KI Briefing #8

KI-GOVERNANCE

Was ein sicheres Unternehmenssystem in Bezug auf KI leisten muss

Wenn Richtlinien allein nicht reichen

Ein Team verwendet ChatGPT für den monatlichen Bericht. In der Fachabteilung wird ein Chatbot getestet. Eine Mitarbeiterin fragt, ob sie Copilot auch mit Kundendaten nutzen darf. Es sind keine Einzelfälle – und keine IT-Themen. Immer mehr Entscheidungen zum KI-Einsatz werden dezentral, still und oft gut gemeint getroffen. Doch was passiert, wenn etwas schiefläuft? Wer ist verantwortlich – und woran erkennt man, was erlaubt ist?

Viele Unternehmen führen aktuell Regeln ein: Tool-Listen, Hinweise zur Datennutzung, Prompt-Guides. Doch das allein reicht nicht. **Sichere KI-Nutzung braucht ein System**: eines, das Zuständigkeiten klärt, Risiken berücksichtigt und trotzdem nicht Innovation verhindert.

Governance ist kein Regelwerk – sondern ein Betriebssystem

Der Begriff „Governance" wirkt oft abstrakt. Doch im Kern beschreibt er etwas sehr Praktisches: **Wie ein Unternehmen etwas regelt, das neu, unübersichtlich oder risikobehaftet ist.** Governance bedeutet nicht Kontrolle im Sinne von Überwachung – sondern Steuerung im Sinne von Verantwortung, Klarheit und Nachvollziehbarkeit.

Bei KI geht es dabei um **Fragen** wie:

- Wer darf KI einsetzen – und wofür?
- Welche Daten dürfen genutzt werden – und unter welchen Bedingungen?
- Was passiert, wenn ein Ergebnis falsch, unangemessen oder riskant ist?
- Welche Rolle hat Führung – und wo endet sie?

Governance ist kein IT-Projekt

Die Verantwortung für KI-Governance liegt oft fälschlich bei der IT. Doch technische Infrastruktur ist nur ein Baustein. Entscheidend ist die **organisationale Steuerungsfähigkeit** – also ob das Unternehmen in der Lage ist, KI-Nutzung vorausschauend zu regeln. Das umfasst:

- **Einbettung in bestehende Führungsprozesse** (z. B. Projektfreigaben, Change Management)
- **Schnittstellen zu Recht, Datenschutz, Kommunikation und Personal**
- **Vorgaben für externe Partnerschaften, Tools und Lizenzen**
- **Verfahren zur Meldung und Bewertung von Zwischenfällen**

Wer Governance richtig aufsetzt, spart sich viele spätere Eskalationen – weil **Entscheidungen nachvollziehbar und abgestimmt** sind, bevor Probleme entstehen.

Drei mögliche Steuerungsmodelle: zentral, dezentral, hybrid

Nicht jede Organisation steuert gleich und nicht jede Governance muss identisch aufgebaut sein. Entscheidend ist, dass Zuständigkeiten klar sind und das System tragfähig bleibt. In der Praxis haben sich drei Grundmodelle herausgebildet, mit denen Unternehmen den KI-Einsatz regeln:

1. Zentralisiertes Modell – einheitlich, aber langsam

In diesem Ansatz liegt die Steuerung bei einer zentralen Stelle – oft in der Rechtsabteilung oder einer Governance-Unit. Alle Entscheidungen, Freigaben und Eskalationen laufen über dieses Gremium.

- **Vorteile**: klare Linie, hohe juristische Absicherung, konsistente Entscheidungen
- **Nachteile**: hohe Belastung der zentralen Stelle, geringe Flexibilität, lange Reaktionszeiten
- **Einsatz sinnvoll, wenn**: die Organisation klein ist oder hohe regulatorische Anforderungen bestehen

2. Dezentrales Modell – praxisnah, aber risikobehaftet

Hier regeln Fachbereiche oder Projekte eigenverantwortlich, wie sie KI einsetzen – im Rahmen übergeordneter Prinzipien oder Leitlinien.

- **Vorteile**: schnelle Entscheidungen, Nähe zum Anwendungsfall, hohe Innovationsfähigkeit
- **Nachteile**: Intransparenz, Inkonsistenzen, erhöhtes Risiko bei sensiblen Anwendungen
- **Einsatz sinnvoll, wenn**: die Organisation reif ist und starke Führungsverantwortung in den Bereichen besteht

3. Hybrides Modell – skalierbar und anschlussfähig

Das hybride Modell kombiniert zentrale Steuerung mit dezentraler Umsetzung. Es gibt einen Governance-Rahmen, definierte Rollen (z.B. „KI-Verantwortliche“ in jedem Bereich) und ein abgestuftes Eskalationssystem.

- **Vorteile**: Kombination aus Konsistenz und Agilität, klare Zuständigkeiten, lernfähige Struktur
- **Nachteile**: höherer Abstimmungsbedarf, Rollen müssen aktiv ausgestaltet werden
- **Einsatz sinnvoll, wenn**: die Organisation wächst, komplex ist oder vielfältige KI-Nutzungen erwartet

Governance ist kein Standardmodell. Es braucht eine passende Architektur – abgestimmt auf Organisationsform, Führungsstil und Reifegrad.

Die Inhalte einer guten KI-Governance

Gute Governance lebt nicht von Umfang, sondern von Klarheit. Es geht nicht darum, jedes Szenario abzudecken – sondern **relevante Entscheidungen so vorzubereiten, dass sie nachvollziehbar, verantwortbar und wiederholbar sind**. Dafür braucht es keine 40-seitigen Richtlinien, sondern eine **klare inhaltliche Ordnung**, die vier zentrale Themenbereiche abdeckt:

1. Zulässigkeit von Anwendungen

Welche Formen der KI-Nutzung sind im Unternehmen grundsätzlich erlaubt, eingeschränkt oder verboten? Dabei geht es z.B. um:

- **Interne Nutzung**: Texterstellung, Protokollierung, Zusammenfassungen u.a.
- **Kundennähe**: Chatbots, E-Mail-Vorlagen, Beratungsunterstützung u.a.
- **Analysefunktione**n: Clustering, Bewertung, Vorhersage u.a.
- **Kreative Inhalte**: Bilder, Videos, Präsentationen u.a.

Ziel: Transparenz darüber, was im Alltag erlaubt ist – und was nicht.

2. Datennutzung und Datenschutz

Hier wird geregelt, welche **Datenarten** für KI-Anwendungen verwendet werden dürfen – und unter welchen Bedingungen. Typische Aspekte sind:

- **Personenbezogene Daten** (z.B. aus Bewerbungen oder Kundensystemen)
- **Unternehmensinterna** (z.B. Strategie, Forschung, Finanzen)
- **Veröffentlichte Quellen** (z.B. Webseiten, externe Berichte)

Ziel: Vermeidung unbeabsichtigter Datenabflüsse und Klärung der Datenhoheit.

3. Qualitätssicherung und Kontrolle

KI-Systeme liefern keine geprüften Ergebnisse. Deshalb muss festgelegt werden:

- Wann muss ein **Ergebnis** geprüft oder ergänzt werden?
- Welche **Standards** gelten für Texte, Analysen oder Empfehlungen?
- Wer trägt die **Verantwortung** für fehlerhafte Ergebnisse?

Ziel: Sicherung der inhaltlichen Integrität – intern wie extern.

4. Rollen, Prozesse, Eskalation

Jede Organisation braucht Klarheit darüber, wer wofür zuständig ist. Dazu gehören:

- **Rollen** wie KI-Verantwortliche, Fachentscheider oder Risiko-Beauftragte
- **Prozesse** für Freigaben, Genehmigungen oder Eskalationen
- **Feedbackwege** bei Problemen, Unklarheiten oder neuen Anwendungsfällen

Ziel: Verlässliche Steuerung, auch bei Unsicherheit oder neuen Tools.

Governance ist nicht nur eine Strukturfrage, sondern auch eine Frage der Inhalte. Sie schafft Vertrauen, wenn sie sich **konkret, verständlich und wirksam auf den Arbeitsalltag auswirkt** – und nicht nur als PDF im Intranet liegt.

Reflexionsfragen

1. Habe ich in meinem Verantwortungsbereich klare Kriterien, wann der Einsatz von KI erlaubt, erwünscht oder riskant ist?
2. Weiß mein Team, an wen es sich bei Unsicherheiten oder Vorfällen wenden kann – und wie der Prozess funktioniert?
3. Habe ich die Rolle, die mir in der Governance zugedacht ist – z.B. als Freigebende:r, Ermöglicher:in oder Eskalationspartner:in – verstanden und angenommen?

Künstliche Intelligenz weiterdenken

Dieses Briefing ist Teil einer Serie für Führungskräfte, die Orientierung rund um KI suchen. Und es ist (natürlich) in enger Zusammenarbeit mit Künstlicher Intelligenz entstanden.

Nächstes Briefing: #9 Zukunftsszenarien mit KI - Was absehbar ist – und was nicht

Unverbindliche Erstberatung: https://calendly.com/freuding/beratung-ki

Bisherige Briefings & weitere E-Books zum Download: ki-briefing.kit.com

Kontakt: Dr. Beate Freuding, freuding@digital-leader.eu, 0152 05188026