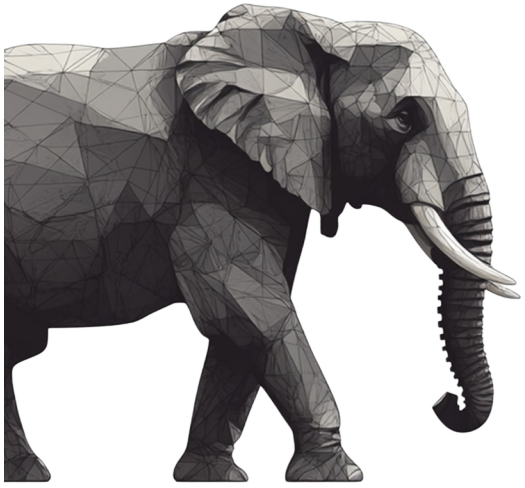
KI CODEX

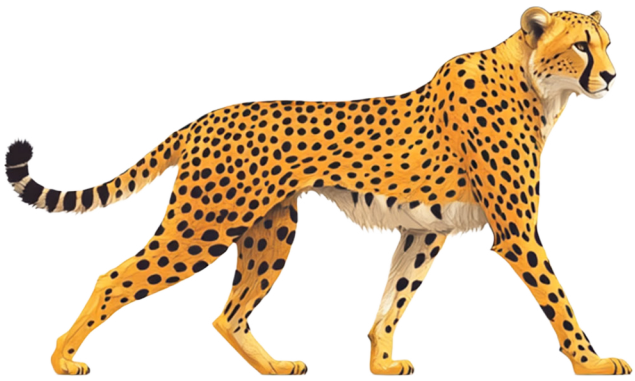
Minimum viable compliance

Mit begrenzten Ressourcen zur EU AI Act Compliance: Der agile Weg für Startups und KMUs.



Klassische Complianceansätze

Klassische Compliance ist schwerfällig: Sie frisst Ressourcen, ignoriert Risiken wegen fehlender Priorisierung, blockiert Innovation – und passt nicht zu den dynamischen Anforderungen des EU AI Acts.



Minium viable compliance

Schnell, schlank, sicher – der MVC-Weg zur KI-Compliance.

https://www.ki-codex.ai/de

“Perfektion ist nicht dann erreicht, wenn es nichts mehr hinzuzufügen gibt, sondern wenn man nichts mehr wegnehmen kann.”

– Antoine de Saint-Exupéry -

Das Problem: Compliance bedroht die Existenz Ihres Unternehmens

Sie stehen vor dem Dilemma, mit begrenzten Ressourcen die komplexen Anforderungen des EU AI Acts umsetzen zu müssen?

Für kleine und mittlere Unternehmen ist das keine akademische Frage – sondern eine existenzielle Herausforderung. Eine falsche Risikoeinschätzung kann über § 35 GewO zur Gewerbeuntersagung führen und Ihr gesamtes Geschäftsmodell zerstören. Während große Konzerne ganze Compliance-Abteilungen mit Budgets im Millionenbereich beschäftigen, stehen Sie mit einem Bruchteil der Mittel vor einem Berg regulatorischer Anforderungen, die bis August 2026 umgesetzt sein müssen.

Die Wahrheit, die niemand ausspricht

Klassische Compliance-Berater verkaufen Ihnen den “Big Bang”-Ansatz – Sie sollen sofort ein vollständiges Compliance-System implementieren, als müsste man direkt eine Luxusyacht bauen, wenn ein solides Motorboot für die Überfahrt völlig ausreichen würde.

Bei der DSGVO war es so, dass bis zu 60% der KMUs wertvolle Ressourcen mit überdimensionierten Compliance-Lösungen verschwendeten.
(ERDSIEK DD (2020) : zewde: „Pressemitteilung: Viele Unternehmen stellen DSGVO schlechtes Zeugnis aus.“, https://www.zew.de/presse/pressearchiv/viele-unternehmen-stellen-dsgvo-schlechtes-zeugnis-aus (2025-04-03))

Diese Ansätze stammen aus einer Zeit, als noch Planbarkeit vorherrschte.

PLANBARE ZUKUNFT = KLASSISCH	NICHT PLANBARE ZUKUNFT = LEAN, AGILE
Langfristige Planung (79 Jahre)	Agiles Management (Scrum, Kanban, Design Thinking)
Strategische Planung (80er Jahre)	Entrepreneurship basierte Methoden (Effectuation, Lean Startup)
Strategisches Management (ab 90er)	Responsive Organisations Manifesto
Akademische Lehre	Neueste Management Literatur
Klassische Industriekonzerne	Startups & Tech-konzerne
Klassische Strategieberatungen	Beratungsboutiquen

Die KI-Regulierung ist so dynamisch wie die Technologie selbst. Wer heute noch mit starren Konzepten hantiert, verschwendet nicht nur Ressourcen – sondern erstickt Innovation im Keim. Genau das können sich KMUs im Wettbewerb mit Großkonzernen nicht leisten, wenn sie überleben wollen.

Der bessere Weg: Minimum Viable Compliance (MVC)

Unser Whitepaper zeigt Ihnen einen wissenschaftlich fundierten, pragmatischen Weg zur EU AI Act-Konformität – maßgeschneidert für die Realität kleiner und mittlerer Unternehmen.

Mit dem MVC-Ansatz:

- Reduzieren Sie Ihre initialen Compliance-Kosten um bis zu 60%

- Erreichen Sie rechtliche Grundsicherheit in nur 4-6 Wochen statt in 6-9 Monaten

- Bewahren Sie Ihre Innovationsfähigkeit durch iterative, ressourcenschonende Implementierung

Nutzen Sie Compliance als strategischen Wettbewerbsvorteil statt als Innovationsbremse.

Sie sind der Gepard! Werden Sie nicht zum trägen Elefanten!

Executive Summary

Der EU AI Act stellt KMUs vor erhebliche Herausforderungen: begrenzte Ressourcen, komplexe regulatorische Anforderungen und das Spannungsfeld zwischen Innovation und Compliance. Klassische Compliance-Ansätze verschärfen diese Probleme durch ihre Ressourcenintensität, mangelnde Flexibilität und fehlende Priorisierung. Dieses Whitepaper präsentiert "Minimum Viable Compliance" (MVC) als agilen Lösungsansatz. Durch diesen Ansatz schaffen Sie ein schlankes, effizientes und kontinuierliches Compliance-Management, inspiriert vom Toyota Production System.

Vorteile

Komponenten

Das entwickelte Framework besteht aus vier Kernkomponenten:

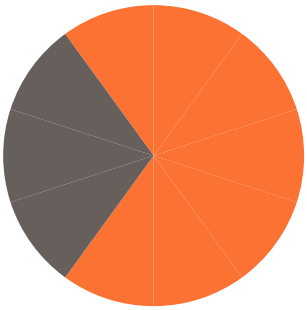
1. **Compliance-Backlog** zur strukturierten Erfassung aller (zu priorisierenden) Anforderungen
2. **Minimum Viable Compliance** als initialer Implementierungsfokus
3. **Iterative Compliance-Prozesse** zur kontinuierlichen Verbesserung
4. **Validierungsmechanismen** zur systematischen Überprüfung

Phasen

Die dreiphasige Implementierung

1. **Risikobewertung**,
2. **MVC-Implementierung**,
3. **iterative Erweiterung**

führt zur schnelleren Markteinführung, effizienterer Ressourcennutzung und adaptionsfähiger Compliance.



EU AI Act bislang ignoriert

76%

24 % der deutschen Unternehmen haben sich erst mit dem EU AI Act beschäftigt, obwohl 62 % davon ausgehen, dass er Rechtssicherheit bringen werde.

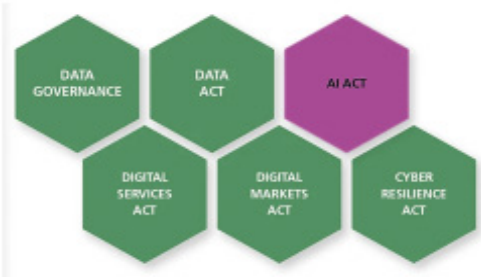
Quelle: Weber, Dr. Anja. "Jedes Vierte Unternehmen Beschäftigt Sich Mit Dem Ai Act Bitkom Research." (2024): Accessed 2025-03-26 - 22:53, https://www.bitkom-research.de/news/jedes-vierte-unternehmen-beschaeftigt-sich-mit-dem-ai-act.

Der EU AI Act: Key Facts

Der neue Rechtsrahmen

Der EU AI Act ist die erste umfassende Regulierung für künstliche Intelligenz (KI) auf supranationaler Ebene. Als Verordnung gemäß Art. 288 Abs. 2 AEUV ist sie in allen Mitgliedstaaten **unmittelbar geltendes Recht** *und bedarf keiner nationalen Umsetzung. Ziel ist die Schaffung harmonisierter Regeln zur Förderung der KI-Entwicklung bei gleichzeitiger Gewährleistung von Sicherheit, Grundrechtsschutz und Marktintegrität.*

Regulatorischer Kontext



für Details mit weiteren Nachweisen => siehe Blogbeitrag des Herausgebers:
https://medium.com/@wackyworld_jenshenneberg/master-the-eu-ai-act-audit-scheme-for-a-risk-free-ai-implementation-716e1c3900c5

Der risikobasierte Ansatz

ABSOLUTE VERBOTE (ART. 5 ABS. 1)
Unzulässige KI-Praktiken – ausnahmslos verboten

Der EU AI Act verbietet unter anderem **unterschwellige Beeinflussung mit erheblichen Schäden**, die **Ausnutzung von Schwächelagen, Social Scoring, prädiktive Polizeiarbeit** ohne rechtsstaatliche Grundlage, **unrechtmäßiges Scraping biometrischer Daten, Emotionserkennung in sensiblen Kontexten** und **diskriminierende biometrische Kategorisierung**.

VERBOT MIT ERLAUBNISVORBEHALT (ART. 5 ABS. 2-3)
Verbotene KI – nur zulässig mit gesetzlicher Ermächtigung

Biometrische Echtzeit-Fernidentifizierung im öffentlichen Raum.

HOCHRISIKO-KI (ART. 6 I.V.M. ANHANG III)
Zulässig – unter umfassender Regulierung

- Zugang zu **Bildung**, **Beschäftigung (KI - Recruiting)**, **Kredit**, Justiz etc.
- **Medizinprodukte** mit KI-Komponente
- Sicherheitskritische Infrastrukturen

ART. 50 - GERINGES RISIKO
Zulässig – mit Transparenzpflichten

- Chatbots
- Deepfakes
- 100 % KI-News
- best. Emotionserk.

MINIMALES RISIKO / NICHT ERFASST (ART. 2, ART.83)
Zulässig – nicht reguliert

- **2. Februar 2025** – Entfernung von KI-Systemen mit unannehmbarem Risiko
- **2. August 2025** – Compliance-Pflicht für neue GPAI-Modelle
- **2. August 2026** – Anwendbarkeit aller Anforderungen für Hochrisiko-KI-Systeme
- **2. August 2027** – Compliance-Pflicht für bestehende GPAI-Modelle

Bußgelder
Hohe Bußgelder von bis zu 35 Millionen Euro oder 7% des weltweiten Jahresumsatzes

Der EU AI Act: Folgen für KMU

Erleichterungen für KMU

Förderprogramme

KMUs können von EU- und nationalen Förderprogrammen profitieren, wie „Digitales Europa“ und „Horizont Europa“, die finanzielle Unterstützung bieten.

Vereinfachte technische Dokumentation

Von der EU-Kommission bereitgestellte, maßgeschneiderte Dokumentation für KMUs

Proportionale Gebühren

Konformitätsbewertungen werden an Unternehmensgröße angepasst

Regulatorische Sandboxes

KMUs haben Priorität beim Testen und Weiterentwickeln ihrer KI-Systeme

Erschwernisse für KMU

Ressourcenknappheit

Begrenzte finanzielle und personelle Ressourcen erschweren die Umsetzung umfangreicher Compliance-Maßnahmen, **insbesondere bei Hochrisiko-Systemen mit ihren weitreichenden Dokumentations- und Umsetzungspflichten**.

Expertisemangel

Die **Schnittstelle zwischen KI-Technologie und Regulierung** erfordert spezialisiertes Fachwissen, das in KMUs oft nicht verfügbar ist. Dies umfasst **sowohl technisches Wissen zur Risikoklassifizierung als auch juristische Expertise** zur korrekten Auslegung der Verordnung.

Komplexe Regulierungslandschaft

Der **EU AI Act überschneidet sich mit anderen Regularien wie der DSGVO, dem Digital Services Act und dem Digital Markets Act**, was zu Unklarheiten und Mehrfachregulierung führen kann.

Spannungsfeld Innovation vs. Compliance

KMUs müssen den **Spagat zwischen schneller Innovation und regulatorischer Konformität** meistern, um wettbewerbsfähig zu bleiben. Insbesondere die frühzeitigen Inventarisierungs- und Bewertungspflichten binden Ressourcen, die für die Produktentwicklung fehlen.

Implementierungsdruck durch enge Fristen

Die gestaffelten, aber insgesamt straffen Umsetzungsfristen erfordern eine **proaktive Planung und frühzeitige Inventarisierung aller KI-Systeme**, was ohne strukturierten Ansatz zu Überlastung führen kann.

Pflichten bei Hochrisiko-Systemen

- **Risikomanagement**
  Identifikation, Bewertung und Minderung von Risiken
- **Datenqualität und -governance**
  Sicherstellung der Qualität und Integrität der verwendeten Daten
- **Technische Dokumentation**
  Erstellung und Pflege umfassender technischer Dokumentationen
- **Aufzeichnungspflichten**
  Dokumentation und Speicherung relevanter Daten und Prozesse
- **Transparenz**
  Offenlegung der Funktionsweise und Nutzung des KI-Systems
- **Menschliche Aufsicht**
  Implementierung von Mechanismen zur menschlichen Kontrolle und Eingriffsmöglichkeiten
- **Robustheit und Genauigkeit**
  Sicherstellung der Zuverlässigkeit und Präzision des KI-Systems
- **Konformitätsbewertung**
  Durchführung einer Konformitätsbewertung, entweder intern oder durch eine notifizierte Stelle
- **Post-Market Monitoring**
  Kontinuierliche Überwachung des KI-Systems nach der Markteinführung
- **Meldeverfahren für Vorfälle**
  Benachrichtigung der Behörden über schwerwiegende Vorfälle

Problem

Klassische Compliance-Ansätze ticken meist noch nach dem guten alten **Wasserfall-Prinzip***: Erst werden alle regulatorischen Anforderungen seziert, dann kommt die große Gap-Analyse,und schließlich wird ein vollständiger Implementierungsplan aus dem Boden gestampft –**alles noch bevor auch nur ein Bit unter den neuen Regularien live geht. Und natürlich ist dabei alles gleich wichtig. Null Priorisierung.***

Alles muss. Alles sofort. Alles auf einmal.

Fundamentale Schwächen des Big Bang Ansatzes

Ressourcenverschwendung

Erfordert massive initiale Investitionen, bindet kritische Personalressourcen, schafft Compliance-Overhead ohne direkten Geschäftswert.

Statische Natur

Unflexibel gegenüber sich entwickelnden Interpretationen des EU AI Acts, reagiert langsam auf technologische Weiterentwicklungen, ignoriert den iterativen Charakter moderner KI-Entwicklung.

Fehlende Priorisierung

Alle Anforderungen werden gleich behandelt, unabhängig von ihrem Risikopotenzial, führt zu ineffizienter Ressourcenallokation, kritische Compliance-Lücken können übersehen werden.

Empirische Evidenz

Studien zu ähnlichen Regulierungen wie der DSGVO zeigen die Probleme:

60 % der KMUs gerieten bei der DSGVO-Implementierung ins Schleudern

Laut einer Studie des ZEW Mannheim (2020) haben rund 60 % der Unternehmen ihre Geschäftsprozesse durch die Einführung der DSGVO als verkompliziert erlebt – mit spürbaren Verzögerungen als Folge. Mehr als zwei Drittel berichten von massivem Mehraufwand bei der Umsetzung. => **Anders gesagt: DSGVO kam – und viele KMUs standen erstmal still.**

Quellen:

- ERDSIEK DD (2020) : zewde: „Pressemitteilung: Viele Unternehmen stellen DSGVO schlechtes Zeugnis aus.“, https://www.zew.de/presse/pressearchiv/viele-unternehmen-stellen-dsgvo-schlechtes-zeugnis-aus (2025-04-03)

- WEDDING N (2022) : techconsult GmbH: „Datenschutz und Informationssicherheit.“, https://www.techconsult.de/studien/kmu-datenschutz-it-sicherheit (2025-04-03)

Solution

Minimum Viable Compliance (MVC) überträgt die Prinzipien des Lean Startup-Ansatzes auf die Welt der Regulierung. So wie ein Minimum Viable Product (MVP) Startups erlaubt, schnell zu testen, zu lernen und iterativ besser zu werden, hilft MVC Unternehmen dabei, Compliance nicht als starres Korsett, sondern als agilen Prozess zu begreifen. Weg von der Vollumsetzung mit Brechstange – hin zu **schlanker, lernorientierter Compliance**.

Definition

MVC ist der kleinste sinnvolle Satz an Compliance-Maßnahmen, der:

- die **zentralen regulatorischen Anforderungen** erfüllt
- die **größten Risiken** adressiert
- eine **rechtlich tragfähige Position** schafft
- mit **minimalem Ressourceneinsatz** umsetzbar ist

Der MVC-Ansatz folgt dem **Build–Measure–Learn-Zyklus** aus der Lean-Methodik:

- **Build**: Umsetzung der absolut kritischsten Compliance-Elemente
- **Measure**: Überprüfung der Wirksamkeit (funktioniert das überhaupt?)
- **Learn**: Iterative Verfeinerung – basierend auf echten Learnings, nicht auf Vermutungen

MVC steht für eine neue Art, Compliance zu denken: fokussiert, dynamisch, risikobasiert.

Nicht weniger verantwortungsvoll – nur deutlich smarter.

Vorteile

Ressourceneffizienz

Fokussierung begrenzter Ressourcen auf kritische Anforderungen, stufenweise Investitionen statt massiver Initialkosten, bessere ROI durch Priorisierung nach Risiko

Time-to-Market

Schnellere Implementierung der grundlegenden Compliance, kürzere Zeit bis zur Markteinführung komplianter Produkte, Wettbewerbsvorteile durch agilere Prozesse

Anpassungsfähigkeit

Flexibilität bei regulatorischen Änderungen oder Interpretationen, kontinuierliche Integration neuer Erkenntnisse, Entwicklung mit dem regulatorischen Umfeld

Risikominimierung

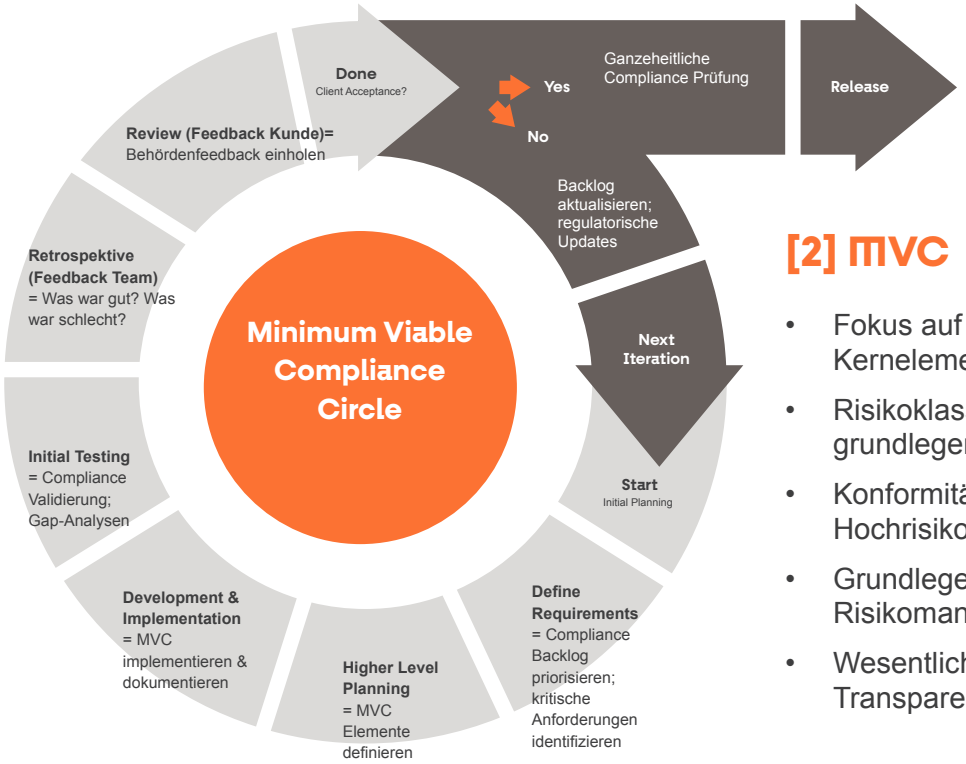
Priorisierung der höchsten Risiken, frühe Erkennung potenzieller Compliance-Lücken, kontinuierliche Validierung und Verbesserung

Das MVC-Framework im Detail

Das agile Compliance-Framework besteht aus vier Kernkomponenten, die zusammenwirken, um eine effektive und effiziente Compliance zu ermöglichen.

[1] Interative Compliance-Prozesse

- Strukturierte Sprints mit festen Zeitboxen (2-4 Wochen)
- Regelmäßige Reviews und Retrospektiven
- Kontinuierliche Integration in bestehende Prozesse
- Klare Verantwortlichkeiten und cross-funktionale Teams



[2] MVC

- Fokus auf kritische Compliance-Kernelemente:
- Risikoklassifizierung und grundlegende Dokumentation
- Konformitätsbewertung für Hochrisiko-KI
- Grundlegendes Risikomanagement-System
- Wesentliche Transparenzmaßnahmen

[3] Compliance Backlog

- Strukturierte Sammlung aller regulatorischen Anforderungen
- Priorisierungsmatrix mit vier Risikoklassen: Kritisch, Hoch, Mittel, Niedrig
- Eindeutige Definition of Done für jede Anforderung
- Kontinuierliche Aktualisierung und Anpassung

[4] Validierungsmechanismen

- Compliance-Checklisten mit konkreten Erfüllungskriterien
- Regelmäßige interne Überprüfungen
- Mehrstufige Validierung mit verschiedenen Perspektiven
- Risk-Based Testing zur Überprüfung von Risikominderungsmaßnahmen

Das MVC-Framework im Detail

*Die praktische Umsetzung des MVC-Frameworks erfolgt in **drei definierten Phasen**, die einen strukturierten, aber flexiblen Implementierungsprozess ermöglichen.*

[1] Phase 1: Initiale Risikobewertung

Risikoidentifikation
Systematische Analyse aller potenziell relevanten Anforderungen des EU AI Acts

Risikoklassifizierung
Einordnung des KI-Systems in die entsprechende Risikoklasse (unannehmbares, hohes, begrenztes oder minimales Risiko)

Detaillierte Risikoanalyse
Bewertung von Eintrittswahrscheinlichkeit, Auswirkung und Mitigationsmöglichkeiten

Risikobewertungsworkshop
Strukturierte Durchführung mit allen relevanten Stakeholdern

Dokumentation
Erstellung eines Risikobewertungsberichts und eines dynamischen Risikoregisters

[2] Phase 2: MVC-Implementierung

Implementierungsplanung
Aufteilung in überschaubare Arbeitseinheiten (Tasks) mit klaren Akzeptanzkriterien

Agile Umsetzung
Implementierung in kurzen, fokussierten Iterationen (siehe Grafik auf der Seite davor!)

Integration in bestehende Prozesse
Anpassung des QMS und Entwicklungsprozesse

Validierung
Systematische Überprüfung der implementierten Maßnahmen

[3] Phase 3: Iterative Compliance-Erweiterung

“Die Zukunft soll man nicht voraussehen wollen, sondern möglich machen.”

– Antoine de Saint-Exupéry -

Der EU AI Act muss für KMUs kein Innovationskiller sein.

Mit dem Konzept der Minimum Viable Compliance (MVC) können auch ressourcenknappe Unternehmen regulatorische Anforderungen erfüllen – ohne ihre Innovationskraft an Bürokratie zu verlieren.

Was MVC bietet:

- **Schnellere Time-to-Market** – durch fokussierte, priorisierte Umsetzung
- **Effizienter Ressourceneinsatz** – dank iterativem, bedarfsgerechtem Vorgehen
- **Mehr Anpassungsfähigkeit** – gegenüber sich wandelnden regulatorischen Rahmenbedingungen
- **Nachhaltige Compliance-Kultur** – durch kontinuierliches Lernen und Optimieren

Wer frühzeitig eine solide Compliance-Basis schafft, baut nicht nur ein Sicherheitsnetz – sondern einen echten Wettbewerbsvorteil:

- Vertrauen bei Kunden
- Zugang zu regulierten Märkten
- Minimierung rechtlicher Risiken

Der EU AI Act ist keine Bedrohung – sondern eine Chance. Eine Einladung, Compliance nicht als Pflichtübung zu sehen, sondern als strategischen Enabler in einer KI-getriebenen Welt.

Starten Sie Ihre MVC-Reise jetzt – denn wie Saint-Exupéry so treffend sagte:

„Die Zukunft soll man nicht voraussehen wollen – sondern möglich machen.“

Buchen Sie entweder mich und / oder den Kurs von meinem Geschäftspartner und mir :

https://www.ki-codex.ai/de/

https://www.ki-codex.ai/de/workshops-ki-compliance-ki-strategy

Ihr Team

Jens Henneberg

Gründer KI-Codex, Jurist, Informatiker und Versicherungskaufmann

Jens Henneberg ist Jurist, Informatiker und Versicherungskaufmann – eine sogenannte **Scannerpersönlichkeit** mit einer Laufbahn, die man weder planen noch kopieren kann. Seit fast einem Jahrzehnt ist er in der IT unterwegs – vom Entwickler zum Softwarearchitekten, mit Fokus auf Cloud, DevOps und später auch auf KI. Davor: Offizier, Versicherungsmakler, Jurist, Geschäftsführer eines Verbands. Zuletzt arbeitete er freiberuflich als KI-Stratege bei adesso und als Cloud Solution Architect bei Microsoft (via Concentrix) – mit Schwerpunkt auf generativer KI in der Cloud, KI-Compliance und strategischer Beratung. Heute begleitet er als Gründer von KI-Codex Unternehmen bei der rechtssicheren Umsetzung von KI-Projekten – insbesondere im Kontext des EU AI Act.

Privat schreibt er, produziert gelegentlich Musik und steht seit drei Jahrzehnten auf der Matte: Krav Maga, Kickboxen, Karate, Muay Thai.

Er ist die fleischgewordene Brücke zwischen Fachdomänen, Technologie und Recht.

Bert Gollnick

Gründer der Gollnick Data Solutions GmbH, Ingenieur, Volkswirt und Data Scientist

Diplom-Ingenieur für Luft- und Raumfahrttechnik, Master of Science in Volkswirtschaftslehre. Fünf Jahre Aerodynamiker für Windenergieanlagen, fünf weitere als Data Analyst. Inhaber mehrerer Patente, erfolgreicher Publizist, Videokurscreator mit Sendungsbewusstsein. Zuletzt sieben Jahre **Data Scientist** bei Siemens Gamesa.

Ein Nachfahre von Daniel Düsentrieb – nur dass er nicht durch Disney-Comichefte wandert, sondern mit traumwandlerischer Sicherheit durch neuronale Netze.

KI CODEX & Gollnick Data