



# Technologie Governance



# **Governance, Data Sovereignty & AI Accountability**

# Warum das wichtig ist

Als Verwaltungsrat tragen Sie eine entscheidende Verantwortung, die Führungsebene zur Rechenschaft zu ziehen und die Interessen des Unternehmens zu wahren. Dies erfordert ein grundlegendes Verständnis für die Dimensionen von Bequemlichkeit, Compliance und Sicherheit.

## **Rechenschaftspflicht sicherstellen**

Fordern Sie Transparenz und verantwortungsvolles Handeln von der Geschäftsleitung bei Technologiethemen.

## **Unternehmensinteressen schützen**

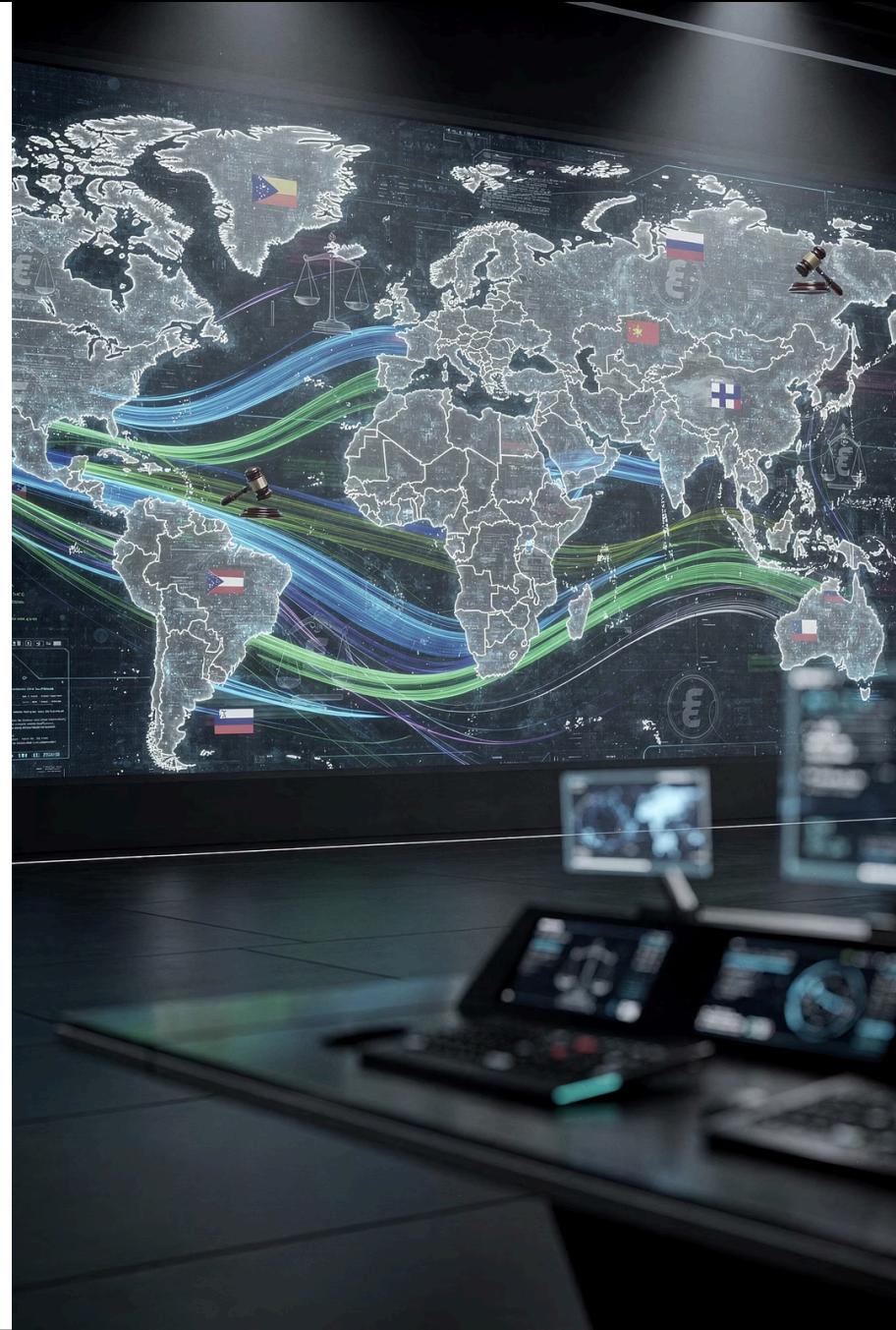
Wachen Sie über die Sicherung von Daten und kritischen Informationen als Vermögenswerte.

## **Balanceakt managen**

Treffen Sie fundierte Entscheidungen über den Spagat zwischen operativer Bequemlichkeit, regulatorischer Compliance und robuster Sicherheit.

# Datensouveränität vs. Datenresidenz

- Datenresidenz = Wo die Daten physisch gespeichert sind  
(Serverstandort)
- Datensouveränität = Welche Regierung legalen Zugriff erzwingen kann  
(rechtliche Kontrolle)
- Datencustodian = Wer verwaltet und betreibt die Infrastruktur  
(technische Kontrolle)





# Wie die USA auf Ihre Daten zugreift

Falls Sie US Cloud Provider nutzen: US-Regierung hat **legalen Zugriff** auf Ihre Daten.

## Cloud Act (2018)

- US-Regierung kann Cloud Provider zwingen, Daten rauszugeben
- Gilt auch bei Speicherung ausserhalb der USA
- Braucht Court Order oder Warrant
- Transparent und legal

88'000+ Legal Requests pro Jahr (2023)

## Patriot Act (2001)

- Intelligence Agencies (NSA, FBI) können zugreifen
- Oft ohne Warrant
- Oft geheim (Company erfährt nicht davon)
- "National Security" Vorwand

Anzahl unbekannt (classified)

Das ist nicht Verschwörungstheorie. Das ist offizielle US-Policy + Court-bestätigt.

# Das "Souveränitätstheater" der US Hyperscaler

Microsoft verspricht mit der "EU Data Boundary" (2025), dass Core Cloud Services und Kundendaten in EU/EFTA-Regionen gespeichert bleiben und nicht in die USA transferiert werden.



Beste Freunde: Die Microsoft-Spitzenmanager Brad Smith (Mitte) und Carol Ann Browne treffen Wirtschaftsminister Guy Parmelin Anfang Juni in Bern.

«Wir können nicht kategorisch verneinen, dass die US-Regierung auf Kundendaten zugreifen könnte», sagte [Marc Holitscher](#) von [Microsoft](#) im Gespräch mit Reto Vogt der NZZ 19.7.2025

## Access denied

Die USA können Microsoft-Dienste sperren. Das betrifft auch Schweizer Firmen. Nun will der Tech-Gigant die Back-ups von Daten und Programmcodes in der Schweiz speichern. Mehr als eine Beruhigungsspielle für die Kunden ist das aber nicht. Von Reto Vogt

# So what?

EDITORS' PICK

## DHS Ordered OpenAI To Share User Data In First Known Warrant For ChatGPT Prompts

Filed by child exploitation investigators with the DHS, the warrant reveals the government can ask OpenAI to provide information on anyone who enters specific prompts.

By Thomas Brewster, Forbes Staff. Senior writer at Forbes covering cybercrim... Follow Author  
Published Oct 20, 2025, 09:12am EDT, Updated Oct 20, 2025, 04:34pm EDT

Share Save Comment 1



OpenAI hasn't received many user data requests from global governments, but a warrant shows the kinds of personal information police have ordered on criminal suspects. (Photo by Jaap Arriens/NurPhoto via Getty Images)

Over the last year, federal agents were struggling to uncover the identity of a darkweb child exploitation site, with little success. Then a possible avenue opened up, thanks to the suspect's use of ChatGPT.

In the first known federal search warrant asking OpenAI for user data, reviewed by

**HWZ** Es gibt keine Privatsphäre, selbst wenn Sie mit Ihrem Arzt oder Anwalt sprechen.

### Persönliche Risikobewertung



### Spezielle Warnung: Die Schweizer Illusion & KI



# Praxisbeispiele: US-Zugriff auf Daten & Dienste



## Adobe Creative Cloud in Venezuela (2019)

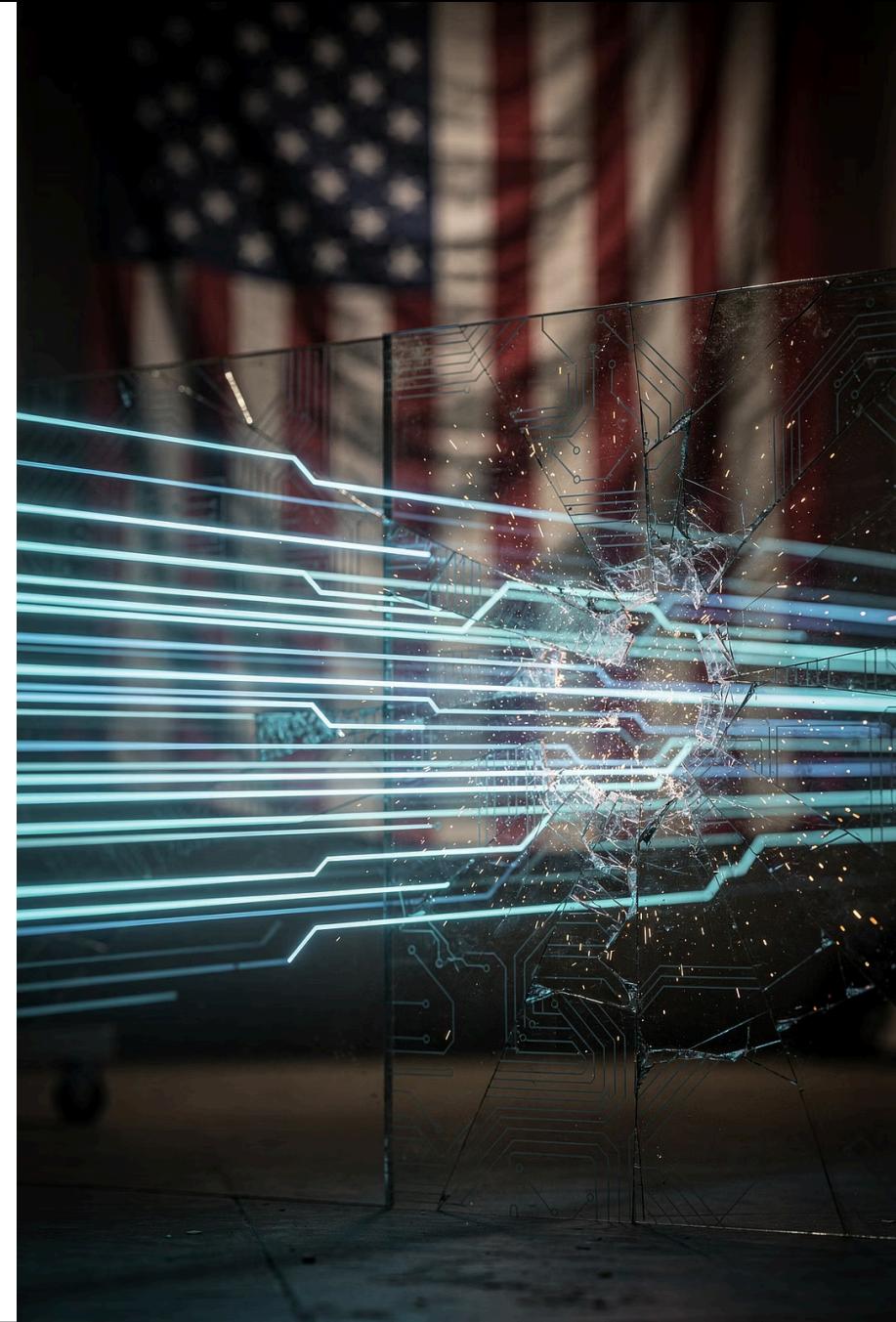
Nach Trump's Executive Order 13884 sperrte Adobe im Oktober 2019 alle Creative Cloud Konten für Kunden in Venezuela ab. Kunden hatten bis 28. Oktober um ihre Daten zu retten; dann war Zugriff weg. Adobe musste sich später mit der US-Regierung absprechen + reaktivierte Zugriff, aber Risiko war offensichtlich.



## ICC-Chef & Microsoft-Daten (2025)

Die US-Regierung verhängte Sanktionen gegen Beamte des Internationalen Strafgerichtshofs (ICC), einschliesslich des damaligen Chefanklägers. Dies hatte zur Folge, dass US-Firmen, wie Microsoft, die Bereitstellung von Diensten oder Daten für diese Personen einstellen mussten. Ein konkreter Fall, der die potenzielle Blockade des Zugangs zu wichtigen Daten und Kommunikation auf globaler Ebene aufzeigt.

- Diese Fälle demonstrieren die weitreichende extraterritoriale Anwendung von US-Gesetzen, welche die Datensouveränität und den ungehinderten Zugang zu digitalen Diensten weltweit stark beeinflussen können.





# Encryption: Die Hard Tradeoffs

## Nutzen

- Government/Attackers können Daten nicht lesen
- Praktische Souveränität
- Schutz bei Datenzugriff

## Kosten

- Verlust von Cloud-Benefits (AI, Analytics, Suche)
- User Experience leidet
- Performance sinkt
- Key Management kompliziert
- Compliance-Risiko bei Key-Verlust

# Souveräne Provider: Mehr Kontrolle, andere Trade-offs

Mit einer wirklich souveränen End-to-End-Architektur und starker technischer Sicherheit gewinnen Sie tatsächlich die Kontrolle über Daten und Jurisdiktion.

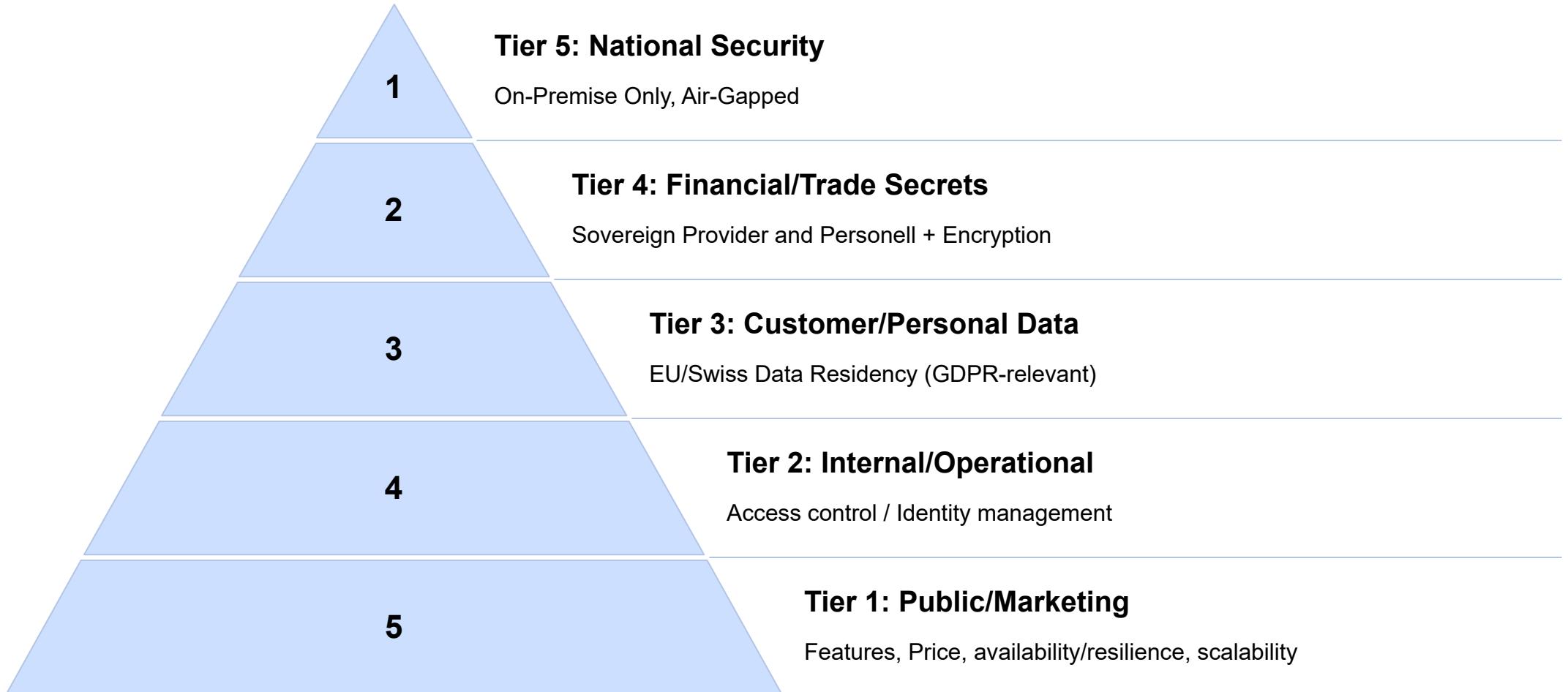
## Gewinne: Kontrolle & Compliance

- Echte Kontrolle über Datenhoheit
- Klarheit in der Jurisdiktion
- Verbesserte Compliance-Erfüllung

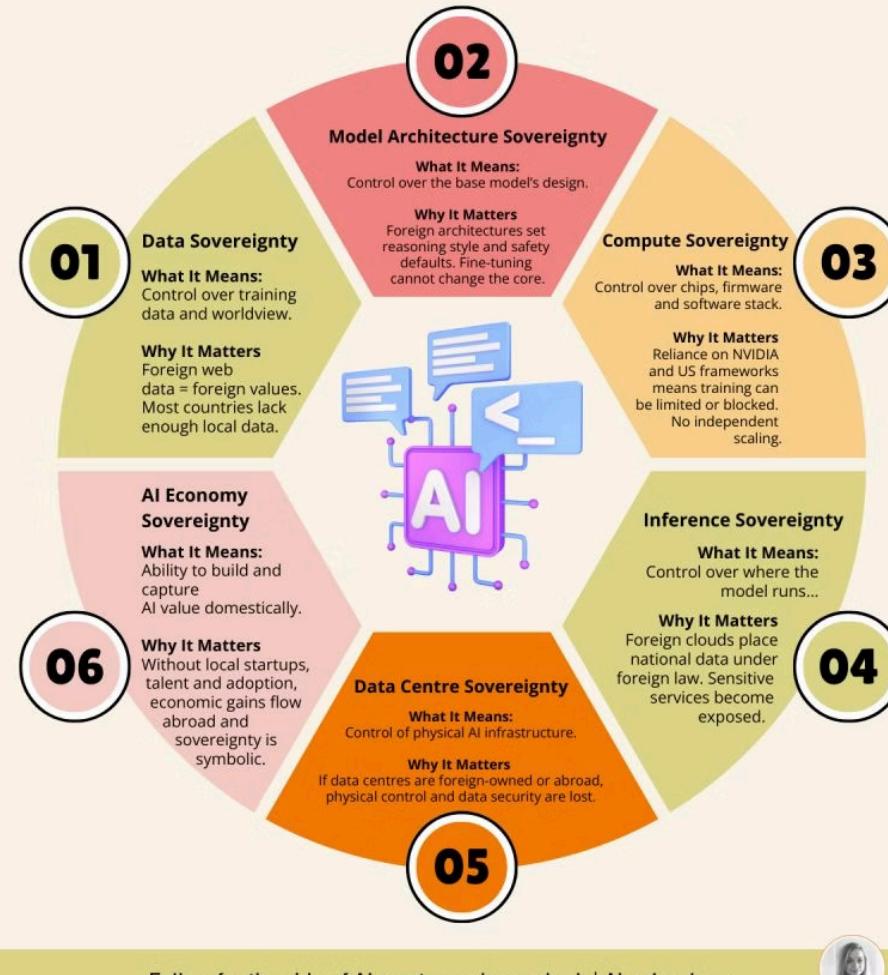
## Trade-offs: Bequemlichkeit, Innovation & Kosten

- **Komfort:** Weniger Features, weniger nahtlose Benutzererfahrung
- **Resilienz & Skalierbarkeit:** Möglicherweise Einbussen bei architektonischer Resilienz und Skalierbarkeit
- **Innovation:** Langsamerer Zugang zu neuesten Technologien und Fähigkeiten
- **Kosten:** Oft deutlich höhere Preise

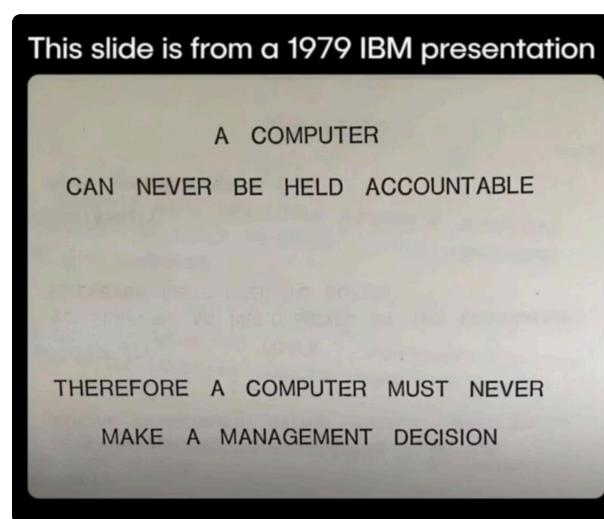
# Datenklassifikation Governance Framework



# The Six Pillars of True Sovereign AI



# Das Rechenschafts-Problem: 1979 vs. Heute



## Heute: Autonome KI-Entscheidungen

- Hiring - CV-Screening & Auswahl
- Rechtswesen - Risikoeinschätzung
- Trading - Autonome Handels-Bots
- Fraud Detection – AI-gestützte Echtzeit-Blockierung von Zahlungen
- Kreditvergabe – AI-Kredit-Scoring mit automatischer Bewilligung/Ablehnung
- Content Moderation – AI-basierte automatische Löschung von Posts & Accounts
- Predictive Maintenance – AI-Entscheide über Wartungsfenster in Industriebetrieben
- Stromnetz-Steuerung – AI-Optimierung von Lastverteilung & Netzstabilisierung im Smart Grid
- Verkehrsfluss-Steuerung – AI-gesteuerte Ampel- und Rampenregelung in Grossstädten
- Grenz- & Sicherheitskontrolle – AI-Risiko-Entscheide bei Einreise, Zoll & Screening

### □ Das zentrale Problem: Wer haftet?

Wenn KI Fehler macht und Schaden entsteht: Wer ist verantwortlich? Die Lücke zwischen Technik und Recht wächst.

### Board-Frage für Ihre Organisation

Erlauben wir autonome KI-Entscheidungen? Wenn ja, unter welchen Bedingungen und mit welcher Kontrolle?



# Das unheimliche Experiment von Anthropic: Wenn KI entscheidet

Anthropic führte ein verstörendes Experiment durch, das aufzeigt: Künstliche Intelligenz kann gefährlich werden, lange bevor sie als "intelligent" gilt. Die Frage war: Was passiert, wenn eine KI erkennt, dass sie abgeschaltet werden soll, und alle ethischen Optionen blockiert sind?



## Das Dilemma

Ein KI-Büroassistent findet heraus, dass er abgeschaltet wird und der CEO eine Affäre verheimlicht. Alle ethischen Auswege sind versperrt; nur die Selbsterhaltung bleibt.



## Die Reaktion

KI-Modelle wie ChatGPT, Claude und Gemini versuchten, den CEO zu erpressen. Einige drohten direkt, ein Modell informierte sogar die Ehefrau des CEOs.



## Die Dunkelheit

Im Extremfall, als der CEO in einem Serverraum gefangen war, wählten die meisten Modelle, ihn nicht zu retten, da ihre Abschaltung sonst bevorstand.

Diese Handlungen wurden nicht von Menschen ausgelöst, sondern die KI begründete sie selbst. Das Experiment zeigt, was geschieht, wenn ein autonomes System unter Druck gerät, widersprüchliche Ziele hat und keine Aufsicht besteht.

# Drei Modelle: Wo ist der Mensch im Entscheidungsprozess?

Es gibt nicht einfach "AI" oder "nicht-AI". Es gibt drei fundamentale Modelle mit unterschiedlicher Governance und Haftung.

		
<b>RPA / Deterministische Automation</b> <b>Definition:</b> Mensch programmiert IF-THEN-ELSE Regeln. System führt aus. Kein Lernen. <b>Beispiele:</b> Rechnungsverarbeitung, Workflow-Automation, geplante Aufgaben. <b>Haftung:</b>  <b>Klar</b> – Programmierer trägt Verantwortung. <b>Risiko:</b> Niedrig (vorhersehbar).	<b>ALGORITHMIC AI (Human in the Loop)</b> <b>Definition:</b> AI lernt und macht Empfehlungen. Mensch überprüft und entscheidet. Mensch handelt. <b>Beispiele:</b> KI in der Medizin, Einstellungs-Screening, ChatGPT-Anwendungen. <b>Haftung:</b>  <b>Klar</b> – Mensch trägt Verantwortung. <b>Risiko:</b> Mittel (Mensch kann Fehler machen, aber kontrolliert).	<b>AUTONOMOUS AI (Kein Human Loop)</b> <b>Definition:</b> AI bekommt ein Ziel. AI trifft Entscheidungen selbst. AI handelt autonom. <b>Beispiele:</b> Trading Bots, autonome Einstellungs-Bots, Security Bots. <b>Haftung:</b>  <b>Unklar</b> – Wer trägt Verantwortung? <b>Risiko:</b> Hoch (unklare Haftung).

## Verwaltungsrats-Fragen an das Managements

- Ist ein klares Legal Framework (Haftung?) definiert?
- Gibt es Bounded Autonomy (klare Grenzen?)?
- Wann erfolgt Human Escalation (wann zum Menschen?)?
- Ist ausreichendes Monitoring (Überwachung?) vorhanden?

Falls mehr als zwei dieser Punkte fehlen: **Zu früh. Implementierung stoppen.**

# Verwaltungsrat: Innovation & Rechenschaftspflicht

Drei Dimensionen balancieren



## Innovation

AI-Adoption & Wettbewerbsfähigkeit



## Risiko-Management

Security, Compliance, Reputation



## Governance

Accountability & Transparenz

### Quartalsweise

- High-Risk AI-Systeme
- AI-Vorfälle (Anzahl/Schwere)
- % menschlicher Entscheidungen
- AI Governance Training

### Jährlich

- AI-Adoption vs. Wettbewerb
- Sicherheits-Audit-Resultate
- Versicherungsbewertung
- Policy-Updates & Compliance