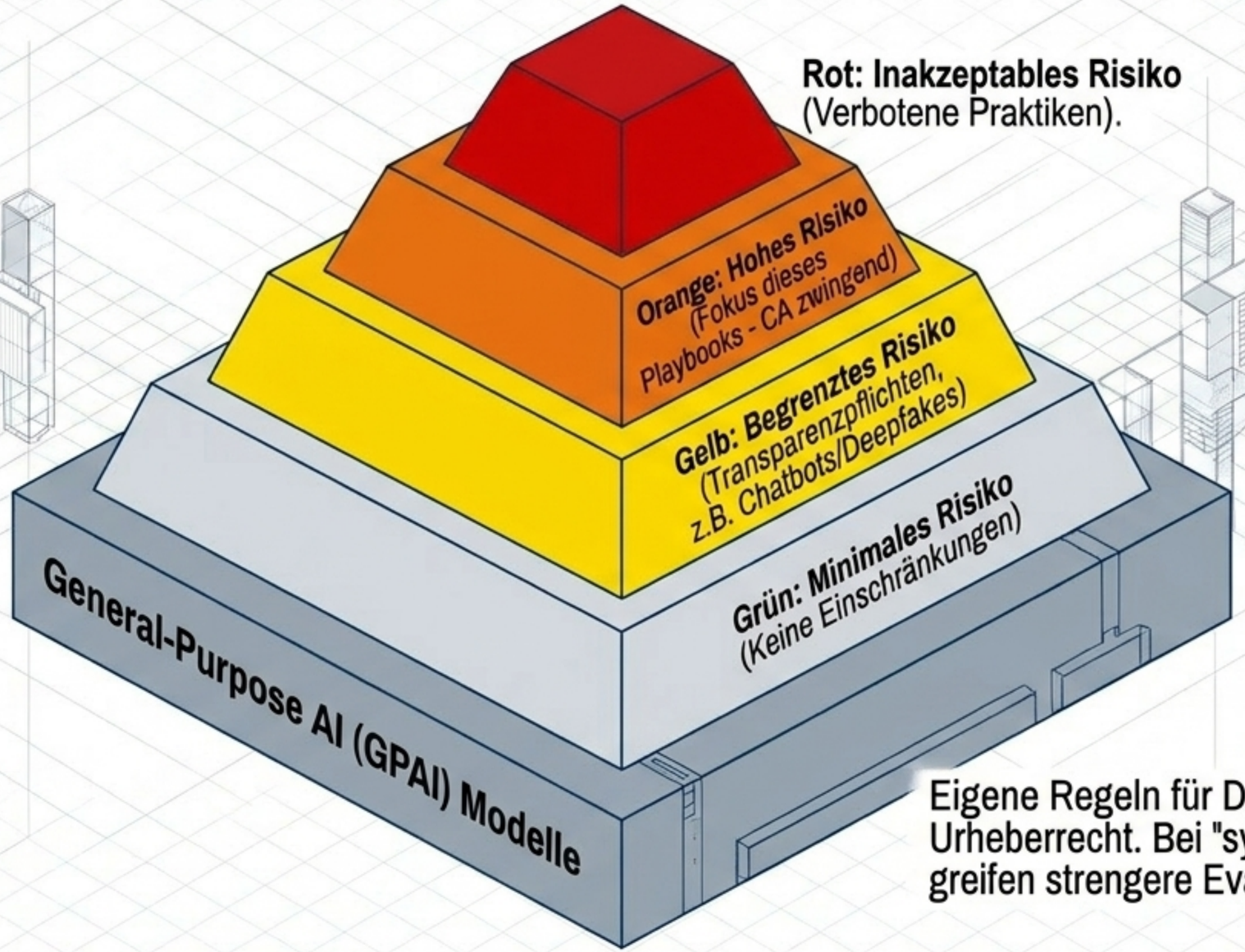
Der Betreiber (Deployer)

Definition:
Nutzt ein KI-System unter eigener Verantwortung (beruflicher Kontext).

Aktion:
Überwacht den Betrieb, meldet Vorfälle.

Achtung: Ein Betreiber wird zum Anbieter, wenn er das System wesentlich verändert oder unter eigener Marke anbietet!

Die KI-Risikopyramide der EU.



Eigene Regeln für Dokumentation und Urheberrecht. Bei "systemischen Risiken" greifen strengere Evaluierungspflichten.

Verbotene Praktiken (Unacceptable Risk)

Februar 2025 Update: EU-Kommission Leitlinien-Entwurf (Art. 5)

Status: Am 4. Feb 2025 veröffentlicht (nicht bindend, aber richtungsweisend für Behörden).

Ziel: Rechtssicherheit für die Auslegung von Verboten. Schützt europäische Werte vor inakzeptablen KI-Anwendungen. Letztgültige Auslegung obliegt dem EuGH.

Der Fokus: High-Risk KI.

Die meisten regulatorischen Anforderungen des AI Acts konzentrieren sich auf eine einzige Kategorie: Hochrisiko-KI-Systeme.

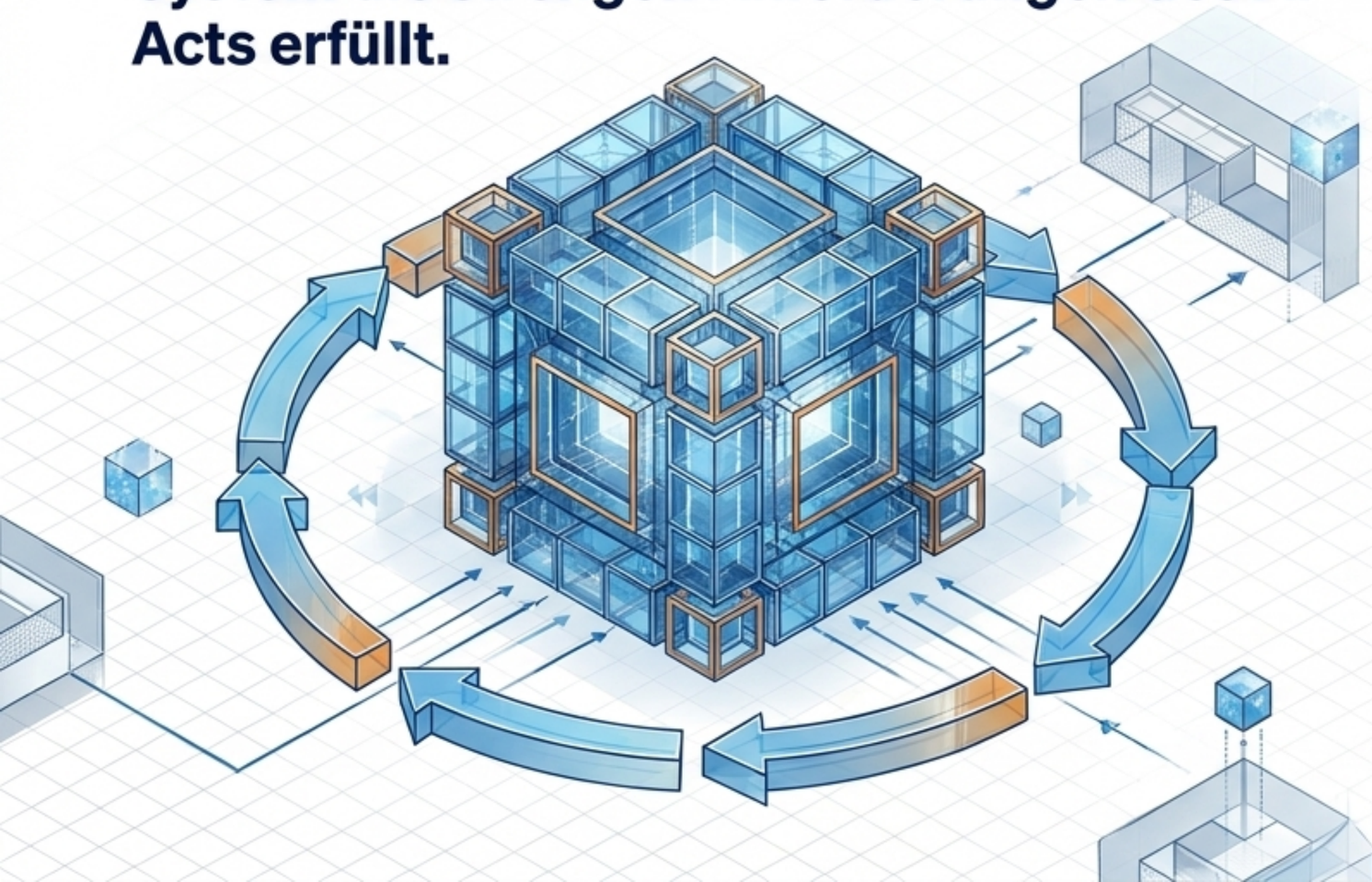
Ein Abwärts-Pfeil leitet in die nächste Phase: Wie identifizieren wir Hochrisiko-KI und wie beweisen wir Konformität?

Matrix: Ist das System "High-Risk"?

Annex I (Produktsicherheit)	Annex III (Sensible Anwendungsbereiche)
Kriterium: KI ist eine Sicherheitskomponente eines bereits regulierten Produkts ODER selbst ein reguliertes Produkt.	**Kriterium:** KI wird in explizit definierten kritischen Bereichen eingesetzt.
Bedingung: Drittanbieter-Zertifizierung ist nach EU-Recht bereits erforderlich.	**Ausnahme:** System führt nur eine “enge verfahrenstechnische Aufgabe” aus (Art. 6(3)).
Beispiele: Maschinen, Medizinprodukte (In-vitro-Diagnostik), Spielzeug, Aufzüge, Zivilluftfahrt.	**Beispiele (8 Kategorien):** Biometrie, Kritische Infrastruktur, Bildung, Personalwesen (HR), Essenzielle Dienstleistungen, Strafverfolgung, Migration, Justiz.

Was ist ein Conformity Assessment (CA)?

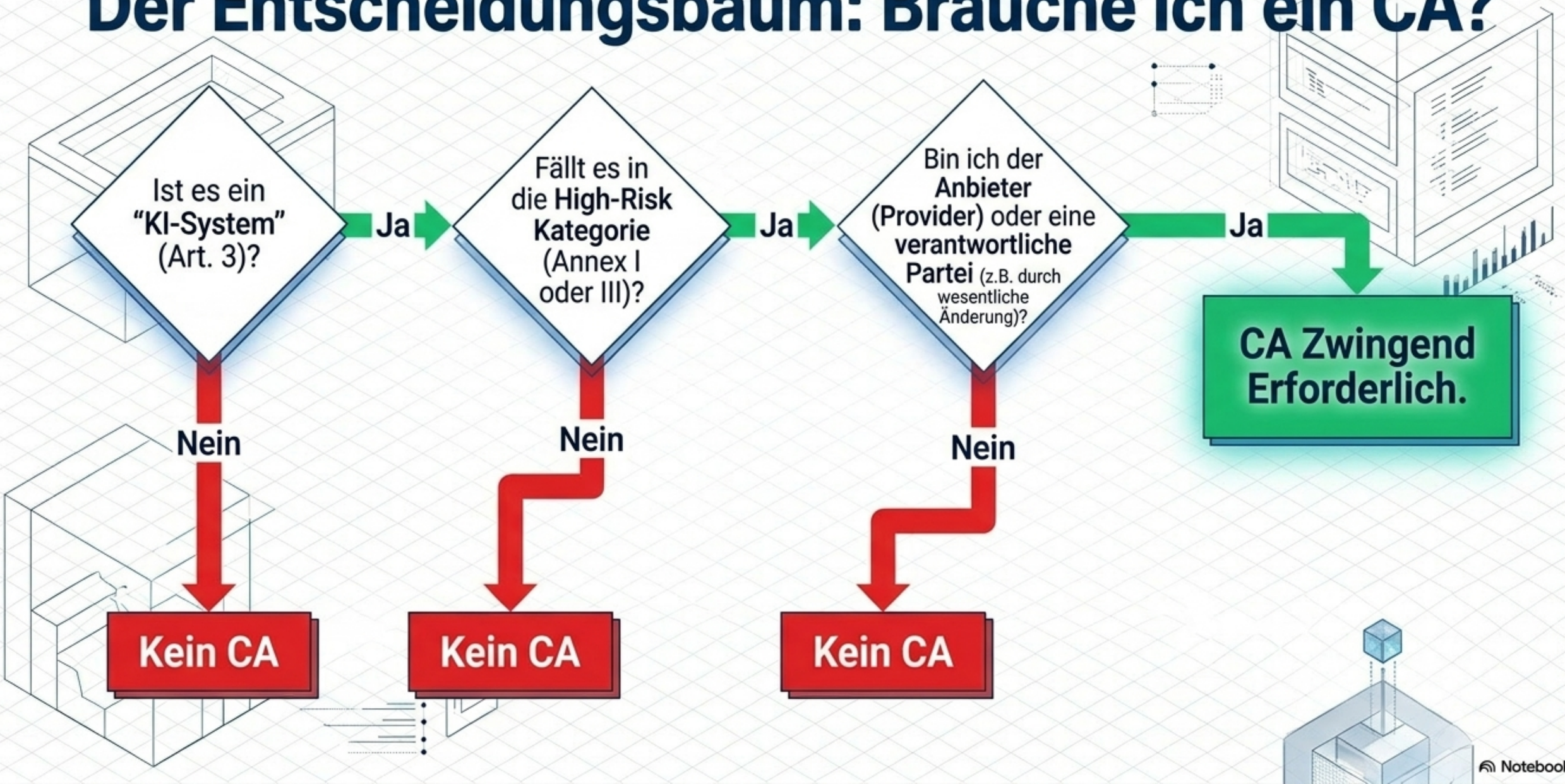
Ein CA ist der systematische Prozess, um nachzuweisen, dass ein Hochrisiko-KI-System die strengen Anforderungen des AI Acts erfüllt.



Drei Säulen des CA

1. **Risiko-Klassifizierung:** Fällt das System in die High-Risk Kategorie?
2. **Qualitätsmanagementsystem (QMS):** Ist ein robustes internes Kontrollsystem nach Art. 17 etabliert?
3. **Technische Evaluierung:** Erfüllt das System die 7 rechtlichen Kernanforderungen (Art. 9–15)?

Der Entscheidungsbaum: Brauche ich ein CA?



Timing & Auslöser: Wann muss das CA erfolgen?

Trigger 1: Pre-Market (Markteintritt)

Zwingend bevor das KI-System in der EU in Verkehr gebracht oder in Betrieb genommen wird.

Trigger 2: Post-Market (Wesentliche Änderung)

- Ein neues CA ist erforderlich, wenn das System nach Markteinführung eine "Substantial Modification" (Wesentliche Änderung) erfährt.
- **Definition:** Eine unvorhergesehene Änderung, die die Konformität beeinträchtigt oder den vorgesehenen Zweck ändert.
- **Ausnahme:** Kontinuierliches Lernen (ML) ist keine wesentliche Änderung, wenn es im initialen CA vorausgeplant und dokumentiert wurde.

Wer bewertet? Internal vs. Third-Party

Internes Assessment (Annex VI)

Wann?

- Standardweg für die meisten Annex III Systeme (z.B. HR, Bildung, Kritische Infrastruktur)

Prozess?

- Anbieter prüft QMS, technische Dokumentation und stellt **selbst** eine 'EU Declaration of Conformity' aus. Bringt CE-Kennzeichnung an.

Third-Party Assessment (Annex VII)

Wann?

- Zwingend für Biometrie (Annex III Punkt 1), Systeme für Strafverfolgung/Migration, sowie Annex I Produkte (wenn harmonisierte Standards fehlen)

Prozess?

- Unabhängige 'Notified Body' (Benannte Stelle) prüft QMS und Dokumentation. Stellt Zertifikat aus (kann bei Verstößen entzogen werden!)

Das 7-Säulen-Framework der Konformität.

1. **Risk Management** (Art. 9)
2. **Data & Data Governance** (Art. 10)
3. **Technical Documentation** (Art. 11)
4. **Record Keeping / Logging** (Art. 12)
5. **Transparency** (Art. 13)
6. **Human Oversight** (Art. 14)
7. **Accuracy, Robustness & Cybersecurity** (Art. 15)

Jede dieser 7 Säulen muss in der **technischen Dokumentation verankert sein,** bevor ein CE-Kennzeichen vergeben werden kann.

Säule 1: Risk Management System (RMS).

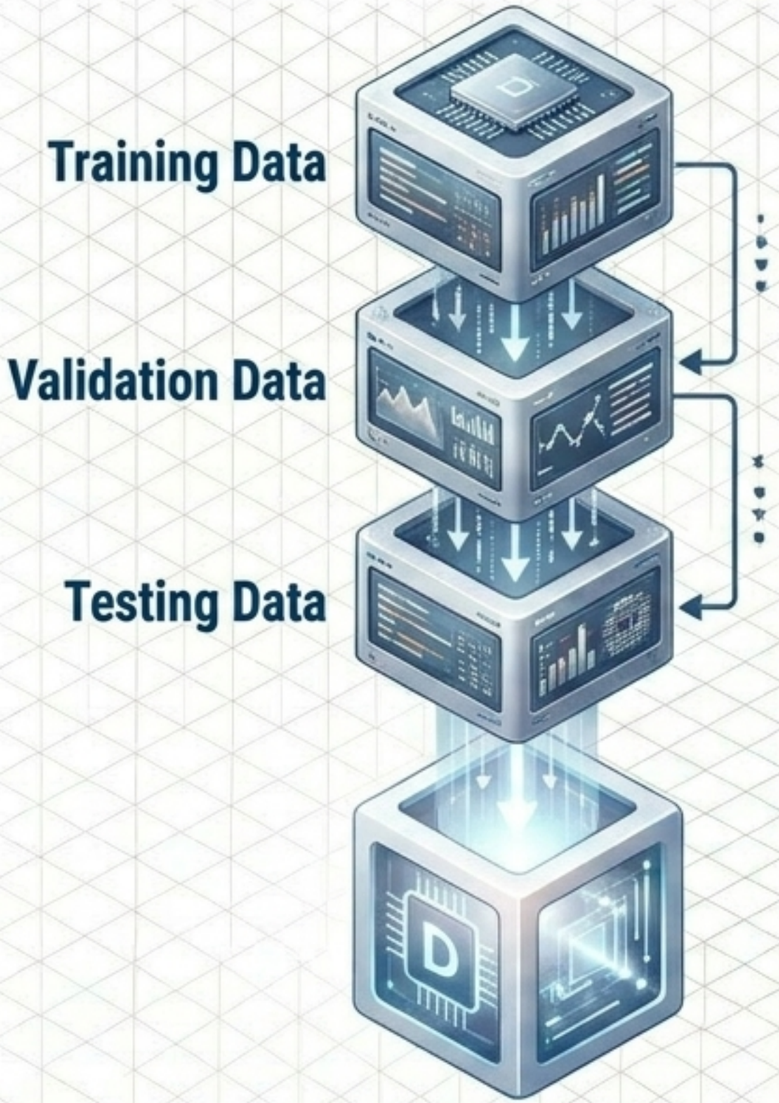
Identifikation:
Bekannte und vernünftigerweise vorhersehbare Risiken (inkl. Fehlgebrauch) ermitteln.

Evaluierung:
Neue Risiken durch Post-Market-Daten analysieren.

Mitigierung:
Risiken auf ein akzeptables Maß reduzieren (Technisch machbares Minimum). Besondere Rücksichtnahme auf vulnerable Gruppen (z.B. Minderjährige).

Testing:
Testen gegen vorab definierte Wahrscheinlichkeitsschwellen (vor Markteinführung!).

Säule 2: Data & Data Governance.



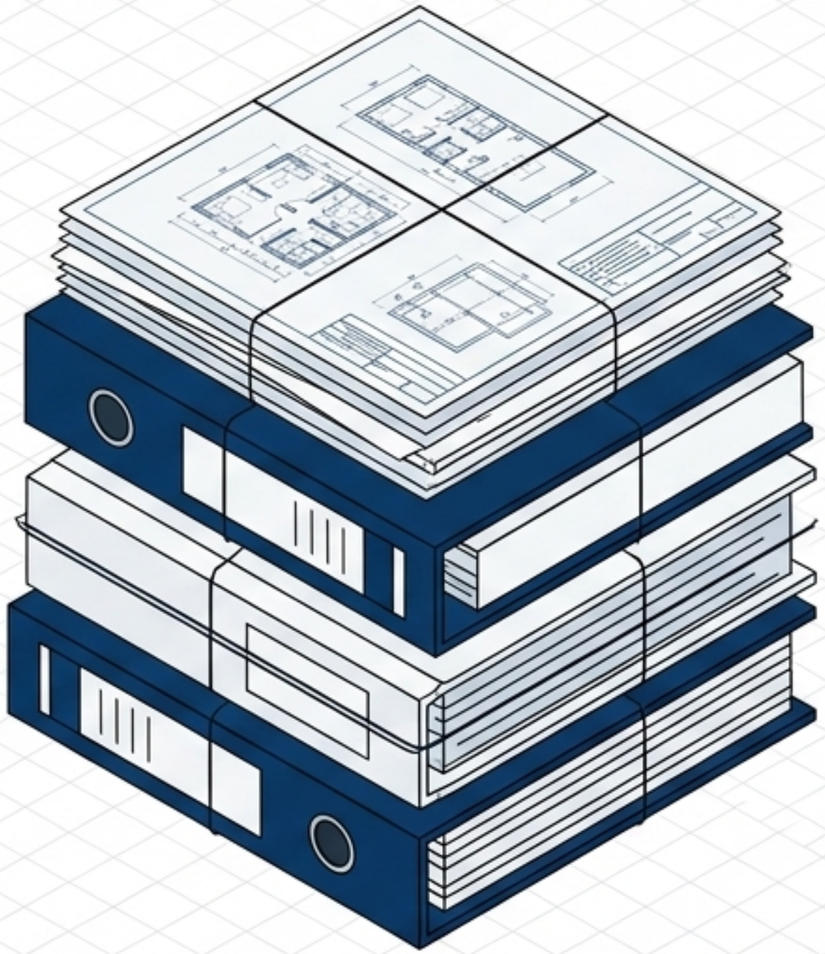
Key Requirements for High-Quality Datasets:
- Müssen relevant, repräsentativ und fehlergeprüft sein.
- Müssen statistische Eigenschaften der Zielgruppe widerspiegeln (Vermeidung von Bias).

GDPR Schnittmenge (Ausnahmeregelung Art. 10(5)):

Regel:
Verarbeitung von besonderen personenbezogenen Daten (sensible Daten nach DSGVO) ist ausnahmsweise erlaubt, wenn dies streng notwendig ist, um Bias zu erkennen und zu korrigieren.

Sicherheitsvorkehrungen:
Pseudonymisierung, strikte Zugangskontrollen, und sofortige Löschung nach Korrektur des Bias.

Säule 3: Technical Documentation.



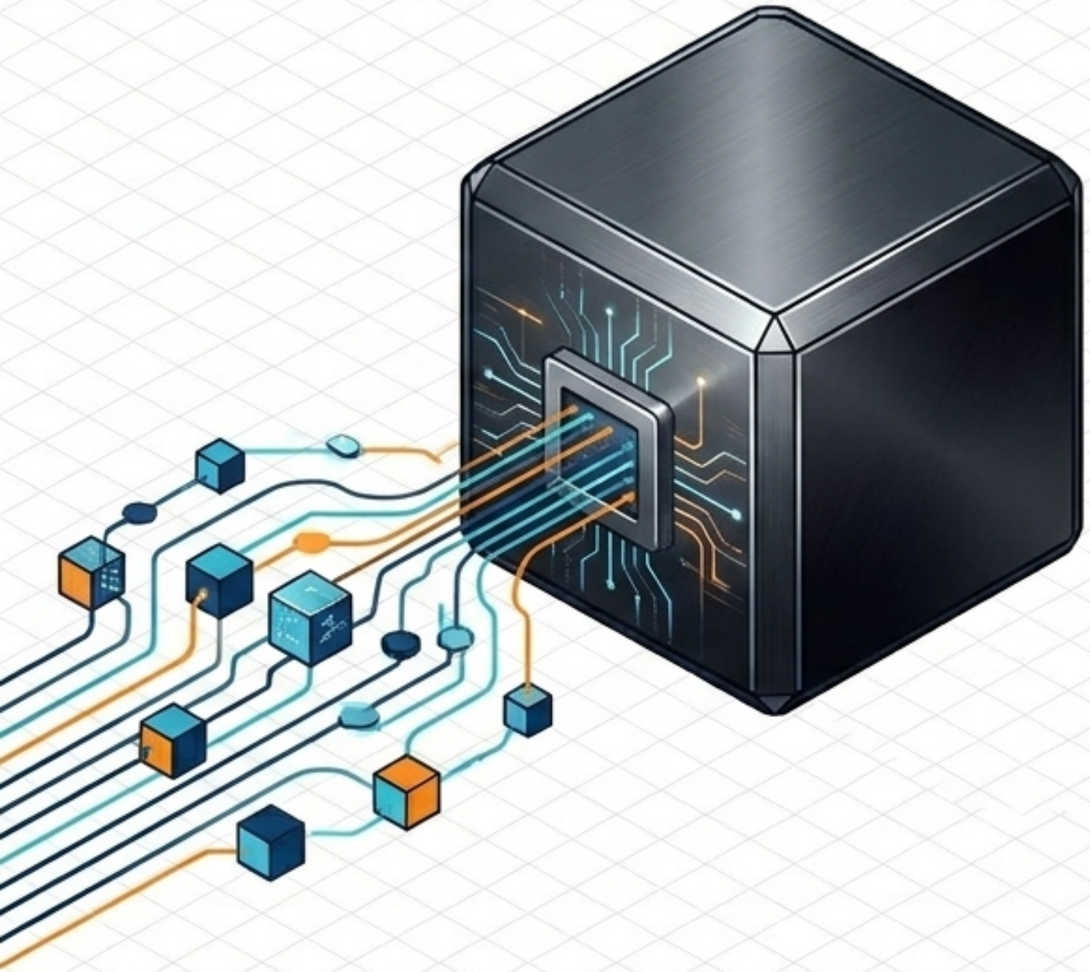
Was muss dokumentiert werden? (Annex IV Checkliste):

- ☑ Systembeschreibung & intendierter Zweck.
- ☑ Architektur, Algorithmen und Entwicklungsprozess.
- ☑ Detaillierte Infos zu Trainings-, Validierungs- und Test-Datensätzen.
- ☑ Performance-Metriken & Beschreibungen von durchgeführten Änderungen.
- ☑ Post-Market Monitoring Plan.

Core Rule: Muss vor Inverkehrbringen erstellt und 10 Jahre aufbewahrt werden.

Warnung: Behörden können bei mangelhafter Dokumentation den Marktrückruf anordnen.

Säule 4: Record Keeping (Logging).



Die "Black Box" der KI:

Das System muss technisch in der Lage sein, Ereignisse (Logs) während des Betriebs automatisch aufzuzeichnen.

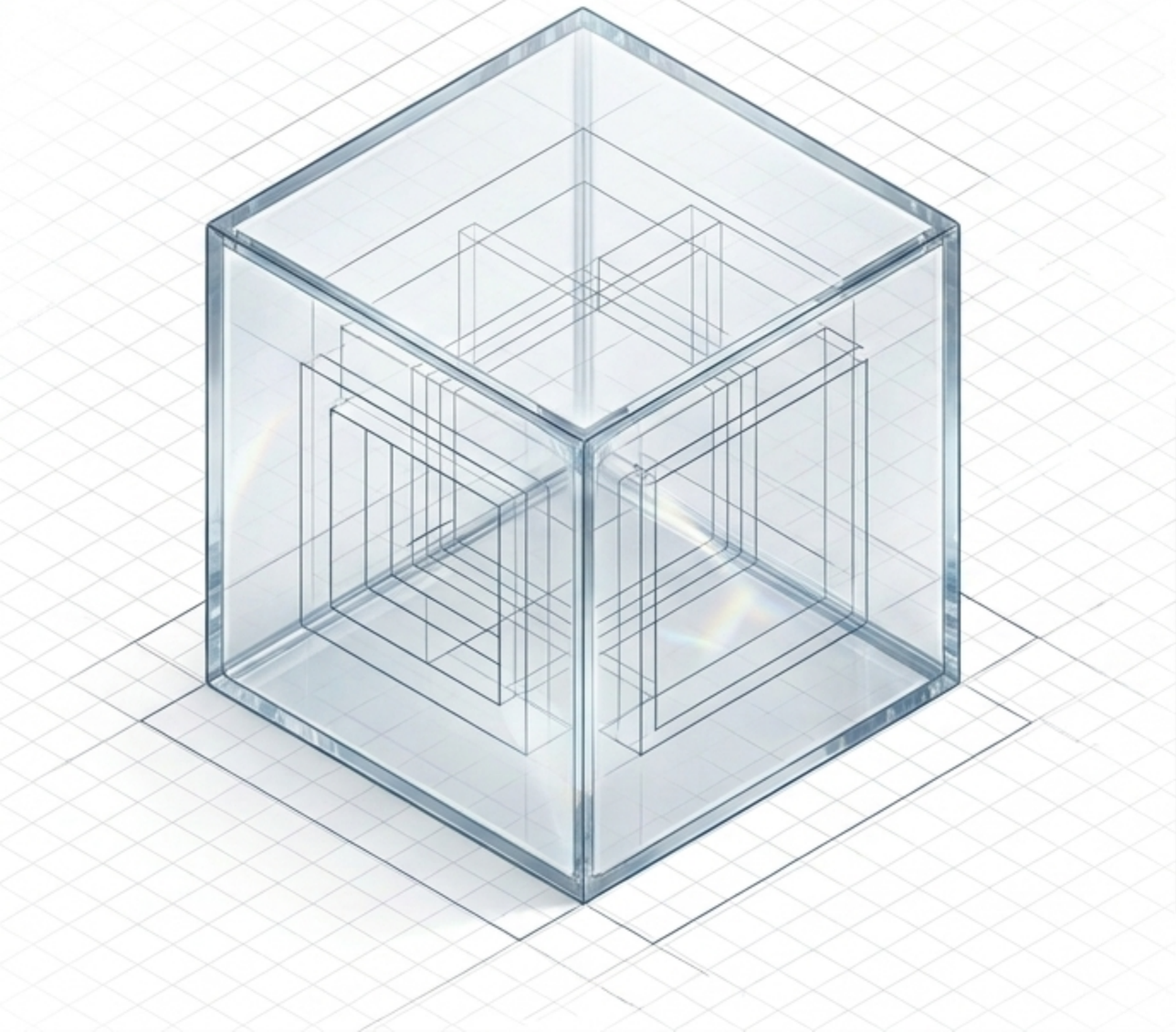
Ziel:

Sicherstellung der Rückverfolgbarkeit (Traceability) über den gesamten Lebenszyklus. Ermöglicht die Identifikation von Risiken nach wesentlichen Änderungen.

Spezifische Pflichten:

- Mindestens 6 Monate Aufbewahrungsfrist.
- Bei Remote-Biometrie: Exakte Erfassung von Zeitraum, Referenzdatenbank, Input-Daten (Match) und der involvierten menschlichen Prüfer.

Säule 5: Transparenz & Informationspflicht



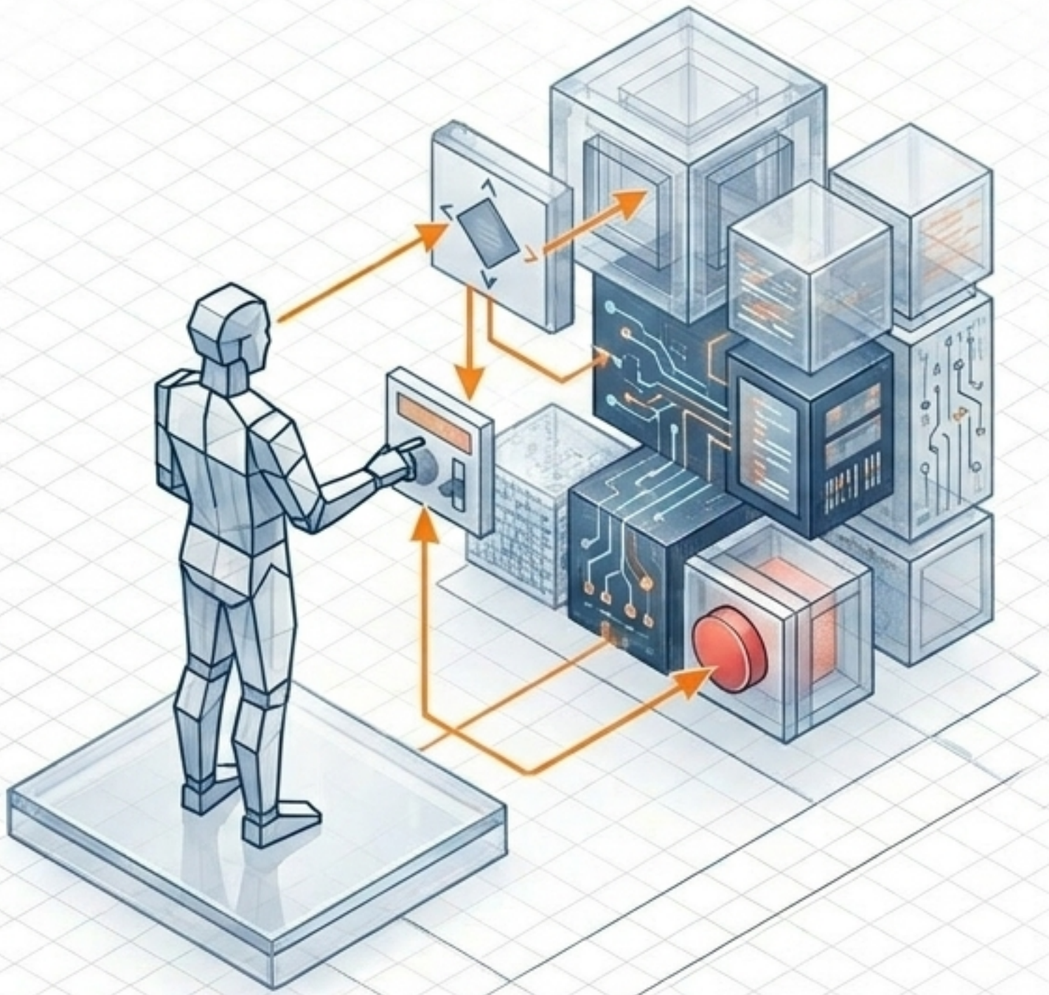
Das ‘Explainability’ Mandat:

Der Betrieb muss ausreichend transparent sein, damit Anbieter und Betreiber die Ergebnisse (Outputs) interpretieren können.

Instructions for Use (Bedienungsanleitung):

- Muss prägnant, vollständig, korrekt und verständlich sein.
- **Zwingende Inhalte:** Identität des Anbieters, Charakteristika, Leistungsfähigkeiten und Leistungsgrenzen (Limitations) des High-Risk Systems.

Säule 6: Human Oversight.



Zwei Umsetzungswege:

1. **Built-in:** Technische Kontrollmechanismen, die direkt in das System integriert sind.

2. **Operational:** Maßnahmen, die durch den Betreiber (Deployer) umgesetzt werden müssen (basierend auf den Instructions for Use).

Eingriffsebenen:

Menschen müssen in der Lage sein, das System vollständig zu verstehen, Outputs zu ignorieren, zu überschreiben oder das System über einen 'Stop-Button' sofort abzuschalten.

Säule 7: Accuracy, Robustness & Cybersecurity.

Performance Standard: Das System muss über den gesamten Lebenszyklus ein angemessenes Maß an Genauigkeit und Robustheit beibehalten.

Cybersecurity-Pflichten:

- Resilienz gegen Angriffe, die das Systemverhalten manipulieren sollen.
- Schutz gegen 'Data Poisoning' (Vergiftung der Trainingsdaten) und 'Adversarial Examples' (gezielte Täuschung des Algorithmus).
- Fehler und Inkonsistenzen in der Umgebungslage (Context of Use) müssen ausgeglichen werden.

Synthese: Die Post-Market Überwachung

Der Kreislauf endet nie:
Compliance endet nicht mit dem Markteintritt. Das System erfordert eine kontinuierliche Feedbackschleife zwischen Betreiber und Anbieter.

Korrekturmaßnahmen:
Bei Nicht-Konformität im Betrieb drohen Meldepflichten an Behörden, Marktrücknahmen oder Updates.

Fazit (Executive Takeaway):
Der EU AI Act ist mehr als eine rechtliche Hürde. Er ist eine strategische Blaupause. Wer die Conformity Assessments als integralen Bestandteil der Qualitäts- und Systemarchitektur begreift, baut nicht nur legale, sondern hochwertigere und vertrauenswürdigere Technologie.