Ein Leitfaden:

Vom AI Act zur AI Governance: Was Unternehmen ab Herbst 2026 operationalisieren müssen

Der 2. August 2026 markiert für viele Unternehmen einen Wendepunkt. Mit der weitgehenden Anwendbarkeit des europäischen AI Act endet zunehmend die Phase, in der sich Unternehmen auf Bestandsaufnahmen, erste AI Policies, Schulungen und einzelne Pilotprojekte konzentrieren konnten.

Die gute Nachricht: Die meisten größeren Unternehmen müssen dafür nicht bei null anfangen.

Datenschutzorganisation, Informationssicherheitsmanagement, Compliance, Risikomanagement, Einkauf, Vertragsmanagement, interne Revision und betriebliche Mitbestimmung existieren bereits. Vielfach bestehen außerdem Richtlinien zur Nutzung generativer KI, erste Freigabeprozesse und Schulungsangebote.

Die entscheidende Frage für die zweite Jahreshälfte 2026 lautet deshalb nicht mehr:

„Haben wir AI Governance?“

Sondern:

„Sind unsere bestehenden Governance-Strukturen präzise genug erweitert worden, um KI-Systeme tatsächlich über ihren gesamten Lebenszyklus zu steuern?“

Genau hier liegt derzeit eine der größten Herausforderungen.

Von der Richtlinie zum operativen Governance-System

Eine AI Policy ist wichtig. Sie ist aber noch kein AI-Governance-System.

Auch ein Verbot, vertrauliche Unternehmensdaten in öffentliche KI-Systeme einzugeben, löst nur einen kleinen Ausschnitt des Problems. Ebenso wenig genügt eine Liste zugelassener Anwendungen, wenn nicht geklärt ist, wer neue Systeme bewertet, welche Änderungen eine erneute Prüfung auslösen und wie die tatsächliche Nutzung kontrolliert wird.

AI Governance muss deshalb in die vorhandene Unternehmensorganisation integriert werden.

Dabei entstehen keine völlig neuen Compliance-Disziplinen. Vielmehr müssen bestehende Strukturen **AI-spezifisch präzisiert und miteinander verbunden** werden.

Bestehende Struktur	Typischer Ausgangspunkt	AI-spezifische Erweiterung
Datenschutz	Verarbeitungsverzeichnisse, DSFA, TOM	Trainings-, Prompt-, Input- und Outputdaten, RAG-Datenquellen, Modellzugriffe, Zweckänderungen
Informationssicherheit	ISMS, Zugriffsmanagement, Incident Response	Prompt Injection, Model Access, AI Agents, Shadow AI, externe Modelle und Schnittstellen
Risikomanagement	Risikoidentifikation und Kontrollen	AI-Systeminventar, Risikoklassifizierung, Use-Case-Risiken, Human Oversight
Einkauf	Lieferantenprüfung	AI Provider Due Diligence, Modellabhängigkeiten, Subprozessoren, Trainingsdaten
Vertragsmanagement	AVV, SLA, Haftung	Modelländerungen, Audit-Rechte, Daten-/IP-Garantien, Exit- und Portabilitätsregelungen
Compliance	Richtlinien und Freigabeprozesse	AI-spezifische Freigaben, Eskalationen, Monitoring und Verantwortlichkeiten
HR	Schulungsprogramme	rollenbezogene AI Literacy und Regeln für KI im Beschäftigungskontext
Interne Revision	Kontroll- und Prüfprogramme	regelmäßige Prüfung von AI-Systemregister, Kontrollen und Governance-Prozessen

Der wesentliche Unterschied liegt damit weniger im Aufbau zusätzlicher Bürokratie als in der **Spezifizierung bestehender Prozesse**.

1. Aus der Softwareübersicht wird ein AI-Systemregister

Eine der ersten Fragen lautet:

Welche KI wird im Unternehmen eigentlich eingesetzt?

Das klingt trivial. In der Praxis ist die Antwort häufig überraschend schwierig.

KI-Funktionalitäten befinden sich längst nicht mehr ausschließlich in Anwendungen, die ausdrücklich als „KI-System“ beschafft wurden. Sie werden in bestehende SaaS-Produkte integriert, erscheinen als Copilots, Analysefunktionen oder Assistenten und können über APIs in andere Systeme eingebunden werden.

Hinzu kommt Shadow AI: Beschäftigte verwenden externe Tools, Browser-Erweiterungen oder private Accounts, ohne dass diese Anwendungen einen formellen Beschaffungsprozess durchlaufen haben.

Ein belastbares AI-Systemregister sollte deshalb zumindest erfassen:

System – Anbieter – Modell – Zweck – organisatorischer Owner – Nutzerkreis – Datenkategorien – Schnittstellen – Risikoklassifizierung – Rechtsgrundlagen – Freigabestatus – Kontrollmaßnahmen – Review-Zyklus.

Das Register darf dabei keine einmalige Inventur bleiben.

Wird das zugrunde liegende Modell ausgetauscht? Ändert der Anbieter seine Bedingungen? Kommen neue Funktionen hinzu? Wird ein bisher internes Assistenzsystem plötzlich für automatisierte Entscheidungen eingesetzt?

Dann kann sich auch die Risikobewertung ändern.

2. Datenschutz muss um die Modellperspektive erweitert werden

Unternehmen verfügen regelmäßig bereits über etablierte DSGVO-Prozesse.

Bei KI-Anwendungen reicht es jedoch nicht aus, lediglich festzustellen, dass personenbezogene Daten verarbeitet werden.

Zusätzlich muss nachvollziehbar sein:

- Welche Daten gelangen als Input oder Prompt in das System?
- Werden Eingaben gespeichert?
- Werden sie zur Verbesserung oder zum Training eines Modells verwendet?

- Wo erfolgt die Verarbeitung?
- Welche externen Anbieter oder Subprozessoren erhalten Zugriff?
- Welche Daten werden über Retrieval-Augmented Generation eingebunden?
- Können Outputs personenbezogene oder vertrauliche Informationen reproduzieren?
- Welche Folgen hat ein Wechsel des Modells oder Providers?

Damit wird aus klassischem Datenschutz zunehmend ein Zusammenspiel aus **Data Governance, Model Governance und Access Governance**.

3. Informationssicherheit endet nicht am Login

Auch bestehende Informationssicherheitskonzepte müssen erweitert werden.

Ein KI-System kann technisch korrekt authentifiziert und trotzdem erhebliche neue Risiken erzeugen.

Dazu gehören beispielsweise manipulierte Eingaben, unkontrollierte Datenabflüsse, Prompt Injection, unsichere Plugins und Schnittstellen oder zunehmend autonome AI Agents mit Zugriff auf Unternehmenssysteme.

Besonders relevant wird dabei die Frage:

Was darf das System nicht nur sehen – sondern was darf es selbst tun?

Sobald KI-Systeme E-Mails versenden, Datensätze verändern, Bestellungen auslösen, Code deployen oder andere Anwendungen ansteuern können, reicht klassisches Zugriffsmanagement allein nicht mehr aus.

Berechtigungen, technische Grenzen, Human Oversight, Logging und Notfallmechanismen müssen gemeinsam gedacht werden.

4. Aus Lieferantenmanagement wird Model Governance

Viele Unternehmen verfügen bereits über professionelle Vendor-Management-Prozesse.

Bei KI-Anbietern kommen jedoch zusätzliche Fragen hinzu.

Woher stammen Trainingsdaten? Welche Rechte räumt sich der Provider an Unternehmensdaten ein? Welche Modelle werden tatsächlich eingesetzt? Können

Modelle ohne Zustimmung des Kunden ausgetauscht werden? Welche Subprozessoren sind beteiligt? Welche Nachweise stehen für Audits zur Verfügung?

Und vor allem:

Was passiert, wenn sich das Produkt verändert?

Bei klassischen Softwareprodukten ist ein Update häufig lediglich ein technischer Vorgang. Bei einem KI-System kann ein Modellwechsel dagegen Eigenschaften, Risiken und Outputqualität erheblich verändern.

Deshalb sollte AI Vendor Management nicht mit der Vertragsunterzeichnung enden.

Es benötigt ein **laufendes Model- und Change-Monitoring**.

5. AI Literacy ist kein einmaliges E-Learning

Unternehmen haben bereits erhebliche Anstrengungen unternommen, ihre Beschäftigten für den Umgang mit KI zu sensibilisieren.

Der nächste Schritt besteht in einer stärkeren Differenzierung.

Eine Mitarbeiterin, die einen freigegebenen Textassistenten nutzt, benötigt andere Kenntnisse als ein Entwickler, der Modelle über APIs integriert.

Ein HR-Team benötigt andere Schulungsinhalte als Einkauf, Rechtsabteilung oder interne Revision.

AI Literacy sollte deshalb rollenbezogen organisiert werden:

Was darf diese Person mit KI tun? Welche Risiken muss sie erkennen? Wann muss sie eskalieren? Welche Entscheidungen darf sie nicht an ein System delegieren?

Aus allgemeiner KI-Kompetenz wird damit ein Bestandteil des internen Kontrollsystems.

6. Human Oversight braucht einen Prozess

„A human is in the loop“ gehört inzwischen zu den häufigsten Aussagen in AI-Governance-Konzepten.

Doch ein Mensch im Prozess ist noch keine wirksame menschliche Aufsicht.

Entscheidend ist vielmehr:

Hat diese Person ausreichend Informationen, um einen Fehler überhaupt erkennen zu können?

Darf sie dem System widersprechen?

Kann sie eine Entscheidung stoppen?

Wird dokumentiert, wann und warum sie eingegriffen hat?

Und besitzt sie genügend fachliche Kompetenz, um nicht lediglich automatisiert erzeugte Ergebnisse abzunicken?

Human Oversight ist deshalb keine Position in einem Prozessdiagramm. Es ist eine Kontrollfunktion.

7. Auch AI Governance selbst muss kontrolliert werden

Schließlich benötigt ein belastbares Governance-System eine zweite Kontrollebene.

Wer prüft, ob das AI-Systemregister vollständig ist?

Wer kontrolliert, ob Reviews tatsächlich stattfinden?

Wer stellt fest, dass ein Fachbereich ein freigegebenes System inzwischen für einen völlig anderen Zweck verwendet?

Wer überwacht Änderungen bei externen Providern?

Und wer berichtet wesentliche AI-Risiken an Geschäftsführung oder Vorstand?

Hier kommt der internen Revision und dem klassischen Three-Lines-Modell eine zunehmend wichtige Rolle zu.

AI Governance muss deshalb nicht nur dokumentiert, sondern **auditierbar** sein.

Das eigentliche Projekt beginnt nach der Bestandsaufnahme

Für viele größere Unternehmen dürfte die Ausgangslage im Herbst 2026 ähnlich sein:

Die wesentlichen Governance-Strukturen existieren bereits.

Datenschutz ist etabliert. Informationssicherheit ist organisiert. Einkauf prüft Anbieter. Compliance erlässt Richtlinien. HR führt Schulungen durch. Die Revision kontrolliert Prozesse.

Das Problem ist deshalb häufig nicht das völlige Fehlen von Governance.

Das Problem sind die **Schnittstellen**.

Wer informiert Datenschutz, wenn der Provider das Modell austauscht?

Wer löst eine erneute Risikoprüfung aus?

Wer entscheidet, ob eine neue Funktion noch von der ursprünglichen Freigabe gedeckt ist?

Wer stellt sicher, dass ein ausgeschiedenes System auch aus dem AI-Systemregister entfernt wird?

Und wer besitzt am Ende die Gesamtverantwortung für den AI Lifecycle?

Genau diese Fragen entscheiden darüber, ob AI Governance lediglich auf dem Papier existiert oder im Unternehmen tatsächlich funktioniert.

Von Compliance zu AI Governance

Der AI Act macht KI nicht zu einer isolierten neuen Compliance-Disziplin.

Er zwingt Unternehmen vielmehr dazu, vorhandene Strukturen neu miteinander zu verbinden.

Die zentrale Aufgabe für die zweite Jahreshälfte 2026 lautet deshalb:

Inventarisieren. Klassifizieren. Verantwortlichkeiten zuordnen. Kontrollen definieren. Änderungen überwachen. Nachweise schaffen.

Unternehmen, die bereits über professionelle Governance-Strukturen verfügen, besitzen dafür einen erheblichen Vorteil.

Sie müssen das Rad nicht neu erfinden.

Sie müssen allerdings sehr genau bestimmen, **welche Speichen für KI bislang noch fehlen.**

AiNJA | Compliance

Dieser Beitrag gibt einen allgemeinen Überblick über organisatorische und regulatorische Anforderungen an AI Governance und ersetzt keine rechtliche Beratung.