KI-Governance im Mittelstand: Wer entscheidet, was die KI darf

Eine Vertriebsmitarbeiterin möchte ein Angebot von einem KI-Assistenten überarbeiten lassen. Darin stehen Kundenname, Rabattstaffel und Liefertermine. Sie fragt ihre Teamleitung, ob das in Ordnung ist. Die Teamleitung weiß es nicht und fragt die IT. Die IT verweist auf den Datenschutz, der Datenschutz auf die Geschäftsführung.

Solche Schleifen gibt es in vielen Betrieben, und sie enden fast immer auf eine von zwei Arten. Entweder wird das Werkzeug heimlich genutzt, oder es wird gar nicht genutzt. Beides ist teuer. Eine KI-Governance sorgt dafür, dass diese Frage beim nächsten Mal eine Antwort hat, und zwar innerhalb von Tagen statt Wochen.

Wozu brauchen Unternehmen eine KI-Governance?

Die meisten Führungskräfte stellen diese Frage aus einem nachvollziehbaren Grund. Die KI-Nutzung im eigenen Haus wirkt überschaubar, ein paar Lizenzen, ein Pilotprojekt, erste Erfahrungen im Marketing. Wozu also ein Regelwerk?

Die Antwort liegt in der Lücke zwischen Nutzung und Regeln. Laut einer aktuellen Bitkom-Umfrage setzt mit 57 Prozent erstmals die Mehrheit der Unternehmen ab 20 Beschäftigten KI ein, ein Jahr zuvor waren es 36 Prozent. Bei den Regeln sah es in der Bitkom-Befragung zu Schatten-KI aus dem Sommer 2025 deutlich dünner aus. Damals hatten erst 23 Prozent der Unternehmen Regeln für den Einsatz von KI-Tools aufgestellt.

Gleichzeitig war in einem Viertel der Unternehmen bekannt, dass Beschäftigte private KI-Lösungen im Job nutzen, weitere 17 Prozent gingen davon aus. Die Nutzung ist also längst da, der Rahmen fehlt in vielen Betrieben.

Daraus entstehen drei handfeste Probleme. Erstens landen Daten in Systemen, über die niemand einen Vertrag hat. Zweitens kann niemand sagen, wo KI im Unternehmen überhaupt eingesetzt wird, und damit auch nicht, welche Pflichten aus dem AI Act gelten. Drittens bleiben gute Ideen liegen, weil keiner weiß, wer sie freigeben darf.

Der dritte Punkt wird am häufigsten unterschätzt. KI-Governance ist aus unserer Erfahrung weniger ein Bremsklotz als eine Beschleunigung. Wenn klar ist, wer entscheidet und nach welchen Kriterien, kommen neue Anwendungsfälle schneller in den Betrieb. Wie Unternehmen diesen Schritt gegangen sind, teilen Praktiker:innen auf der Mittelstands-Stage des data:unplugged Festivals am 13. und 14. April in Münster.

Was ist KI-Governance und was unterscheidet sie von Data Governance?

KI-Governance, international meist AI Governance genannt, ist der Rahmen, in dem ein Unternehmen den Einsatz von KI steuert. Sie legt fest, welche KI-Systeme genutzt werden dürfen, wer über neue Anwendungen entscheidet, welche Daten wohin dürfen, wie Ergebnisse geprüft werden und wie das alles dokumentiert wird.

Mit Data Governance wird der Begriff ständig verwechselt. Beides gehört zusammen, regelt aber unterschiedliche Dinge. Data Governance kümmert sich um die Daten selbst: Qualität, Verantwortlichkeiten, Zugriffsrechte, Definitionen. Sie gilt für jede Auswertung und jedes System, ob mit oder ohne KI.

KI-Governance setzt eine Ebene darüber an. Sie fragt, was ein KI-System mit diesen Daten tun darf, wofür es eingesetzt wird und wer für seine Ergebnisse geradesteht. Greifbar wird der Unterschied an einem Beispiel aus dem Personalbereich. Dass Bewerbungsunterlagen korrekt, vollständig und nur für die Personalabteilung zugänglich sind, regelt die Data Governance. Ob ein KI-System diese Unterlagen vorsortieren darf und wer die Auswahl am Ende verantwortet, ist eine Frage der KI-Governance.

Ohne saubere Data Governance steht eine KI-Governance deshalb auf wackligem Fundament. Umgekehrt reicht gute Datenpflege allein nicht, sobald Systeme Vorschläge machen, Texte erzeugen oder Entscheidungen vorbereiten.

Was der AI Act von Unternehmen verlangt

Der EU AI Act ist für viele der Anlass, sich mit dem Thema zu befassen, und die Zahl der Betroffenen wächst. In der aktuellen Bitkom-Umfrage gehen 37 Prozent der Unternehmen davon aus, als Anwender vom AI Act betroffen zu sein, nach 23 Prozent im Vorjahr. Von denen, die betroffen sind oder das prüfen, rechnen 89 Prozent mit einem hohen Umsetzungsaufwand.

Viel Nervosität nimmt dabei eine Unterscheidung. Die meisten Mittelständler sind keine Anbieter von KI-Systemen, sondern Betreiber. Sie nutzen Werkzeuge, die andere entwickelt haben. Die umfangreichsten Pflichten, etwa zu technischer Dokumentation und Konformitätsbewertung, liegen bei den Anbietern.

Für Betreiber sind vor allem vier Punkte relevant. Seit Februar 2025 gelten die Verbote bestimmter Praktiken, darunter Emotionserkennung am Arbeitsplatz. Ebenfalls seit Februar 2025 gilt die Pflicht zur KI-Kompetenz. Seit dem Digital Omnibus, der am 27. Juli 2026 in Kraft getreten ist, ist sie weicher formuliert. Unternehmen müssen Maßnahmen ergreifen, um die Entwicklung der KI-Kompetenz ihres Personals zu unterstützen. Ein bestimmtes Kompetenzniveau müssen sie ausdrücklich nicht garantieren. Die Pflicht zum Handeln bleibt.

Seit dem 2. August 2026 greifen außerdem Transparenzpflichten. Wer etwa mit KI erzeugte Bilder oder Videos veröffentlicht, die echt wirken, muss das in vielen Fällen kenntlich machen. Der vierte Punkt betrifft Hochrisiko-Anwendungen, zum Beispiel KI in der Personalauswahl oder bei der Leistungsbewertung von Beschäftigten. Die zugehörigen Betreiberpflichten wie menschliche Aufsicht, Protokollierung und Information der Belegschaft gelten nach der Verschiebung ab dem 2. Dezember 2027.

Die Details zu Zeitplan und Risikostufen haben wir in unserem Beitrag zu KI, Datenschutz und DSGVO zusammengefasst. Für die Governance ist vor allem entscheidend, dass die Pflichten vom Anwendungsfall abhängen. Ein Unternehmen muss also wissen, wo es KI einsetzt. Genau das leistet eine Governance. Zuständige Aufsicht in Deutschland ist seit Ende Juli 2026 die Bundesnetzagentur. Ihr KI-Service Desk bietet mit dem KI-Compliance-Kompass einen Selbstcheck, der für eine erste Einordnung gut taugt.

Wer entscheidet, was die KI darf?

Diese Frage ist der Kern jeder KI-Governance, und im Mittelstand lässt sie sich schlanker beantworten als in Konzernen. Es braucht kein eigenes Gremium mit Geschäftsordnung. Es braucht drei klar verteilte Rollen.

Die Geschäftsführung

Die Verantwortung für den KI-Einsatz liegt bei der Unternehmensleitung und lässt sich nicht delegieren. Sie legt fest, welche Risiken das Unternehmen eingehen will, und entscheidet über Fälle, die über den Alltag hinausgehen. Das bedeutet nicht, dass jede neue Anwendung auf ihrem Tisch landen muss.

Eine verantwortliche Person für KI

Der AI Act schreibt keine KI-Beauftragten vor, anders als die DSGVO beim Datenschutz. Trotzdem empfehlen wir, eine Person oder ein kleines Team klar zu benennen. Diese Rolle sammelt Anfragen, prüft neue Anwendungsfälle nach festen Kriterien, pflegt die Übersicht über eingesetzte Systeme und ist Ansprechpartner:in für alle Fragen. In kleineren Unternehmen übernimmt das oft jemand aus der IT oder aus dem Datenschutz, idealerweise mit einem festen Zeitbudget statt nebenbei.

Die Fachbereiche

Wer ein Werkzeug nutzt, weiß am besten, wofür es taugt und wo es danebenliegt. Die Fachbereiche bringen Anwendungsfälle ein und verantworten die Prüfung der Ergebnisse in ihrem Bereich. Wo es einen Betriebsrat gibt, gehört er früh an den Tisch. Viele KI-Werkzeuge können Leistung oder Verhalten von Beschäftigten erfassen und sind damit mitbestimmungspflichtig. Wer das am Ende klärt statt am Anfang, verliert Monate.

KI-Governance-Umsetzung: ein Rahmen in vier Bausteinen

Ein praktikabler Rahmen passt für den Anfang auf wenige Seiten. Einen guten Einstieg bietet der Leitfaden des Mittelstand-Digital Zentrums Berlin. Er beschreibt eine KI-Richtlinie in sieben Schritten und verweist auf kostenfreie Vorlagen, etwa eine Muster-Richtlinie der IHK Schwaben. Aus unserer Sicht sind vier Bausteine entscheidend.

Freigaben

Neue Anwendungsfälle brauchen einen festen Weg: Wer stellt den Antrag, wer prüft, bis wann gibt es eine Antwort? Bewährt hat sich eine Einstufung in drei Stufen. Unkritische Anwendungen wie Textentwürfe ohne vertrauliche Daten laufen ohne Einzelprüfung. Anwendungen mit internen Daten brauchen die Freigabe der verantwortlichen Person. Alles, was Personalentscheidungen berührt oder nach außen wirkt, geht zusätzlich an die Geschäftsführung.

Erlaubte Werkzeuge

Eine Liste freigegebener Werkzeuge schafft mehr Klarheit als ein Katalog von Verboten. Zu jedem Werkzeug gehört die Angabe, welche Datenklassen hinein dürfen. Wie die Werkzeugfrage mit heimlicher Nutzung zusammenhängt und warum Verbote dort selten funktionieren, beschreiben wir ausführlich im Artikel zu Schatten-KI im Unternehmen.

Dokumentation

Hier reicht zu Beginn eine Tabelle. Sie hält fest, welches System wofür eingesetzt wird, wer verantwortlich ist, welche Daten verarbeitet werden und wie das Risiko eingestuft wurde. Dieses KI-Verzeichnis ist die Grundlage, um die Pflichten aus dem AI Act überhaupt zuordnen zu können. Es erspart außerdem die hektische Suche, wenn Kund:innen, Prüfer:innen oder die Aufsicht nachfragen.

Schulung

Regeln wirken nur, wenn die Menschen sie kennen und verstehen. Schulung ist deshalb Teil der Governance und kein separates Projekt. Sie sollte nach Rollen unterscheiden, denn wer Werkzeuge freigibt, braucht anderes Wissen als jemand, der täglich damit schreibt. Wie das im Mittelstand konkret aussieht, zeigt unser Beitrag zur KI-Weiterbildung im Unternehmen.

Einmal aufgesetzt, braucht der Rahmen eine regelmäßige Überprüfung, etwa halbjährlich. Werkzeuge ändern sich schnell, und mit ihnen die Fragen. Wie andere Unternehmen ihre Freigaben und KI-Verzeichnisse aufbauen und auf welchem Datenfundament das steht, erlebst du im direkten Austausch auf der d:u27 in Münster, auf der sieben unterschiedlichen Stages und in 80 Masterclasses, in denen du direkt an deinem eigenen Rahmen arbeitest.

Praxisbeispiel Delivery Hero: Governance, die nicht bremst

Bei aller Struktur bleibt eine naheliegende Sorge: Macht so ein Rahmen die Teams nicht langsamer? Juan Carlos Vasquez von Delivery Hero hat auf der Data Stage der d:u26 gezeigt, warum Governance nicht bremsen muss. Und er hat offen erzählt, wie das Unternehmen zunächst den anderen Weg gegangen ist.

Delivery Hero ist in über 70 Ländern aktiv, viele der lokalen Marken kamen durch Übernahmen dazu, mit jeweils unterschiedlicher Technik. Anfangs durften die lokalen Teams weitgehend selbst entscheiden, die Zentrale stellte nur Werkzeuge bereit. Die Folge: Personenbezogene Daten waren oft nicht gekennzeichnet, die Marken verstanden unter einem Kunden jeweils etwas anderes, und drei wichtige Dashboards zeigten drei verschiedene Kundenzahlen. Aus unserer Erfahrung kennen viele mittelständische Unternehmen dieses Muster, nur in kleinerem Maßstab.

Delivery Hero hat daraus die Konsequenz gezogen: Werkzeuge bereitzustellen reicht nicht, es braucht einen einheitlichen Weg, auf dem die Regeln von Anfang an mitlaufen. Wie dieser Kurswechsel gelungen ist, lässt sich an drei Learnings festmachen, die sich nach unserer Einschätzung gut auf den Mittelstand übertragen lassen.

Automatisierung schlägt Richtlinien

Regeln zur Kennzeichnung sensibler Daten gab es bei Delivery Hero schon vorher. Nur hielten sich viele nicht daran, weil es ohne schneller ging und das Risiko erst auffällt, wenn es eintritt. Heute prüft ein zentrales Backend bei jeder Veröffentlichung automatisch die Regeln und stoppt kritische Datenprodukte, wenn etwas fehlt, für Engineers per Code, für Fachbereiche über eine grafische Oberfläche. Im Mittelstand kann das aus unserer Sicht deutlich einfacher aussehen, etwa wenn nur freigegebene KI-Werkzeuge mit Firmenzugang bereitstehen.

Governance passend zum Risiko

Delivery Hero teilt Datenprodukte in Stufen ein. Geschäftskritische brauchen Data Contracts und SLAs, also verbindliche Vereinbarungen zu Inhalt, Qualität und Verfügbarkeit, während Auswertungen für den persönlichen Gebrauch ohne solche Kontrollen auskommen. Damit niemand für Wichtiges den bequemen Weg nimmt, dürfen kritische Datenprodukte nur auf andere geprüfte Datenprodukte zugreifen. Dasselbe Prinzip steckt aus unserer Sicht in der abgestuften Freigabe, die wir weiter oben beschreiben.

Compliant by default

„Der einfachste Weg muss der richtige sein, dann folgen ihm alle“, fasst Vasquez den Ansatz zusammen. Weil die Plattform die Regeln automatisch mitliefert, müssen sich die Nutzer:innen nicht mehr selbst darum kümmern. Statt rund 300 erstellen heute rund 3.000 Menschen bei Delivery Hero eigenständig Datenprodukte.

Spannend für die KI-Frage ist, was danach kommt. Weil die Governance automatisiert ist, liegen bei Delivery Hero alle Metadaten vor, um Daten künftig im Dialog abzufragen, also in natürlicher Sprache. Auch dabei gilt die Stufung: Datenprodukte für den persönlichen Gebrauch bleiben außen vor, damit die KI nicht mit ungeprüften Daten arbeitet. Das zeigt, wie eng Daten- und KI-Governance zusammenhängen.

Weitere dieser Use Cases und Erfahrungen teilen Daten und KI-Expert:innen sowie Praktiker:innen aus ihren Projekten auf den Stages der data:unplugged.

Wie wichtig ist Governance in KI-Projekten?

Wichtiger, als es in der Projektplanung meist aussieht. Viele KI-Projekte kommen über den Pilotstatus nicht hinaus. Häufig bremsen dabei keine technischen Probleme, sondern offene Fragen, die erst beim Übergang in den Betrieb auftauchen: Wer haftet für Fehler? Dürfen diese Daten dauerhaft verarbeitet werden? Wer prüft die Ergebnisse, wenn das Projektteam weiterzieht?

Wer diese Fragen vor dem Pilotprojekt klärt, spart sich die Schleife danach. Governance gehört deshalb in die Projektplanung, als fester Prüfpunkt vor der Entscheidung, ein Projekt in die Breite zu bringen.

Dazu kommt ein zweiter Effekt, der in keinem Projektplan steht, nämlich Vertrauen. Wenn klar ist, was erlaubt ist, nutzen Beschäftigte KI offen. Sie erzählen von ihren Erfahrungen, teilen gute Prompts und melden Probleme, statt sie zu verstecken. Das Unternehmen erfährt dadurch, wo KI tatsächlich Nutzen stiftet. Eine Governance, die vor allem verbietet, erreicht das Gegenteil.

Fazit: Klare Zuständigkeiten statt dickes Regelwerk

Im Kern beantwortet KI-Governance die Frage, wer entscheidet, was die KI darf. Für den Mittelstand bedeutet das keine Bürokratie, sondern drei klare Rollen und einen Rahmen aus Freigaben, erlaubten Werkzeugen, Dokumentation und Schulung. Der AI Act gibt dabei die Mindestanforderungen vor. Den eigentlichen Nutzen bringt die Klarheit im Alltag.

Unsere Empfehlung für den Einstieg: Beginnt mit einer Bestandsaufnahme, welche KI-Werkzeuge heute schon genutzt werden, auch inoffiziell. Benennt danach eine verantwortliche Person und legt die ersten Regeln fest. Nach sechs Monaten wird

nachgeschärft. Ein Rahmen, der im Betrieb gelebt wird, bringt mehr als ein perfektes Dokument, das niemand kennt.

Wie Unternehmen diesen Weg konkret gehen, welche Freigabeprozesse sich bewährt haben und wie sie den Betriebsrat eingebunden haben, steht im Mittelpunkt der d:u27 am 13. und 14. April 2027 in Münster. Auf sieben Stages und in 80 Masterclasses kommen rund 17.000 Teilnehmende zusammen, mit einer eigenen Mittelstands-Stage und der Data Stage für alle, die Daten und KI vom Fundament her denken.

KI-Governance ist Teamarbeit zwischen Geschäftsführung, IT, Datenschutz und Fachbereichen. Deshalb lohnt es sich, gemeinsam zu kommen. Jetzt Tickets für die d:u27 sichern!