DOSSIER

KI-Goverance gestalten

KI-Governance gestalten

Von den ersten Regeln bis zur Umsetzung der EU AI Act Vorgaben

Von der Strategie zu den Regeln

Im Dossier „Entwickeln und Umsetzen einer KI-Strategie“ (gesondertes Dokument, Link auf der letzten Seite) stand die strategische Verortung im Fokus: Wofür setzen wir Künstliche Intelligenz (KI) ein – und warum. Damit ist der Kurs gesetzt. Doch ein Kurs allein verhindert noch keine Zusammenstöße.

Wer eine Strategie hat, braucht als Nächstes **Regeln für die Umsetzung**. Regeln, die festlegen, wer Vorfahrt hat, wer kontrolliert und wer im Zweifel entscheidet.

Stellen Sie sich eine Großstadt ohne Verkehrsordnung vor. Jeder fährt, wann und wohin er will. Manche kommen erstaunlich weit, andere geraten ins Chaos – und irgendwann passiert ein Unfall.

Genau so sieht KI ohne Governance aus: Fachbereiche probieren Tools, Mitarbeitende nutzen ChatGPT für ihre Arbeit, neue Systeme entstehen „nebenbei“. Manchmal geht es gut. Aber wenn etwas schiefläuft, fragt jeder: „Wer war eigentlich verantwortlich?“ – und niemand hat eine Antwort.

Governance ist das, was die Verkehrsregeln für KI schafft. Sie sorgt dafür, dass Innovation möglich bleibt – aber nicht auf Kosten von Sicherheit, Transparenz und Führungsautorität.

Wichtig: **Ab 2026 macht der EU AI Act Governance zur Pflichtaufgabe der Geschäftsleitung**.

Fehlende Strukturen sind dann nicht nur ein organisatorisches Risiko, sondern auch ein rechtliches Haftungsproblem.

Warum Governance unverzichtbar ist

Künstliche Intelligenz hält selten über zentrale Projekte Einzug, sondern meist still und dezentral:

- Ein Team verwendet ChatGPT für den Monatsbericht.
- In einer Fachabteilung wird ein Chatbot getestet.
- Eine Mitarbeiterin fragt, ob sie Copilot mit Kundendaten nutzen darf.

All das sind keine Einzelfälle – und längst keine reinen IT-Themen mehr. Immer mehr Entscheidungen zum KI-Einsatz werden spontan und oft gut gemeint getroffen.

Doch was passiert, wenn etwas schiefläuft? Wer ist verantwortlich – und woran erkennt man, was erlaubt ist?

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

Genau hier setzt der EU AI Act an. Er verpflichtet Unternehmen, Governance nicht dem Zufall zu überlassen, sondern verbindlich zu regeln. Damit wird aus einer organisatorischen Notwendigkeit ein rechtlicher Zwang. Geschäftsleitungen müssen nachweisen, dass sie die Kontrolle über die KI-Nutzung behalten – unabhängig davon, ob es sich um kleine Experimente oder große Systeme handelt.

Der rechtliche Rahmen: Was der EU AI Act vorgibt

Der **EU AI Act** ist die erste europaweite Regulierung, die KI nicht nur technisch, sondern ausdrücklich auch als Führungs- und Verantwortungsthema adressiert. Für Unternehmen bedeutet das: Governance ist kein optionales Rahmenwerk, sondern eine **gesetzliche Pflicht.**

Die zentralen Vorgaben im Überblick:

Verantwortung und Haftung (Art. 4)

- Geschäftsleitungen tragen die oberste Verantwortung für den sicheren Einsatz von KI.
- Zuständigkeiten, Prozesse und Kontrollen müssen nachweisbar dokumentiert sein.
- Delegation ist möglich – Entzug der Verantwortung nicht.
- Hinweis: Wer hier nur ein Policy-Dokument erstellt, aber keine Verfahren hinterlegt, verstößt gegen die Pflicht zur Nachweisführung.

Risikomanagement (Art. 9)

- Für Hochrisiko-Systeme ist ein systematisches Risikomanagement vorgeschrieben.
- Risiken müssen identifiziert, bewertet, begrenzt und laufend überprüft werden.
- Einbindung in bestehende Risiko- oder Compliance-Prozesse ist möglich und vom Gesetzgeber erwünscht.
- Wichtig: Unternehmen können hier häufig auf bestehende Strukturen im Risikomanagement aufsetzen – entscheidend ist, dass KI-Anwendungen dort sichtbar werden.

Datenqualität (Art. 10)

- Eingesetzte Daten müssen qualitativ hochwertig, repräsentativ und frei von Verzerrungen sein.
- Herkunft, Aufbereitung und Prüfung der Daten sind verpflichtend zu dokumentieren.
- Typischer Fehler: Alte oder unvollständige Datenbestände werden unreflektiert eingesetzt – und verletzen damit die Anforderungen an Qualität und Fairness.

Transparenz und Nachvollziehbarkeit (Art. 13–15)

- Ergebnisse von KI-Systemen dürfen nicht als „Black Box“ akzeptiert werden.
- Beschäftigte müssen die Ergebnisse einordnen, prüfen und ggf. korrigieren können.
- Teilweise sind Transparenzpflichten gegenüber Nutzenden vorgeschrieben (z.B. Hinweis „Dieses System basiert auf KI“).
- Beispiel: Ein Chatbot im Kundenservice muss klar erkennbar machen, dass er automatisiert arbeitet.

Schulung und Befähigung (Art. 4, 29)

- Mitarbeitende, die mit KI arbeiten, müssen geschult sein.
- Ziel: Verständnis der Funktionsweise, Risiken und Meldewege.
- Schulungen sind zu dokumentieren – Teilnahme und Inhalte gelten als Nachweis gegenüber Aufsichtsbehörden.
- Umfang: Kurze Pflichtmodule (z.B. zwei Stunden) genügen oft, wenn sie alle Kernrisiken abdecken.

Melde- und Dokumentationspflichten (Art. 62 ff.)

- Zwischenfälle und schwerwiegende Fehlfunktionen müssen gemeldet werden.
- Unternehmen benötigen feste Prozesse für Erfassung, Bewertung, Eskalation und Meldung an Behörden.
- Sämtliche Prüfungen, Freigaben und Änderungen sind nachvollziehbar zu dokumentieren.
- Praxisempfehlung: Ein quartalsweises Governance-Reporting schafft Überblick und erfüllt zugleich die Nachweispflichten.

Kernaussage**:** Der EU AI Act zwingt Unternehmen dazu, Governance als **belastbares Führungsinstrument** einzurichten. Die Vorgaben reichen von Verantwortung und Risikoanalyse über Datenqualität bis hin zu Schulungspflichten und Incident Reporting – und verlangen Strukturen, die im Alltag funktionieren und im Ernstfall belastbare Nachweise liefern.

Was Governance im Kern leisten muss

„Governance" klingt abstrakt – ist aber praktisch. Im Kern geht es um eine einfache Frage:

Wie regelt ein Unternehmen etwas, das neu, unübersichtlich oder risikobehaftet ist?

Governance bedeutet nicht Überwachung, sondern **Steuerung durch Verantwortung, Klarheit und Nachvollziehbarkeit**. Sie schafft einen Rahmen, in dem Fachbereiche experimentieren dürfen, ohne dass Risiken außer Kontrolle geraten.

Für KI heißt das konkret:

- 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 die Führung – und wo endet sie?

Damit wird Governance zum doppelten Instrument:

- **Innen** sorgt sie für Ordnung, Transparenz und Effizienz.
- **Außen** dient sie als rechtlicher Nachweis gegenüber Aufsichtsbehörden, Kunden und Partnern.

Besonders wichtig: Der EU AI Act macht diese Fragen rechtlich verbindlich. Governance ist nicht mehr bloß internes „Regelwerk", sondern ein **Pflicht-Nachweis**, dass Unternehmen Risiken vorausschauend managen und Verantwortung klar geregelt haben.

Praxisbeispiel: Ein neues Tool taucht auf

Ein Vertriebsbereich entdeckt ein KI-Tool, das automatisch Angebote erstellt. Es funktioniert erstaunlich gut, spart Zeit – und wird von den ersten Mitarbeitenden begeistert genutzt.

Variante 1: Ohne Governance

- Niemand fragt nach einer Genehmigung.
- Kundendaten werden in das Tool hochgeladen, ohne rechtliche Prüfung.
- Nach einigen Wochen wundert sich die Geschäftsleitung, warum verschiedene Angebotslayouts im Umlauf sind.
- Als ein Kunde reklamiert, dass sein vertrauliches Dokument im Tool auftaucht, weiß niemand: Wer hat das freigegeben? Wer trägt Verantwortung?

Folge: Chaos, Rechtsrisiko, ein möglicher Reputationsschaden – und zusätzlich: ein klarer Verstoß gegen den EU AI Act.

- Keine dokumentierte Risikoanalyse (Pflicht nach Art. 9).
- Keine geprüften Datenkategorien (Pflicht nach Art. 10).
- Keine klare Verantwortlichkeit in der Geschäftsleitung (Pflicht nach Art. 4).

Variante 2: Mit Governance

- Der Fachbereich meldet das Tool über ein einfaches Antragsformular.
- Ein Risikosteckbrief erfasst Zweck, Nutzen, Datenarten und mögliche Risiken.
- Datenschutz, Recht und IT-Sicherheit prüfen innerhalb weniger Tage.
- Das Governance-Board entscheidet: Ja, Pilotfreigabe – unter der Bedingung, dass keine Kundendaten hochgeladen werden.
- Nach drei Monaten liegt ein Bericht vor: 25 % Zeitersparnis pro Angebot, keine Risiken aufgetreten. Entscheidung: Skalierung auf weitere Teams.

Folge: Transparenz, dokumentierte Entscheidungen, nachvollziehbare Verantwortung – und volle Compliance mit dem EU AI Act.

- Risikoanalyse liegt vor (Art. 9).
- Datenkategorien wurden geprüft und freigegeben (Art. 10).
- Eskalations- und Entscheidungswege sind klar geregelt (Art. 4).

Fazit: Governance ist kein Selbstzweck, sondern ein Schutzschild – für Innovation, Rechtssicherheit und Führungsautorität zugleich.

Bausteine einer guten Governance

Der EU AI Act definiert Pflichten, aber er gibt Unternehmen nicht vor, wie eine Governance im Detail auszusehen hat. Damit bleibt Raum für eine praxisnahe Ausgestaltung. In der Erfahrung kristallisieren sich vier Themenfelder heraus, die in keiner Richtlinie fehlen dürfen.

1. Zulässigkeit von Anwendungen

Nicht jede KI-Nutzung ist gleich riskant. Deshalb braucht es eine Einordnung:

- **Unkritisch** sind etwa Texterstellung oder interne Protokolle.
- **Eingeschränkt zulässig** sind Anwendungen, die sensible Informationen berühren – z.B. Kundendaten.
- **Unzulässig** sind automatisierte Entscheidungen ohne menschliche Kontrolle.

Eine solche Kategorisierung schafft Sicherheit im Alltag: Mitarbeitende wissen, was erlaubt ist, Führungskräfte behalten die Kontrolle.

2. Datennutzung und Datenschutz

Die Qualität einer KI-Anwendung hängt unmittelbar von den Daten ab, die sie verarbeitet. Governance muss hier klare Leitplanken setzen:

- Welche Datenarten dürfen überhaupt genutzt werden?
- Unter welchen Bedingungen ist das zulässig?
- Wie werden Herkunft, Dokumentation und Löschung geregelt?

Der EU AI Act (Art. 10) verlangt, dass Daten **hochwertig, repräsentativ und frei von Verzerrungen sind**. Für die Praxis heißt das: Unternehmen müssen nicht nur interne Regeln aufstellen, sondern auch **dokumentieren können**, dass sie eingehalten werden.

3. Qualitätssicherung und Kontrolle

Eine KI liefert Vorschläge, aber keine geprüften Ergebnisse. Darum gehört in jede Richtlinie eine klare Antwort auf die Frage: Wann darf man einer Maschine vertrauen – und wann ist eine menschliche Kontrolle Pflicht?

Typische Festlegungen sind:

- Prüfung von Texten und Analysen durch Fachverantwortliche.
- Standards für Prognosen und Berichte.
- Dokumentation, wer bei Fehlern haftet und nachbessert.

So entsteht Verlässlichkeit: nach innen durch klare Prozesse, nach außen durch die Fähigkeit, Ergebnisse nachvollziehbar zu erklären – eine Anforderung, die der EU AI Act (Art. 13–15) ausdrücklich macht.

4. Rollen, Prozesse und Eskalation

Selbst die besten Regeln bleiben wirkungslos, wenn unklar ist, wer sie umsetzt. Darum müssen Governance-Richtlinien **Zuständigkeiten benennen**:

- Wer prüft neue Tools und gibt sie frei?
- Wer trägt die Verantwortung, wenn Risiken auftauchen?
- Welche Eskalationswege greifen, wenn ein Problem nicht im Fachbereich gelöst werden kann?

Der EU AI Act (Art. 4 und 62) schreibt vor, dass Verantwortlichkeiten dokumentiert und Zwischenfälle gemeldet werden. Für Unternehmen heißt das: Ohne klare Rollen ist weder Innovation steuerbar noch Rechtssicherheit gewährleistet.

Kurzum: Die Bausteine einer Governance-Richtlinie sind keine abstrakte Theorie. Sie übersetzen die rechtlichen Mindestanforderungen in konkrete Spielregeln für den Alltag – und schaffen so die Grundlage, auf der KI verantwortungsvoll und zugleich effizient genutzt werden kann.

Steuerungsmodelle in der Praxis

Nicht jede Organisation steuert KI gleich – und es gibt damit auch kein einziges Muster, das für alle passt. Drei Modelle haben sich in der Praxis herausgebildet. Sie unterscheiden sich nicht nur in der Logik, sondern auch darin, wie sie den Anforderungen des EU AI Act gerecht werden.

1. Zentralisiertes Modell – sicher, aber möglicherweise schwerfällig

Hier liegt alles in einer Hand: Eine zentrale Stelle prüft, genehmigt und dokumentiert jede KI-Anwendung. Meist wird das als Center of Excellence (CoE) organisiert – ein kleines Kernteam aus Recht, Datenschutz, IT-Sicherheit und Compliance.

- **Alltagsszene**: Wenn ein Fachbereich ein neues Tool nutzen will, landet der Antrag auf dem Tisch des CoE. Erst nach Prüfung, Freigabe und dokumentierter Risikoanalyse geht es weiter.
- **Stärke**: Dieses Modell bietet maximale Konsistenz. Mit Blick auf den EU AI Act (insbesondere Art. 9 zur Risikoanalyse und Art. 10 zur Datenqualität) ist es der beste Nachweis: Alles ist zentral dokumentiert, alles nachprüfbar.
- **Schwäche**: Geschwindigkeit könnte etwas verloren gehen. Jedes Projekt hängt an derselben Stelle und Innovationen können ins Stocken geraten.
- **Insbesondere sinnvoll für**: Organisationen in stark regulierten Branchen – Banken, Versicherungen, Gesundheitswesen – wo Nachweisführung Vorrang vor Tempo hat.

2. Dezentrales Modell – schnell, aber riskant

Das Gegenteil ist das dezentrale Modell: Die Fachbereiche regeln den Einsatz selbst. Jede Abteilung benennt KI-Verantwortliche, die Ideen prüfen, Risiken einschätzen und Berichte erstellen. Entscheidungen fallen dort, wo die Anwendung entsteht.

- **Alltagsszene**: Ein Marketing-Team testet ein neues Text-Tool, die KI-Verantwortliche prüft Zweck und Daten, dokumentiert kurz und gibt die Nutzung frei.
- **Stärke**: Entscheidungen sind nah am Anwendungsfall. Anpassungen erfolgen schnell, Innovationen werden nicht ausgebremst.
- **Schwäche**: Die Gefahr von Inkonsistenzen ist hoch. Unterschiedliche Abteilungen entwickeln unterschiedliche Regeln – und der Überblick geht verloren.
- **EU AI Act Bezug:** Genau hier liegt der Knackpunkt. Nach Art. 4 bleibt die Geschäftsleitung auch bei dezentraler Steuerung haftbar. Fehlt die zentrale Nachweisführung, kann ein eigentlich gut gemeintes Experiment im Ernstfall als Pflichtverletzung gewertet werden.
- **Sinnvoll für**: Reife Organisationen mit starker Führungskultur und eher unkritischen KI-Anwendungen.

3. Hybrides Modell – anschlussfähig und lernfähig

Zwischen diesen beiden Polen liegt der Ansatz, den viele Unternehmen anstreben: Zentrale Leitplanken mit dezentraler Umsetzung. Hier sorgt ein Governance-Board für den übergreifenden Rahmen, während Fachbereiche Geschwindigkeit und Praxisnähe sichern.

- **Alltagsszene**: Ein Fachbereich bringt eine neue Idee ein, erstellt einen Risikosteckbrief und legt ihn dem Board vor. Dieses prüft, legt Bedingungen fest und dokumentiert die Entscheidung. Parallel bleibt die Umsetzung im Fachbereich – schnell und praxisnah.
- **Stärke**: Konsistenz und Agilität werden verbunden. Risiken werden zentral im Blick behalten, Innovation bleibt möglich.
- **Herausforderung**: Mehr Abstimmungsaufwand. Rollen müssen klar definiert und aktiv ausgefüllt werden, sonst droht das Board zur Formalie zu werden.
- **EU AI Act Bezug**: Für viele Organisationen ist dies das tragfähigste Modell. Die zentralen Pflichten (Risikoanalysen nach Art. 9, Datenqualität nach Art. 10, Meldepflichten nach Art. 62) werden systematisch abgedeckt, gleichzeitig können Fachbereiche schnell handeln.
- **Sinnvoll für**: Wachsende und komplexe Organisationen, die viele unterschiedliche Anwendungsfälle parallel entwickeln.

Zwischenfazit:

Alle drei Modelle haben ihre Berechtigung – wichtig ist, dass sie bewusst gewählt und konsequent ausgestaltet werden. Der EU AI Act setzt dabei einen klaren Rahmen: Ohne dokumentierte Zuständigkeiten, Risikoanalysen und Meldeverfahren sind weder zentrale noch dezentrale Ansätze tragfähig. In der Praxis zeigt sich, dass hybride Modelle am besten geeignet sind, Compliance-Sicherheit mit Innovationsfähigkeit zu verbinden.

Rollen für eine wirksame KI-Governance

Ein Governance-System bleibt abstrakt, solange nicht klar ist, wer welche Verantwortung trägt.

Der EU AI Act gibt einige Rollen zwingend vor, andere haben sich in der Praxis bewährt. Entscheidend ist, dass Zuständigkeiten nicht nur auf dem Papier existieren, sondern im Alltag wirken.

Geschäftsleitung – Verantwortung bleibt oben (Art. 4)

Egal wie viele Gremien und Prozesse existieren: Die Geschäftsleitung trägt die letzte Verantwortung. Art. 4 des EU AI Act macht unmissverständlich klar, dass Haftung nicht delegiert werden kann.

Die Geschäftsleitung

- definiert Prinzipien und rote Linien,
- entscheidet in kritischen Fällen selbst,
- muss jederzeit nachweisen können, dass Governance-Strukturen existieren.

Wenn diese Rolle nicht greift: Im Ernstfall fehlt der rechtliche Schutz – und persönliche Haftung droht.

Governance-Board – Herzstück im hybriden Modell

In komplexen Organisationen reicht Einzelverantwortung nicht. Ein Governance-Board bündelt Perspektiven: Leitung, Fachbereiche, Recht, Datenschutz, IT-Sicherheit.

Seine Aufgabe: Entscheidungen nicht nur fällen, sondern **dokumentieren und nachvollziehbar machen**. Damit entsteht der Nachweis, den der EU AI Act verlangt – und gleichzeitig ein Forum, in dem Innovation nicht ausgebremst wird.

Stärke: Balance zwischen Agilität und rechtlicher Sicherheit.

Schwäche: Wenn es nur als Formalie läuft, verliert Governance ihre Wirkung.

KI-Verantwortliche – Nähe zum Alltag

Nicht jedes Risiko taucht in Vorstandssitzungen auf. Deshalb braucht es Rollen in den Fachbereichen: KI-Verantwortliche erkennen früh, wenn neue Tools auftauchen oder Risiken entstehen.

KI-Verantwortliche:

- erfassen Anwendungen und erstellen Risikosteckbriefe,
- begleiten Pilotprojekte,
- melden Auffälligkeiten ans Governance-Board.

Praxisnutzen: Sie sind die „Frühwarnsysteme“ der Organisation – ohne sie bliebe vieles im Verborgenen.

Schulungsverantwortliche – Befähigung dokumentieren (Art. 4)

Der EU AI Act verpflichtet Unternehmen, Mitarbeitende im Umgang mit KI zu schulen. Hierfür braucht es Verantwortliche, die Programme steuern, Inhalte dokumentieren und Teilnahme nachweisen.

Nicht, um selbst Trainer zu sein – sondern um sicherzustellen, dass Organisation und Aufsicht jederzeit belegen können: **Wissen und Befähigung sind vorhanden**.

Risikomanagement-Funktion – Pflicht bei Hochrisiko (Art. 9 ff.)

Hochrisiko-Anwendungen erfordern systematische Prüfungen. Der EU AI Act schreibt dafür ein Risikomanagement vor. Ob als eigene Funktion oder als erweiterte Aufgabe im Governance-Board – klar muss sein:

- Wer identifiziert Risiken?
- Wer bewertet Eintrittswahrscheinlichkeit und Schwere?
- Wer legt Gegenmaßnahmen fest?

Ohne diese Rolle: Lässt sich kein EU AI Act konformer Nachweis führen.

Querschnittsrollen – Stabilität im Hintergrund

Manche Funktionen sind keine „Stars“, aber unverzichtbar:

- **Recht** prüft Vertrags- und Haftungsfragen.
- **Datenschutz** schützt personenbezogene Daten.
- **IT-Sicherheit** bewertet technische Risiken.
- **Compliance** achtet auf Regelkonformität.

Zusammen liefern sie das Fachwissen, das Governance belastbar macht. In vielen Unternehmen werden diese Kompetenzen in einem **Center of Excellence (CoE)** gebündelt – gerade im zentralisierten Modell eine tragende Struktur.

Mitarbeitende – erste Linie der Praxis

Auch die beste Governance bleibt wirkungslos, wenn Mitarbeitende nicht wissen, was erlaubt ist. Sie brauchen klare Leitlinien, einfache Meldewege und sichtbare Unterstützung.

Denn Governance lebt wie immer nicht nur von Gremien – sie beginnt dort, wo jemand im Alltag fragt:

„Darf ich dieses Tool für Kundendaten nutzen – oder nicht?“

Zwischenfazit

Rollen sind das Rückgrat der Governance. Einige sind gesetzlich vorgeschrieben, andere ergeben sich aus der Praxis. Entscheidend ist, dass sie zusammenspielen – und dass die Geschäftsleitung jederzeit nachweisen kann: Zuständigkeiten existieren, Risiken werden geprüft, Entscheidungen sind dokumentiert.

Handlungsanleitung: In 7 Schritten zur wirksamen KI-Governance

Eine gute Governance-Struktur muss nicht kompliziert sein. Entscheidend ist, dass sie den rechtlichen Rahmen des EU AI Act berücksichtigt – und im Alltag handhabbar bleibt. Sinnvoll ist ein Vorgehen in drei Phasen: **Start – Ausbau – Verstetigung.**

Phase 1: Start – in 30 Tagen umsetzbar

Am Anfang geht es nicht darum, perfekte Strukturen zu schaffen, sondern die Grundlage: Verbindlichkeit, Sichtbarkeit und Nachweisbarkeit. Ohne diese Basis bleibt Governance unverbindlich – und kann im Ernstfall nicht belegt werden.

Schritt 1: Governance-Dokument verabschieden (Pflicht nach Art. 4)

Ohne schriftlich fixierte Regeln fehlt die Grundlage für jede spätere Steuerung. Ein kurzes Dokument von 5–7 Seiten reicht – entscheidend ist der Inhalt: Zuständigkeiten, Entscheidungswege und Eskalationen. Welche Elemente enthalten sein sollten, wurde oben beschrieben.

Das Dokument

- dient als offizieller Nachweis gegenüber Aufsicht, Behörden oder Stakeholdern
- schafft Orientierung für Mitarbeitende, welche Regeln verbindlich gelten
- Rolle der Geschäftsleitung: Prinzipien festlegen, Dokument offiziell verabschieden

Wenn dieser Schritt fehlt: Es gibt keine Referenz, auf die man sich im Ernstfall berufen kann – weder intern noch extern.

Schritt 2: Rollen benennen und kommunizieren (Pflicht nach Art. 4)

Selbst das beste Dokument bleibt wirkungslos, wenn niemand weiß, wer verantwortlich ist.

Deshalb müssen Rollen von Beginn an benannt und sichtbar gemacht werden: KI-Verantwortliche in den Fachbereichen sowie ein Governance-Board als koordinierende Stelle. Diese Aufgabe

- stellt sicher, dass Zuständigkeiten nicht nur festgeschrieben, sondern auch bekannt sind
- verhindert, dass Verantwortung im Alltag „zwischen den Stühlen“ bleibt
- Rolle der Geschäftsleitung: Auswahl der Personen und klare Kommunikation, dass Governance Priorität hat

Wichtig: Fehlt diese Klarheit, besteht in der Praxis ein Risiko, denn niemand weiß im Ernstfall, wer ein neues Tool prüfen oder stoppen darf.

Schritt 3: Schulungspflicht erfüllen (Pflicht nach Art. 4)

Der EU AI Act verpflichtet Unternehmen, Mitarbeitende im Umgang mit KI zu schulen. Ziel ist nicht Perfektion, sondern eine gemeinsame Basis. Ein kompaktes Pflichtmodul – zwei Stunden reichen – vermittelt Grundlagen, Risiken und Meldewege.

Mit diesem Schritt wird

- dafür gesorgt, dass Mitarbeitende KI nicht „blind“ einsetzen
- Wissen und Befähigung dokumentiert – ein zentraler Nachweis für Behörden

Die **Rolle der Geschäftsleitung** besteht darin, die Schulungen zu beauftragen und sicherzustellen, dass Programm und Dokumentation existieren.

Denn: Ohne nachweisbare Schulung bleibt jedes Governance-System lückenhaft – rechtlich wie praktisch.

Mit diesen drei Schritten entsteht in kürzester Zeit eine **belastbare Grundlage**: ein dokumentierter Rahmen, benannte Verantwortliche und nachweisbar geschulte Mitarbeitende. Governance wird sichtbar – und das Unternehmen kann belegen, dass es seiner Pflicht nachkommt.

Phase 2: Ausbau – in 2–6 Monaten

Nach den ersten Weichenstellungen beginnt die eigentliche Arbeit: Governance muss so ausgestaltet werden, dass sie tragfähig bleibt – und zwar sowohl für einfache Anwendungsfälle als auch für hochriskante Systeme. Zwei Elemente stehen dabei im Vordergrund: Risikoprüfungen und klare Eskalationsregeln.

Schritt 4: Risikoprüfung zweistufig aufsetzen

Damit der Überblick über die Vielzahl an KI-Anwendungen nicht verloren geht, braucht es ein Verfahren, das handhabbar ist – und zugleich den Anforderungen des EU AI Act standhält. In der Praxis hat sich ein zweistufiges Vorgehen bewährt.

Basisprüfung (Steckbriefverfahren)

Ein einheitliches Kurzformular (1–2 Seiten) erfasst für jede neue Anwendung die wichtigsten Eckpunkte:

- Zweck und erwarteter Nutzen
- eingesetzte Datenarten
- erste Risikoeinschätzung
- verantwortliche Person

Ziel ist nicht die Detailanalyse, sondern die Sichtbarkeit: Alle Anwendungen tauchen im Governance-System auf, keine bleibt „unter dem Radar".

Beispiel: Ein Fachbereich testet ein Tool zur Texterstellung. Der Steckbrief hält fest: Einsatz für interne Protokolle, keine sensiblen Daten, Verantwortliche Person X. Ergebnis: geringe Risiken, Freigabe ohne weitere Prüfung.

Vertiefte Risikoprüfung (für Hochrisiko-Anwendungen)

Sobald eine Anwendung sensible Daten nutzt oder in den Bereich der Hochrisiko-Systeme fällt, verlangt der EU AI Act eine ausführliche Prüfung. Diese umfasst:

- eine detaillierte Risikoanalyse (Eintrittswahrscheinlichkeit und Schwere möglicher Schäden)
- Datenprüfung: Qualität, Verzerrungsfreiheit, Repräsentativität (Art. 10)
- geplante Maßnahmen zur Risikobegrenzung (technisch und organisatorisch)
- Monitoring-Plan für den laufenden Betrieb.

Damit wird das Verfahren EU AI Act konform, ohne jede kleine Anwendung mit Bürokratie zu überlasten.

Beispiel: Ein Unternehmen prüft, ob Kundendaten mit Copilot verarbeitet werden dürfen. Hier greifen die vertieften Vorgaben: Datenschutzanalyse, Bias-Checks und ein Monitoring-Verfahren. Erst danach kann die Anwendung freigegeben werden.

Die Rolle der Geschäftsleitung ist dabei zentral: Sie muss sicherstellen, dass **beide Stufen verbindlich etabliert** sind. In der Praxis bedeutet das, sich regelmäßig Basis-Steckbriefe vorlegen zu lassen – und mindestens eine vertiefte Prüfung als Pilot abzunehmen, damit das Verfahren für Hochrisiko-Fälle erprobt wird.

Schritt 5: Eskalationsregeln festlegen

Selbst ein gutes Prüfverfahren stößt an Grenzen, wenn Risiken auftauchen, die nicht allein in Fachbereichen gelöst werden können. Der EU AI Act verpflichtet Unternehmen daher, klare Eskalationswege vorzusehen.

Typische Eskalationsgründe sind:

- hochsensible Daten (z.B. Gesundheitsinformationen)
- rechtliche Grauzonen (unklare Rechtsgrundlagen, DSGVO-Bezug)
- erhebliche Reputationsrisiken (z.B. diskriminierende Ergebnisse in Kundeninteraktionen)
- Hinweise auf systematische Verzerrungen oder Fehlfunktionen

Ziel der Eskalation ist es nicht, dass jeder Fall zur Geschäftsleitung getragen wird. Aber wenn Risiken existenziell sind – für Recht, Reputation oder Haftung –, muss die Leitung selbst entscheiden.

Beispiel: Ein Chatbot, der Kundendaten verarbeitet, zeigt diskriminierende Antworten. Hier ist nicht nur eine technische Korrektur nötig. Die Frage lautet: Darf dieses System überhaupt weiter eingesetzt werden?

Die Geschäftsleitung ist Adressat dieser Eskalationen. Wichtig ist nicht, jedes Detail selbst zu prüfen, sondern verbindlich festzulegen, wann, wie und unter welchen Kriterien ein Fall eskaliert wird – und dafür Sorge zu tragen, dass Entscheidungen dokumentiert sind.

Mit der Kombination aus zweistufiger Risikoprüfung und klaren Eskalationsregeln entsteht ein belastbares Fundament. Damit ist Governance nicht nur konform mit dem EU AI Act aufgesetzt, sondern auch praxisnah – und vorbereitet auf die Integration in die bestehenden Steuerungs- und Berichtssysteme, die in der Verstetigungsphase folgen.

Phase 3: Verstetigung – dauerhaft etablieren

Wenn Governance in der Start- und Ausbauphase aufgebaut wurde, geht es im nächsten Schritt darum, sie **dauerhaft in die bestehenden Strukturen einzubetten**. Nur so wird aus einem Sonderprojekt ein belastbares Führungssystem, das den Anforderungen des EU AI Act genügt und zugleich im Alltag funktioniert. Zwei Aufgaben stehen im Mittelpunkt: Integration in bestehende Systeme und Etablierung von Reporting- und Meldeprozessen.

Schritt 6: Governance in bestehende Systeme integrieren

Governance darf nicht neben den regulären Steuerungsprozessen laufen – sonst bleibt sie fragil. Dauerhaft wirksam wird sie nur, wenn sie dort verankert ist, wo Unternehmen Risiken, Qualität und Compliance ohnehin steuern.

Wichtig:

- **Integration ins Risikomanagement**: KI-Anwendungen sollten als fester Bestandteil im Unternehmens-Risikoregister auftauchen. Das erleichtert die Übersicht und schafft Verbindlichkeit.
- **Anbindung an Compliance-Prozesse**: Prüfungen von KI-Systemen gehören in dieselben Routinen, die heute für Datenschutz, Informationssicherheit oder Lieferantenkontrolle gelten.
- **Einbindung in Revision und Audits**: Regelmäßige Überprüfungen durch interne oder externe Revision stellen sicher, dass die Regeln nicht nur existieren, sondern auch eingehalten werden.

Beispiel: Ein Unternehmen führt quartalsweise Risiko-Reviews durch. Ab sofort enthält der Standardbericht auch einen Abschnitt „KI-Anwendungen“, in dem Steckbriefe, Prüfergebnisse und offene Eskalationen aufgeführt sind.

Rolle der Geschäftsleitung: Sie sorgt dafür, dass diese Integration verbindlich umgesetzt wird – etwa indem sie anordnet, dass KI ab dem nächsten Quartal ein Pflichtpunkt in Risiko-, Compliance- und Revisionsberichten wird.

Schritt 7: Reporting- und Meldepflichten umsetzen

Der EU AI Act verlangt Nachweisfähigkeit – intern wie extern. Dazu braucht es zwei komplementäre Ebenen.

Regelmäßige interne Reports

- Übersicht über alle geprüften Anwendungen
- dokumentierte Risiken und deren Behandlung
- getroffene Freigaben, Stopps oder Eskalationen
- idealerweise quartalsweise Berichterstattung an die Geschäftsleitung

Beispiel: Das Governance-Board legt einen Bericht vor, der zeigt: 14 geprüfte Anwendungen, 9 freigegeben, 3 mit Auflagen, 2 abgelehnt. Für die Geschäftsleitung ist auf einen Blick sichtbar, dass Regeln greifen und Entscheidungen dokumentiert sind.

Incident Reporting

Dieses Reporting regelt:

- das Verfahren, um schwerwiegende Zwischenfälle oder Fehlfunktionen zu melden (Art. 62 ff.).
- ein klare Zuständigkeit: Wer meldet, wer prüft, wer kommuniziert mit Behörden.
- die Dokumentation, wie Vorfälle behandelt und welche Korrekturmaßnahmen eingeleitet wurden.

Beispiel: Ein KI-System zur Betrugserkennung generiert wiederholt falsche Treffer. Der Fachbereich meldet den Vorfall über ein internes Formular. IT und Recht bewerten den Fall, das Governance-Board beschließt Maßnahmen – und die Meldung an die zuständige Behörde wird dokumentiert.

Die Geschäftsführung ist Empfänger dieser Reports und verantwortlich dafür, dass Meldeverfahren existieren – und genutzt werden. Wichtig ist nicht, jeden Vorfall selbst zu prüfen, sondern sicherzustellen, dass ein funktionierendes System etabliert ist.

Mit Integration und Reporting erreicht Governance ihre Reifephase. Sie ist dann kein Projekt mehr, sondern ein Teil der Führungsarchitektur – sichtbar, überprüfbar und anschlussfähig an die rechtlichen Anforderungen.

Governance als Startpunkt – drei Orientierungsfragen

KI-Governance entsteht selten als fertiges System. Meist beginnt sie schlicht damit, dass erste Regeln nötig werden – weil Tools im Alltag auftauchen oder weil externe Vorgaben greifen.

Der EU AI Act verschiebt diesen Zeitpunkt: **Ab 2026 ist Governance kein „Kann", sondern ein rechtliches „Muss".**

Damit wird klar: Unternehmen brauchen nicht sofort ein perfektes Modell, sondern einen gangbaren Einstieg. Drei Orientierungspunkte helfen, die Richtung zu finden:

1. Wo beginnen?

Mit einem schlanken Governance-Dokument und klar benannten Rollen. So entsteht ein erster Nachweis, dass Zuständigkeiten geregelt sind – eine Pflicht nach Art. 4 des EU AI Act.

2. Was ausbauen?

Mit einfachen Prüfverfahren und Schulungen: Ein Risikosteckbrief für neue Anwendungen und ein Basis-Schulungsmodul für Mitarbeitende reichen, um die Kernpflichten aus Art. 9 und 10 abzudecken.

3. Wohin entwickeln?

Zu einem lernfähigen System, das in bestehende Prozesse integriert ist – von Risiko-Reports bis zu Eskalationswegen. Ziel ist ein Modell, das sowohl rechtssicher als auch innovationsfähig bleibt.

Denn: Governance ist nicht das Endprodukt einer ausgereiften KI-Strategie, sondern der Rahmen, der den Anfang möglich macht. Wer früh eine belastbare Grundlage schafft, behält die Kontrolle – organisatorisch wie rechtlich.

Künstliche Intelligenz weiterdenken

Die anderen, **im Dokument erwähnten Dokumente** finden sich auf der Webseite von The Digital Leader unter www.digital-leader.eu/fuehren-mit-ki.

Wenn Sie Interesse an weiterführenden Informationen haben, melden Sie sich gern:

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

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

Weitere Dossiers & E-Books zum Download: ki-briefing.kit.com

Hinweis: Die Regulierung innerhalb Europas entwickelt sich sehr schnell. Dieses Dokument ist im September 2025 erstellt worden. Zum Zeitpunkt des Lesens können die im Dokument genannten Fakten bereits überholt sein.

Dieses Dokument dient der allgemeinen Information und Orientierung und ist in enger Zusammenarbeit mit Künstlicher Intelligenz entstanden. Es stellt keine Rechtsberatung dar und kann eine individuelle juristische Prüfung im Einzelfall nicht ersetzen.

Alle Angaben wurden sorgfältig recherchiert und nach bestem Wissen erstellt. Dennoch übernimmt die Autorin keine Gewähr für die Aktualität, Vollständigkeit oder Richtigkeit der Inhalte, insbesondere im Hinblick auf sich fortentwickelnde gesetzliche Vorgaben.

Für Entscheidungen, die auf Basis dieses Dokuments getroffen werden, übernimmt die Autorin keine Haftung. Die Umsetzung rechtlicher Anforderungen – insbesondere im Bereich KI-Governance – sollte stets in Abstimmung mit fachkundiger Rechtsberatung erfolgen.