Whitepaper

Wie Unternehmen ein KI-Governance- und Compliance-Management-System aufbauen

Warum Unternehmen jetzt handeln müssen

Künstliche Intelligenz (KI) durchdringt immer mehr Geschäftsbereiche – von **generativer KI** in der Kundenkommunikation bis zu datengetriebenen Entscheidungsmodellen. Doch mit den Chancen wachsen auch die Risiken und Pflichten. Unternehmen stehen vor Herausforderungen wie **„Schatten-KI“**, also der ungenehmigten Nutzung von KI-Tools durch Mitarbeiter ohne IT- oder Compliance-Aufsicht. Dies kann zu **Datenlecks und Datenschutzverstößen** führen, etwa wenn Mitarbeitende vertrauliche Informationen in externe KI-Systeme eingeben. Bereits 38 % der Beschäftigten geben zu, sensible Arbeitsdaten ohne Erlaubnis mit KI-Tools geteilt zu haben – ein enormes Risiko für **Datenschutz, IP und Geschäftsgeheimnisse**. Unkontrollierter KI-Einsatz erhöht die Gefahr von **Compliance-Verstößen** (z.B. gegen DSGVO) und empfindlichen Bußgeldern. Hinzu kommen **Bias-Risiken**: Unbeaufsichtigte KI-Modelle können diskriminierende oder fehlerhafte Ergebnisse liefern. **Verzerrte Trainingsdaten** oder **„Modelldrift“** sind typische KI-Risiken, die zu unfairen Entscheidungen und Reputationsschäden führen können. Das Vertrauen von Kunden und Partnern steht auf dem Spiel, wenn KI-Systeme ohne Governance daneben greifen.

Ailance
By 2B Advice

KI braucht klare Regeln

- KI kann Urheberrechte verletzen.
- Datenschutzverstöße gefährden Vertrauen.
- Fehlende Governance stoppt Projekte.
- 99 % sehen Governance als Top-Priorität.

Auch Rechts- und Haftungsfragen drängen: KI-generierte Inhalte können geistige Eigentumsrechte Dritter verletzen. So birgt der Output generativer KI stets das Risiko, urheberrechtlich geschützte Werke oder Marken unbefugt zu enthalten, da Unternehmen kaum nachvollziehen können, mit welchen Daten ein Modell trainiert wurde. Solche IP-Verstöße oder Datenschutzvorfälle (z.B. durch fehlende Datenschutz-Folgenabschätzung bei KI-Projekten) können nicht nur juristische Konsequenzen, sondern auch öffentlichen Vertrauensverlust nach sich ziehen. Eine aktuelle Studie unterstreicht den Handlungsdruck deutlich: 99 % der befragten Unternehmen nennen den Aufbau guter KI-Governance als eine der Top-Herausforderungen bei der AI-Nutzung. Nahezu die Hälfte der Firmen musste KI-Projekte bereits unterbrechen oder neu aufsetzen – häufig wegen Datenschutzproblemen (48 %) oder fehlendem Governance-Rahmen (37 %). KI-Governance ist also kein Luxus, sondern erfolgskritisch, um Innovation zu ermöglichen, ohne in Chaos oder Rechtsrisiken zu enden.

Ailance
By 2B Advice

KI-Governance im Zeitalter der Regulierung

Die Regulierung von Künstlicher Intelligenz gewinnt rasant an Fahrt. Unternehmen stehen zunehmend unter Druck, ihre KI-Anwendungen regelkonform und verantwortungsvoll zu gestalten. Der Aufbau eines strukturierten KI-Compliance-Managements wird zur strategischen Notwendigkeit.

Der EU AI Act: Ein neues Kapitel der KI-Regulierung

Mit dem EU AI Act entsteht ein umfassendes europäisches Gesetz zur Regulierung von KI-Systemen. Es klassifiziert Anwendungen nach Risikostufen (minimal bis intolerabel) und sieht bei Verstößen empfindliche Strafen von bis zu 35 Mio. € oder 7 % des globalen Umsatzes vor. Besonders Hochrisiko-KI unterliegt strengen Anforderungen wie Risikomanagement, Datenqualität, Transparenz und menschlicher Kontrolle – mit Haftungsrisiken bis in die Unternehmensführung.

48 % stoppen KI-Projekte wegen Datenschutz

Pflicht zur aktiven Selbstprüfung

Unternehmen müssen frühzeitig prüfen, ob ihre KI-Systeme unter den Anwendungsbereich des AI Acts fallen. Entsprechend sind Kontroll- und Governance-Strukturen einzuführen. Regulatoren wie die BaFin verlangen bereits jetzt, dass Verantwortlichkeiten klar zugewiesen, Diskriminierung vermieden und IT-Sicherheit nachgewiesen werden – unabhängig davon, ob die Maschine Entscheidungen trifft.

Regionale Unterschiede, gemeinsamer Druck

Während EU-Mitgliedsstaaten wie Deutschland und Österreich sich direkt auf den AI Act vorbereiten, verfolgt die Schweiz einen sanfteren Weg über Gesetzesanpassungen und Konventionen. In Großbritannien setzt die Regierung auf Prinzipien statt verbindlicher Gesetze. Trotz dieser Unterschiede gilt: Ohne Governance drohen regulatorische Lücken, Imageschäden und strategische Nachteile.

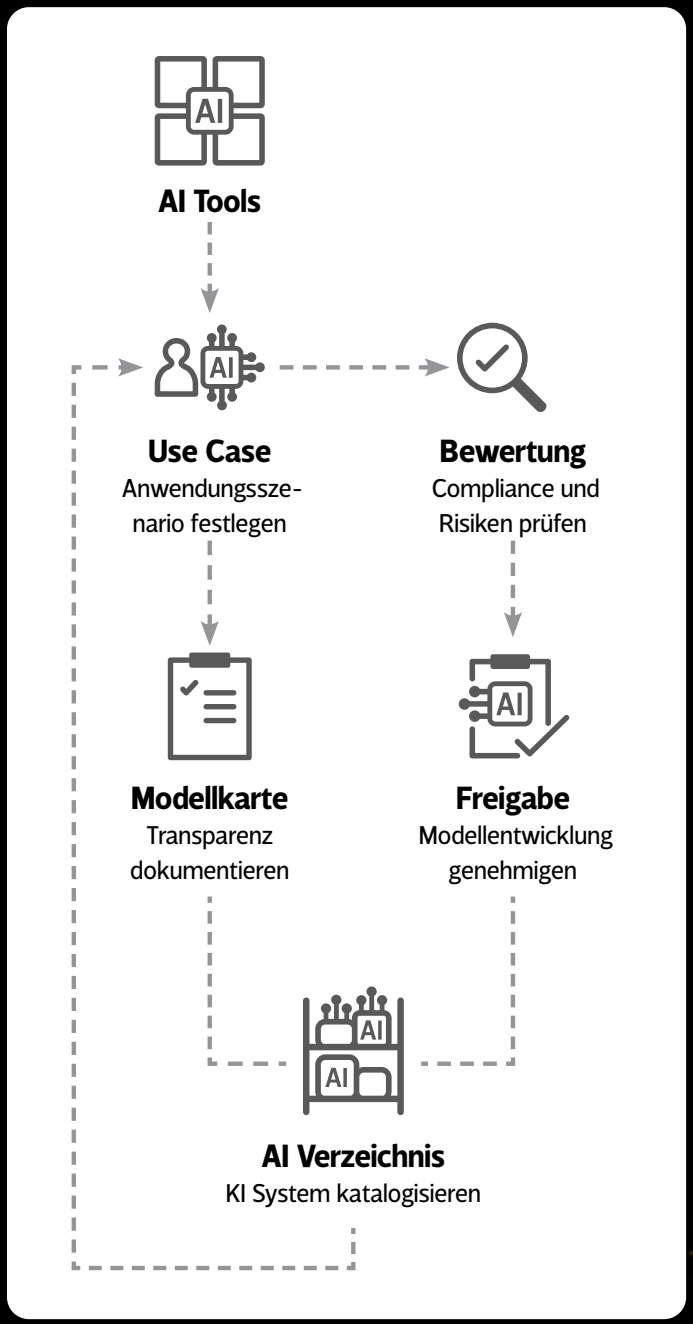
Governance operationalisieren: Vom Prinzip zur Praxis

Moderne Governance-Tools machen Richtlinien umsetzbar: Prozesse wie Risikobewertungen, Genehmigungen oder Datenschutz-Folgenabschätzungen (DPIA) lassen sich automatisieren und in Workflows integrieren. So wird KI-Governance nicht nur dokumentiert, sondern aktiv im Unternehmen verankert – mit automatischen Prüfmechanismen, Eskalationen und Erinnerungen für regelmäßige Reviews.

37 % wegen fehlender Governance

Ailance
By 2e Advice

Zusatzhinweis: Eine moderne KI-Governance-Lösung sollte es ermöglichen, **Richtlinien in automatisierte, verbindliche Prozesse zu überführen.** So können Vorgaben zur Risikobewertung, Genehmigung oder Prüfung von KI-Systemen direkt als Workflows im Tool abgebildet werden. Anstatt auf manuelle Umsetzung zu hoffen, wird Governance „in den Prozess eingebaut“: Freigaben erfolgen nur nach vollständiger Risikoprüfung, ein DPIA wird automatisch angestoßen, wenn personenbezogene Daten im Spiel sind, und Erinnerungssysteme sichern regelmäßige Reviews. So wird Governance nicht nur formuliert, sondern *gelebt und automatisch durchgesetzt*.



Was eine geeignete KI-Governance-SaaS-Lösung leisten muss

Eine KI-Governance-Lösung ist kein „Nice-to-have“, sondern ein strategisches Fundament zur Einhaltung regulatorischer Pflichten und zur Minimierung von Haftungsrisiken. Entscheider sollten bei der Auswahl eines SaaS-Tools darauf achten, dass es nicht nur Daten verwaltet, sondern Governance tatsächlich operationalisiert. Die wichtigsten Anforderungen:

1. **Abbildung des gesamten Lebenszyklus von KI-Projekten:**
   Von der Idee über die Risikoprüfung bis zur Freigabe und dem kontinuierlichen Monitoring. Alle Phasen müssen im System abgebildet und nachvollziehbar dokumentiert sein.

2. **Integration bestehender Datenschutz- und IT-Compliance-Prozesse:**
   Eine gute Lösung dockt an vorhandene Abläufe an – etwa die Datenschutz-Folgenabschätzung (DPIA), die Risikobewertung oder die IT-Governance. Das Tool sollte die gleichen Rollenmodelle und Verantwortlichkeiten abbilden wie bestehende Compliance-Strukturen.

3. **Automatisierung und Workflow-Management:**
   Entscheidend ist die Fähigkeit, Richtlinien in automatisierte Prozesse zu übersetzen: - Wenn ein Use Case personenbezogene Daten verarbeitet, wird automatisch eine DPIA initiiert. - Freigaben erfolgen nur nach Abschluss aller erforderlichen Prüfungen. - Erinnerungen an Re-Audits oder Überprüfungen erfolgen automatisch.

4. **Transparenz durch Dashboards und Reports:**
   Führungskräfte brauchen eine zentrale Übersicht über alle laufenden KI-Projekte, deren Risiken und Freigabestatus. Dashboards müssen die wichtigsten KPIs liefern – etwa wie viele Use Cases aktuell freigegeben sind, wie viele als „High Risk“ gelten, wo Engpässe bestehen.

5. **Flexibilität und Skalierbarkeit:**
   Die Lösung muss mit der Organisation wachsen und sich an neue regulatorische Anforderungen (z.B. EU AI Act, neue ISO-Normen) anpassen lassen.

6. **Rollenbasierte Rechtevergabe und Datenschutz by Design:**
   Nur wer autorisiert ist, darf KI-Use-Cases anlegen oder bewerten. Zugriffe, Datenkategorien und Zweckbindung müssen granular steuerbar sein.

7. **Interoperabilität mit anderen GRC-Tools:**
   Die KI-Governance sollte Teil einer integrierten Governance-, Risk- und Compliance-Architektur sein. Schnittstellen zu RoPA, Risikomanagement, Lieferantenbewertungen oder Vertragsprüfungen sind essenziell.

Ailance
By 2B Advice

Expertentipp: Wählen Sie keine Lösung, die Governance nur dokumentiert, aber nicht durchsetzt. Moderne Tools bilden nicht nur Richtlinien ab, sondern erzwingen deren Umsetzung – über automatisierte Freigabeprozesse, Pflichtfelder, Workflows und Alerting. Das reduziert Fehlerquellen, verhindert Vergessen und sorgt für „Compliance by Design“.

AI Governance

Erfahren Sie, wie KI-Governance in Ihrem Unternehmen funktioniert

Termin buchen

Vereinbaren Sie jetzt Ihren persönlichen Beratungstermin

LinkedIn folgen

Aktuelle Insights & News direkt aus unserem Netzwerk

2B Advice

www.2b-advice.com

Tel. +49 228 926165-100

Anmeldung News: 2b-advice.com/de/newsletter/