AI Act entschlüsselt: Was jetzt zählt

Know-how to go: KI verstehen und sicher gestalten

HiSolutions AG

Robert Manuel Beck

Robert Manuel Beck

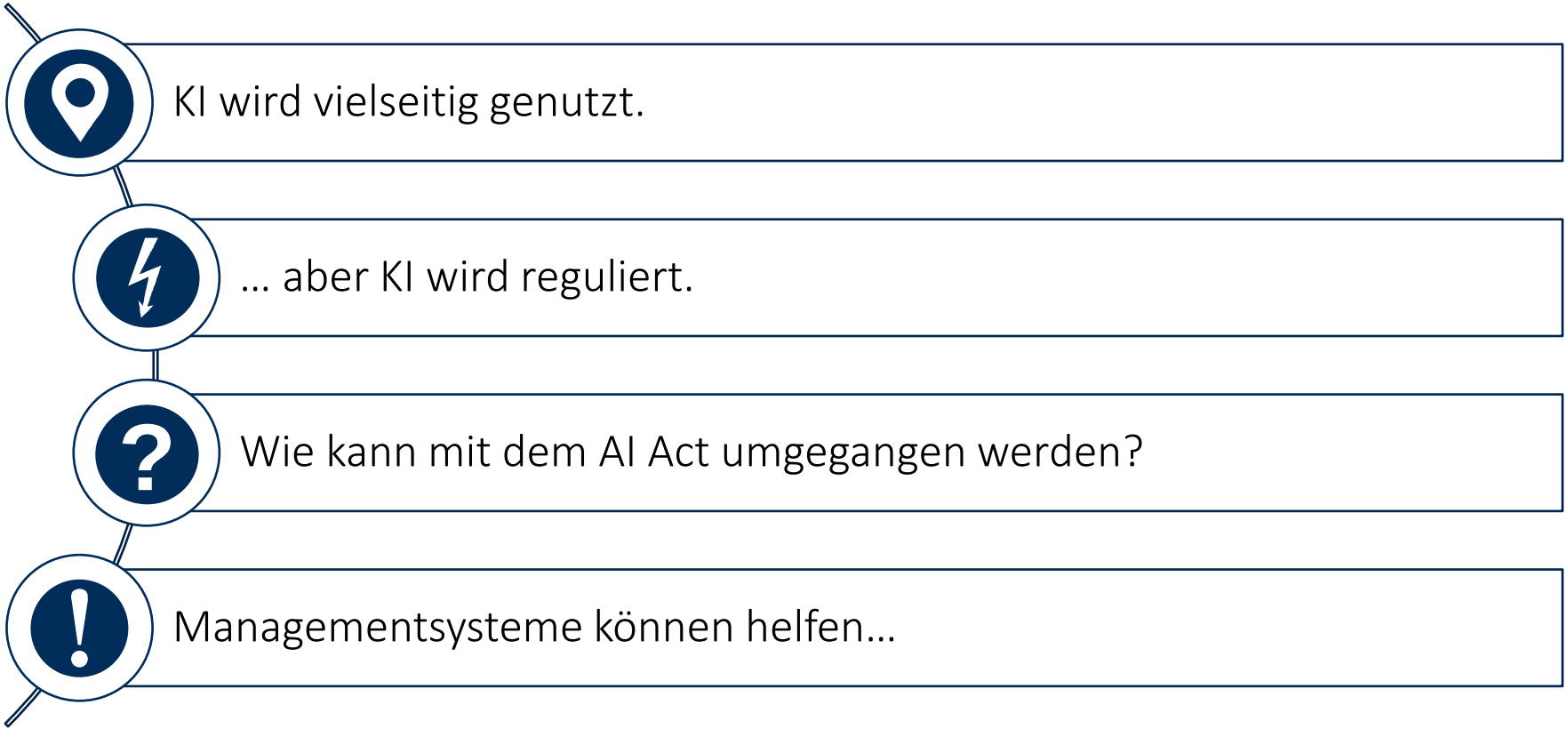
Principal

- Einführung und Auditierung von Informationssicherheitsmanagementsystemen (ISMS) nach ISO 27001 oder ISO 27001 auf Basis IT-Grundschutz
- Erstellung von Sicherheitskonzepten und Koordinierung der Umsetzung
- Erstellung von Richtlinien und Regelungen
- Beratung zum Risikomanagement und Durchführung von Risikoanalysen
- Durchführung von Workshops zu Informationssicherheitsthemen

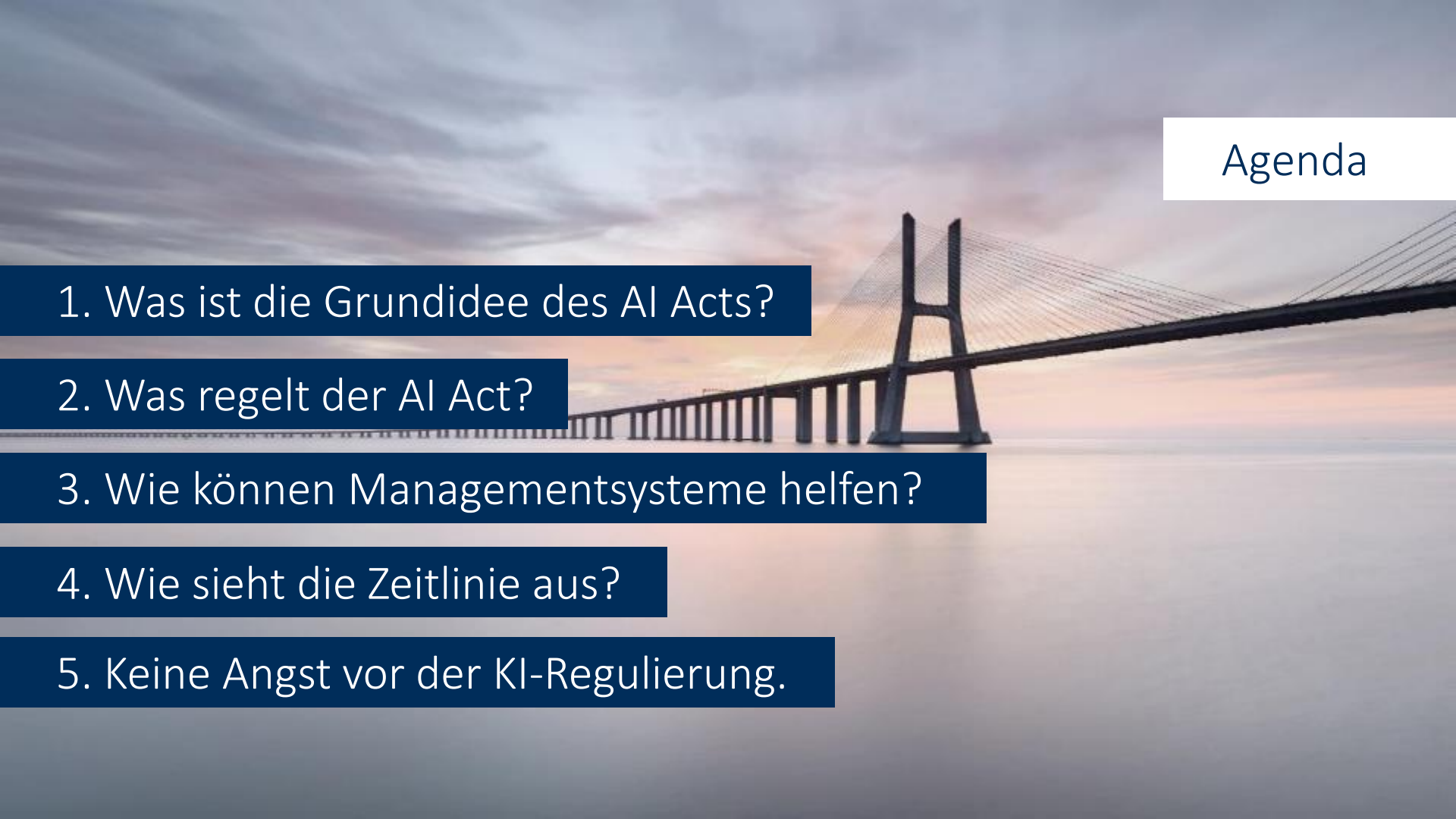
---

- ISO 27001 Lead Auditor
- ISO 22301 Lead Auditor
- Auditor IT-Si.-Kat. nach EnWG 11 Abs. 1a und 1b
- Auditteamleiter für ISO-27001-Audits auf der Basis von IT-Grundschutz
- IS-Revisions- und -Beratungsexperte auf der Basis von IT-Grundschutz
- IT-Grundschutz-Berater
- Prüfverfahrenskompetenz nach § 8a BSIG

Wie sollte mit dem AI Act umgegangen werden?



Agenda



1. Was ist die Grundidee des AI Acts?
2. Was regelt der AI Act?
3. Wie können Managementsysteme helfen?
4. Wie sieht die Zeitlinie aus?
5. Keine Angst vor der KI-Regulierung.

1. Was ist die Grundidee des AI Acts?

Die Grundidee des AI Acts

Menschen & Grundrechte schützen

Transparenz & Vertrauen schaffen

Innovation & fairen Markt fördern

Risikobasierter Regelungsrahmen

2. Was regelt der AI Act?

Der EU AI Act stellt komplexe Anforderungen an KI.

KI-Systeme

- „Verbotene Praktiken“ (unannehmbares Risiko)
- „Hoch-Risiko KI-Systeme“ (hohes Risiko)
- „Bestimmte KI-Systeme“ (begrenztes Risiko)
- Nicht regulierte KI-Systeme (geringes Risiko)

Akteure


Produkthersteller

Anbieter

Bevollmächtigter

Händler


Einführer


Betreiber

- „KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko“
- „KI-Modelle mit allgemeinem Verwendungszweck“
- „frei und quelloffen“ (ohne systemisches Risiko)

KI-Modelle mit allgemeinem Verwendungszweck

EU

- Reallabore
- Büro für KI
- Gremium
- Beratungsforum
- Wiss. Gremium

DB für Hoch-Risiko-KI

national

- Nat. Behörden
- Nat. Anlaufstellen

Innovation & Governance

Von Verboten bis nicht definiert.

KI-Systeme

„Verbotene Praktiken“ (unannehmbares Risiko)

„Hoch-Risiko KI-Systeme“ (hohes Risiko)

„Bestimmte KI-Systeme“ (begrenztes Risiko)

Nicht-regulierte KI-Systeme (geringes Risiko)

KI darf nicht alles in Europa.

Verboten sind…

Manipulation, Beeinflussung und Ausnutzung

Social Scoring und Profiling*

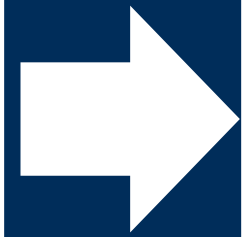
biometrische Erkennung, Überwachung und Kategorisierung*

* mit Ausnahmen

Hochrisiko-KI-Systeme stehen unter besonderer Aufsicht.

Hochrisiko-KI-Systeme beinhalten:

- Sicherheitsbauteile
- Biometrie
- KRITIS
- Bildung
- Beschäftigung, Personalmanagement und Zugang zur Selbständigkeit
- Private und öffentliche Dienste und Leistungen
- Strafverfolgung
- Migration, Asyl und Grenzkontrolle
- Rechtspflege und demokratische Prozesse



Pflichten:

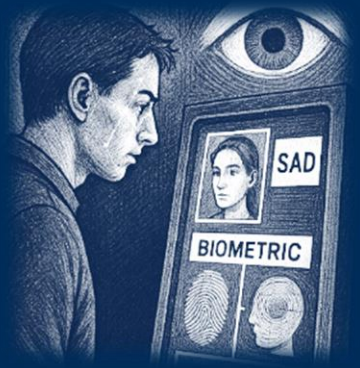
- Registrierung
- Risikomanagementsystem
- Daten und Daten-Governance
- Technische Dokumentation
- Aufzeichnungspflichten
- Transparenz und Bereitstellung von Informationen
- Menschliche Aufsicht
- Genauigkeit, Robustheit und Cybersicherheit
- (zusätzliche „Akteur“-spezifische Pflichten)
- …

Sinngemäß: Wo KI kritische Entscheidungen trifft…

„Bestimmte Systeme“ haben Transparenzpflichten.

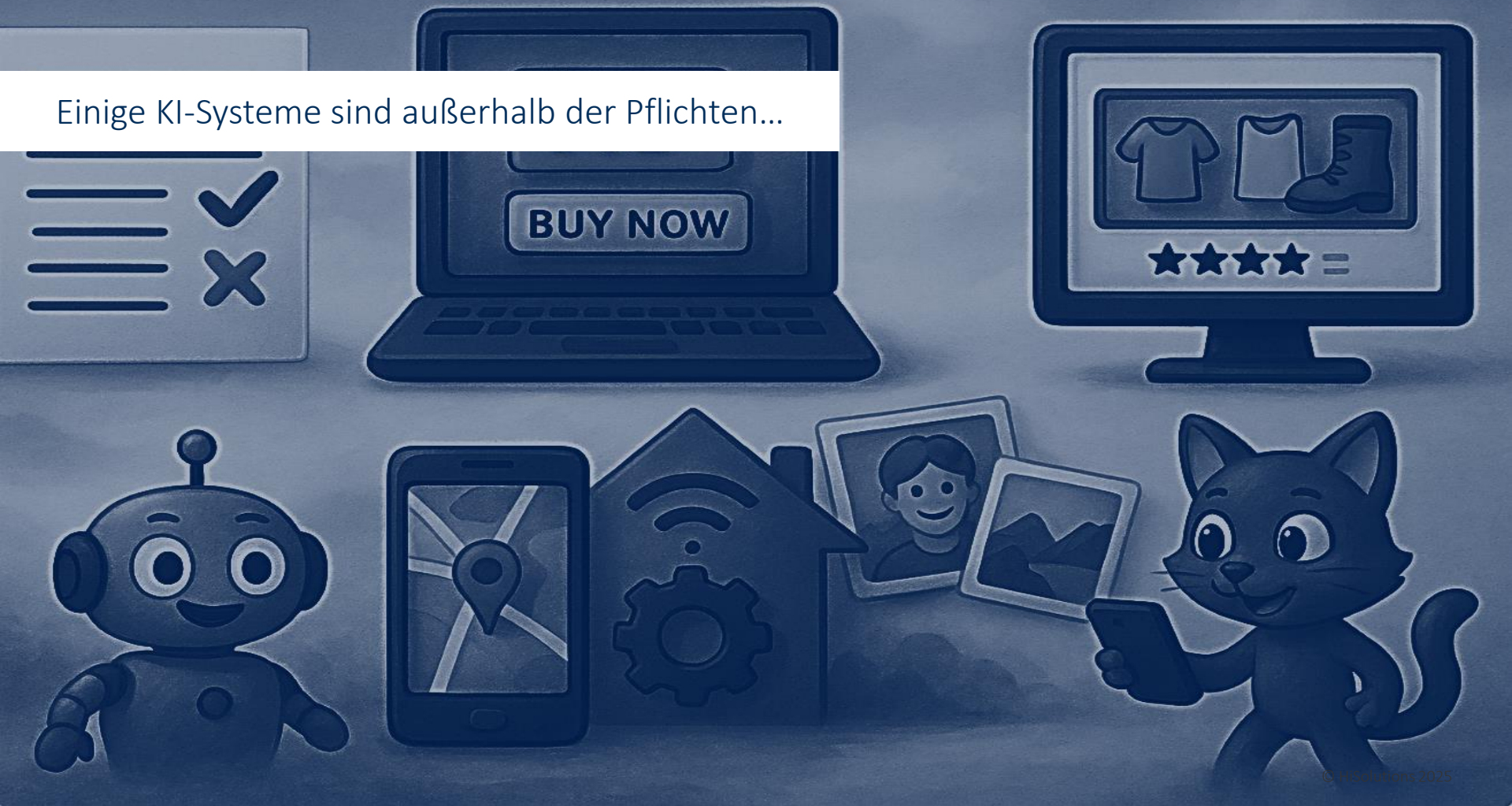
Interaktion

Manipulation oder Generation von Bild, Text oder Videos.



Emotionserkennung oder biometrische Kategorisierung

Einige KI-Systeme sind außerhalb der Pflichten…



Geschult werden muss aber quasi immer.

AI Act - Artikel 4:

„Die **Anbieter und Betreiber** von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr **Personal und andere Personen**, die in ihrem Auftrag mit dem **Betrieb und der Nutzung** von KI-Systemen befasst sind, über ein **ausreichendes Maß an KI-Kompetenz** verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind.“

Der EU AI Act stellt komplexe Anforderungen an KI.

KI-Systeme

- „Verbotene Praktiken“ (unannehmbares Risiko)
- „Hoch-Risiko KI-Systeme“ (hohes Risiko)
- „Bestimmte KI-Systeme“ (begrenztes Risiko)
- Nicht regulierte KI-Systeme (geringes Risiko)

Akteure


Produkthersteller

Anbieter

Bevollmächtigter

Händler


Einführer


Betreiber

- „KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko“
- „KI-Modelle mit allgemeinem Verwendungszweck“
- „frei und quelloffen“ (ohne systemisches Risiko)

KI-Modelle mit allgemeinem Verwendungszweck

EU

- Reallabore
- Büro für KI
- Gremium
- Beratungsforum
- Wiss. Gremium

DB für Hoch-Risiko-KI

national

- Nat. Behörden
- Nat. Anlaufstellen

Innovation & Governance

GPAI können nach drei Kategorien unterschieden werden.

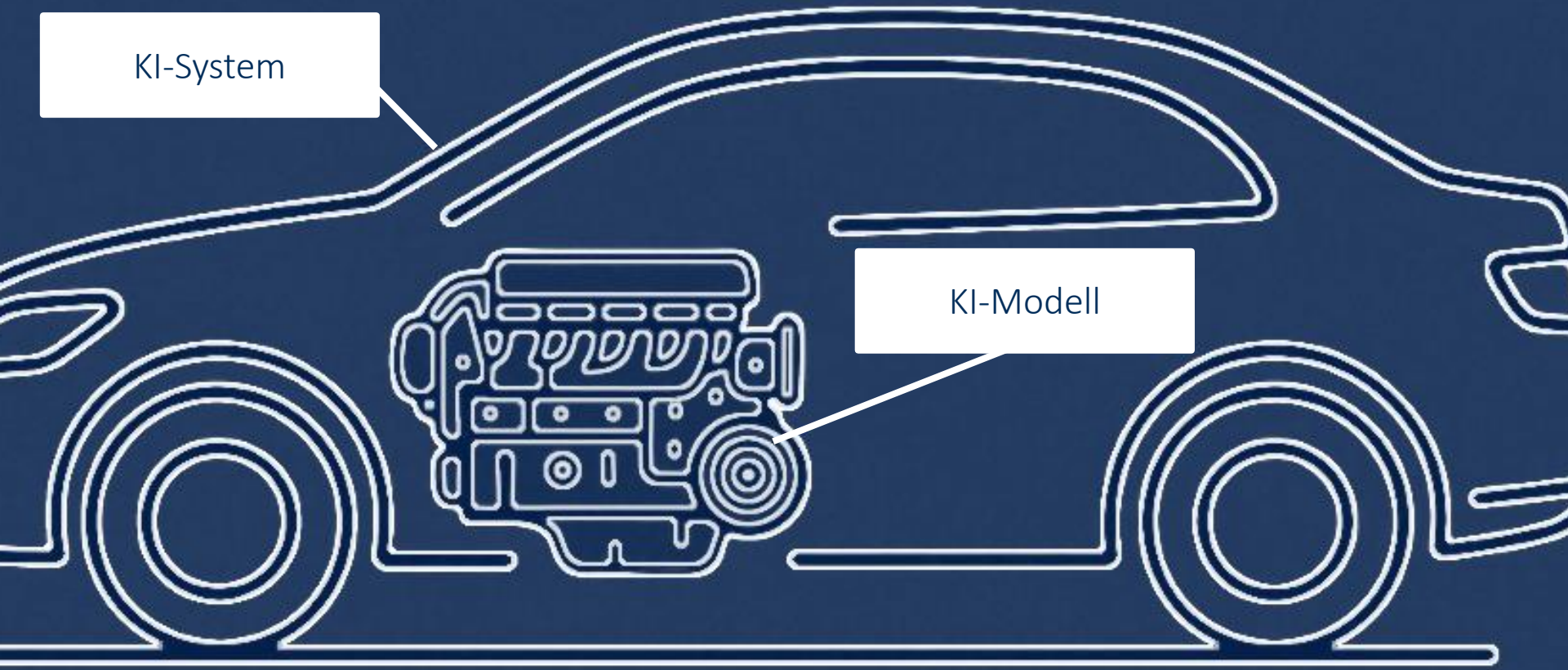
„KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko“

„KI-Modelle mit allgemeinem Verwendungszweck“

„frei und quelloffen“ (ohne systemisches Risiko)

KI-Modelle mit allgemeinem Verwendungszweck

Das Modell ist der Motor für das System.



Bei einem „hohen Wirkungsgrad“ besteht ein „systemisches Risiko“

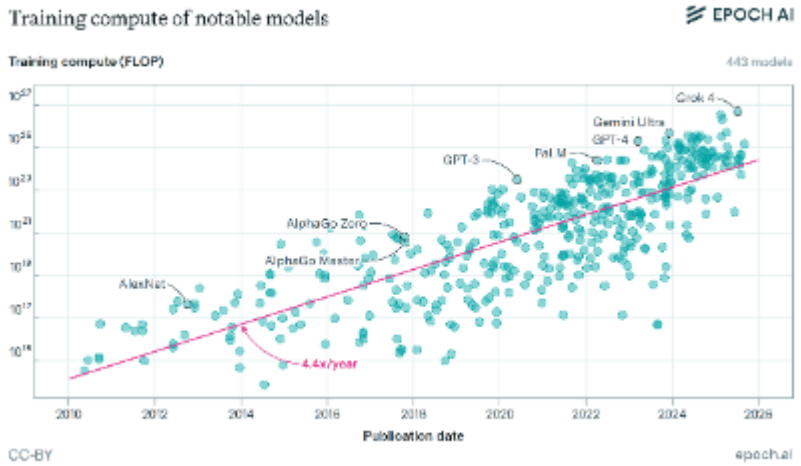
„Systemisches Risiko“
=

„hoher Wirkungsgrad“

=

a) Bewertung oder Entscheidung

b) Training mit > 10^{25} FLOPs



Quelle: https://epoch.ai/data/ai-models?view=table

„Mit großer Macht kommt große Verantwortung“

KI-Modelle mit allgemeinem Verwendungszweck

- Technische Dokumentation
- Einhaltung des Urheberrechts
- Zusammenfassung des Trainings
- …

… mit systemischem Risiko

- Meldepflicht
- Risikomanagement
- schwerwiegende Vorfälle erfassen, dokumentieren und melden
- …

Der EU AI Act stellt komplexe Anforderungen an KI.

KI-Systeme

- „Verbotene Praktiken“ (unannehmbares Risiko)
- „Hoch-Risiko KI-Systeme“ (hohes Risiko)
- „Bestimmte KI-Systeme“ (begrenztes Risiko)
- Nicht regulierte KI-Systeme (geringes Risiko)

Akteure


Produkthersteller

Anbieter

Bevollmächtigter

Händler


Einführer


Betreiber

- „KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko“
- „KI-Modelle mit allgemeinem Verwendungszweck“
- „frei und quelloffen“ (ohne systemisches Risiko)

KI-Modelle mit allgemeinem Verwendungszweck

EU

- Reallabore
- Büro für KI
- Gremium
- Beratungsforum
- Wiss. Gremium

DB für Hoch-Risiko-KI

national

- Nat. Behörden
- Nat. Anlaufstellen

Innovation & Governance

Wer bin ich? Und wenn ja, wieviele?

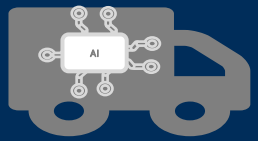
Akteure

Produkthersteller

Anbieter

Bevollmächtigter

Händler



Einführer

Betreiber

Der EU AI Act stellt komplexe Anforderungen an KI.

KI-Systeme

- „Verbotene Praktiken“ (unannehmbares Risiko)
- „Hoch-Risiko KI-Systeme“ (hohes Risiko)
- „Bestimmte KI-Systeme“ (begrenztes Risiko)
- Nicht regulierte KI-Systeme (geringes Risiko)

Akteure


Produkthersteller

Anbieter

Bevollmächtigter

Händler


Einführer


Betreiber

- „KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko“
- „KI-Modelle mit allgemeinem Verwendungszweck“
- „frei und quelloffen“ (ohne systemisches Risiko)

KI-Modelle mit allgemeinem Verwendungszweck

EU

- Reallabore
- Büro für KI
- Gremium
- Beratungsforum
- Wiss. Gremium

DB für Hoch-Risiko-KI

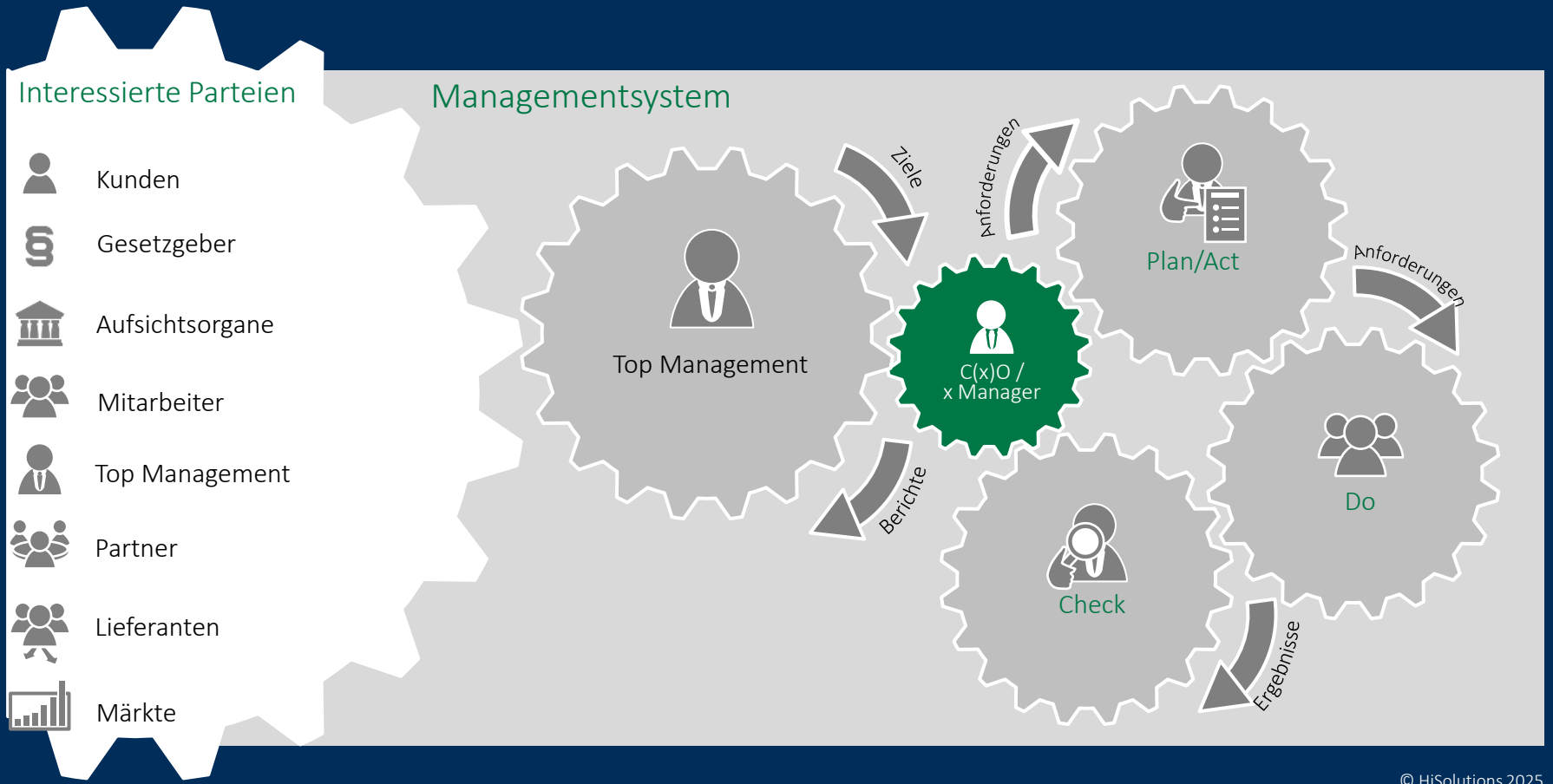
national

- Nat. Behörden
- Nat. Anlaufstellen

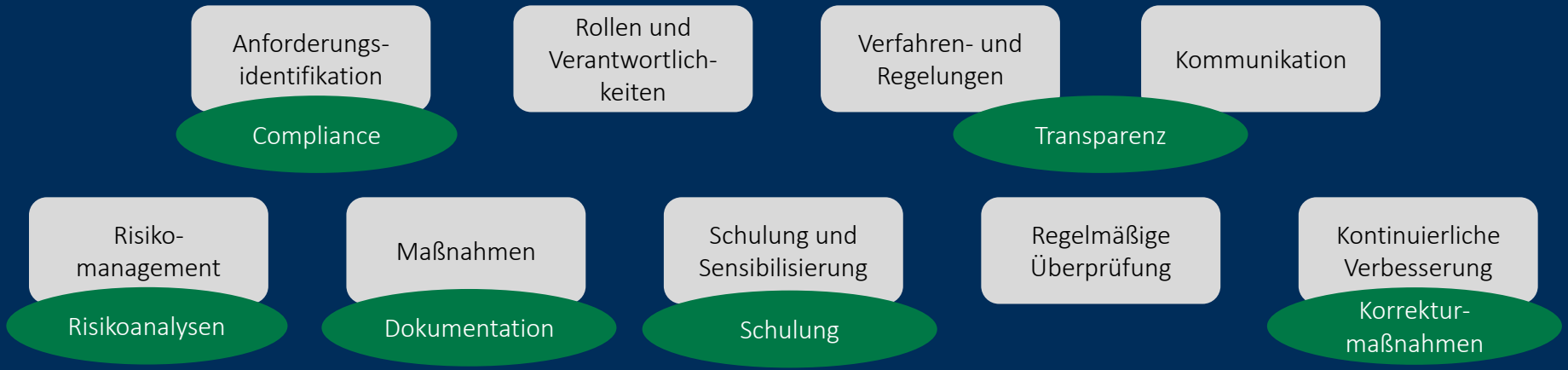
Innovation & Governance

Wie können Managementsysteme helfen?

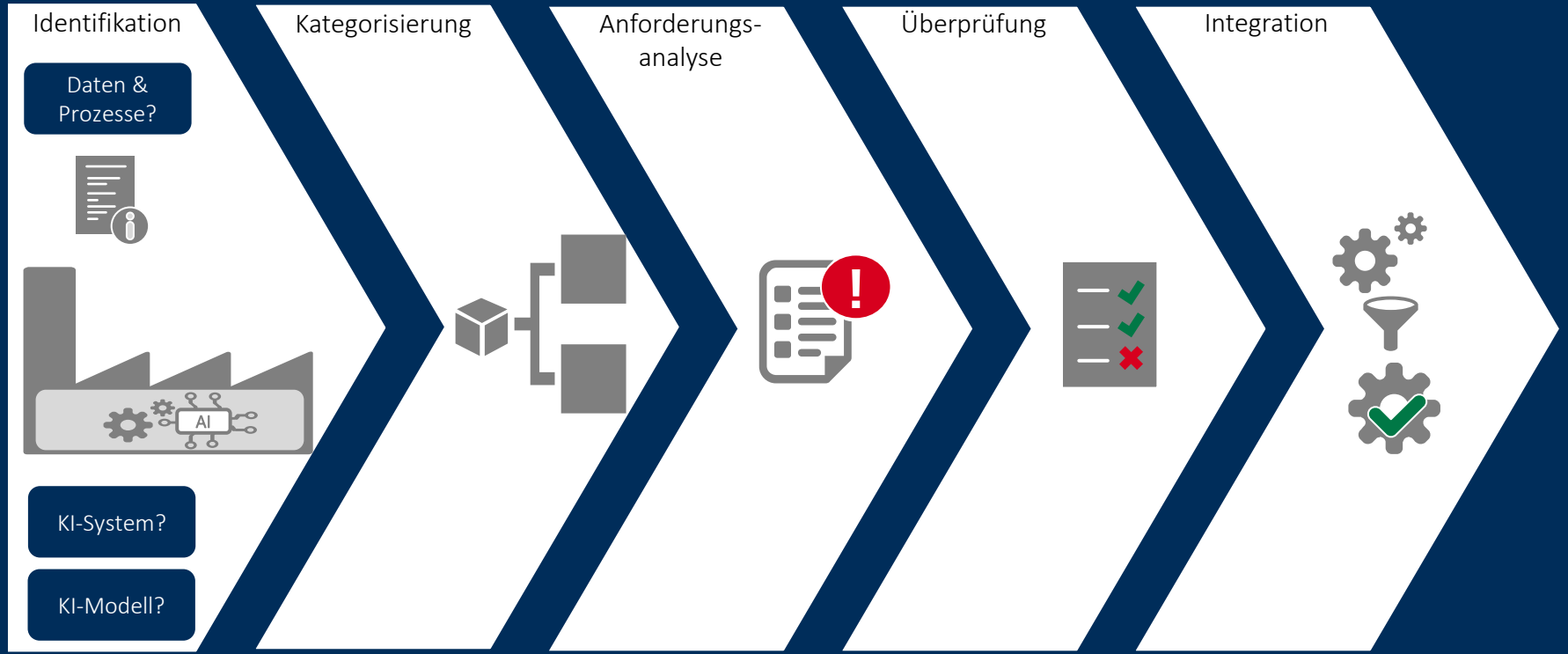
Anforderungen können in einem Managementsystem behandelt werden.



Die Anforderungen aus dem AI Act lassen sich in die unterschiedlichen Bestandteile eines Managementsystems integrieren.



Eine strukturierte Vorgehensweise ist wichtig, um Anforderungen zu identifizieren und Konformität herzustellen.



Wie sieht die Zeitlinie aus?

Vergangene Termine

12.07.2024
Veröffentlichung

01.08.2024
Inkrafttreten

02.02.2025 – Kap. I und Kap. II
- Anforderungen an die KI-Kompetenz
- Verbotene Praktiken

02.08.2025
- Benannte Stellen(Kapitel III, Abschnitt 4),
- GPAI-Modelle (Kapitel V),
- Governance (Kapitel VII),
- Vertraulichkeit(Artikel 78)
- Sanktionen (Artikel 99 und 100)

Zukünftige Termine

02.08.2026
Verbleibende Bestimmungen des AI Acts außer Artikel 6 Absatz 1 („Sicherheitsbauteile“)

02.08.2027
Artikel 6 Absatz 1 – („Sicherheitsbauteile“)

Keine Angst vor der KI-Regulierung.

Keine Angst vor der KI-Regulierung

- Kein Innovationskiller – verantwortungsvolle Nutzung
- Managementsysteme können bei kontinuierlicher Integration von Anforderungen helfen
- Eine strukturierte Vorgehensweise ist wichtig

Heute vorbereiten …

… morgen vertrauenswürdig und wettbewerbsfähig sein.

Fragen?

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com