watsonx.governance™

# KI-Governance

## ↪ für das Unternehmen

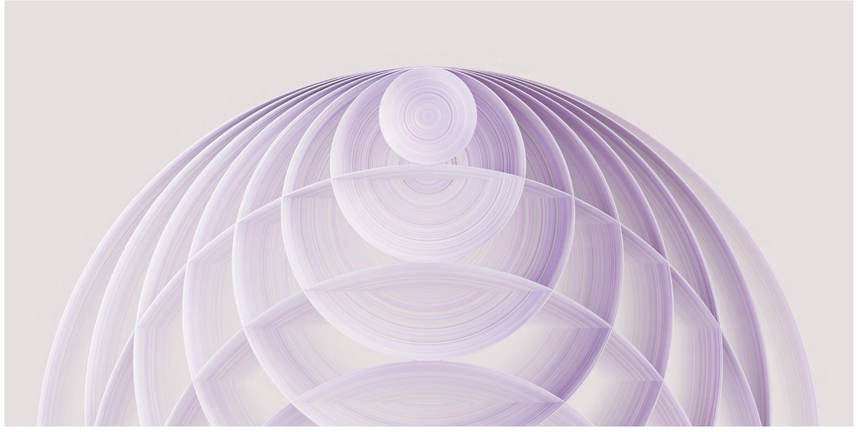

IBM

# Inhalte



# 01
# Einführung

## KI-Einsatz im Unternehmen dank Governance



Drängen Ihre Kollegen auf den operativen Einsatz von KI? Zu Recht!

In der Harvard Business Review wird berichtet[1], dass „es keine Übertreibung ist, die generative KI als revolutionär zu bezeichnen. Sie hat das Potenzial, die Produktivität in jeder Funktion, die kognitive Aufgaben umfasst, zu steigern."

Das Versprechen der KI ist unbestreitbar, und ebenso sicher ist es mit reellen Risiken verbunden. Ein gut durchdachter Governance-Ansatz bietet allen die Chance zum Fortschritt.

Mit Governance als Sicherheitsnetz gibt es keinen Grund, vor den revolutionären Aspekten der KI zurückzuschrecken.

Bringen Sie Ihr Unternehmen auf Erfolgskurs.

Lesen Sie weiter, um die ganze Geschichte zu erfahren, oder testen Sie watsonx.governance kostenlos.

Für den Markt der generativen KI wird eine jährliche Wachstumsrate von 24,40 % erwartet.[2]

02

# Herausforderungen bei der Skalierung von KI

Der Einfluss von KI nimmt exponentiell zu, da inzwischen Führungskräfte in Unternehmen aus fast jeder Branche diese Technologie einsetzen.

Gleichzeitig haben Mitarbeiter und Führungskräfte in vielen dieser Unternehmen Schwierigkeiten mit den folgenden Aspekten der Implementierung von KI.

**Es ist schwierig, KI sicher einzusetzen**
Es gibt eine Vielzahl von Tools für die KI-Governance, aber allzu oft werden Modelle ohne angemessene Klarheit, Überwachung oder Katalogisierung erstellt. Ohne eine durchgängige Verfolgung des KI-Lebenszyklus durch automatisierte Prozesse werden Skalierbarkeit und Transparenz der Prozesse behindert. Erklärbare Ergebnisse sind schwer zu erreichen.

Sie haben vielleicht schon von „Black-Box-Modellen“ gehört, die ein wachsendes Problem für KI-Akteure darstellen. KI-Modelle werden erstellt und implementiert, aber es ist nicht immer einfach nachzuvollziehen, wie und warum Entscheidungen getroffen wurden, selbst für die Data Scientists, die sie erstellt haben. Diese Herausforderungen führen zu mangelnder Effizienz, die Abweichungen beim Umfang, verzögert oder gar nicht in Produktion gehende Modelle zur Folge haben, oder Modelle mit uneinheitlichen Qualitätsniveaus und nicht erkannten Risiken.

Lesen Sie die wichtigsten Erkenntnisse aus einer Umfrage unter globalen IT-Entscheidungsträgern zum Tempo der KI-Einführung.

IBM Global AI Adoption Index 2022 →

**Es ist schwierig, Risiko und Reputation zu verwalten**
Sie kennen die Schlagzeilen: unfaire, unerklärliche oder verzerrte KI-Modelle in der Produktion. Die daraus resultierenden Fehlannahmen und -entscheidungen können sich auf Kunden auswirken und Ihrer Marke schaden.

Erklärbare Prozesse und Ergebnisse helfen Prüfern und Kunden zu verstehen, wie bestimmte Analyseergebnisse zustande gekommen sind. Solche Prozesse tragen dazu bei, dass die Ergebnisse keine Voreingenommenheit hinsichtlich Hautfarbe, Geschlecht, Alter oder anderen Schlüsselfaktoren widerspiegeln. Diese Verfahren sind für Patientendiagnosen und Behandlungspläne, die Überprüfung verdächtiger Transaktionen und abgelehnter Kreditanträge von entscheidender Bedeutung.

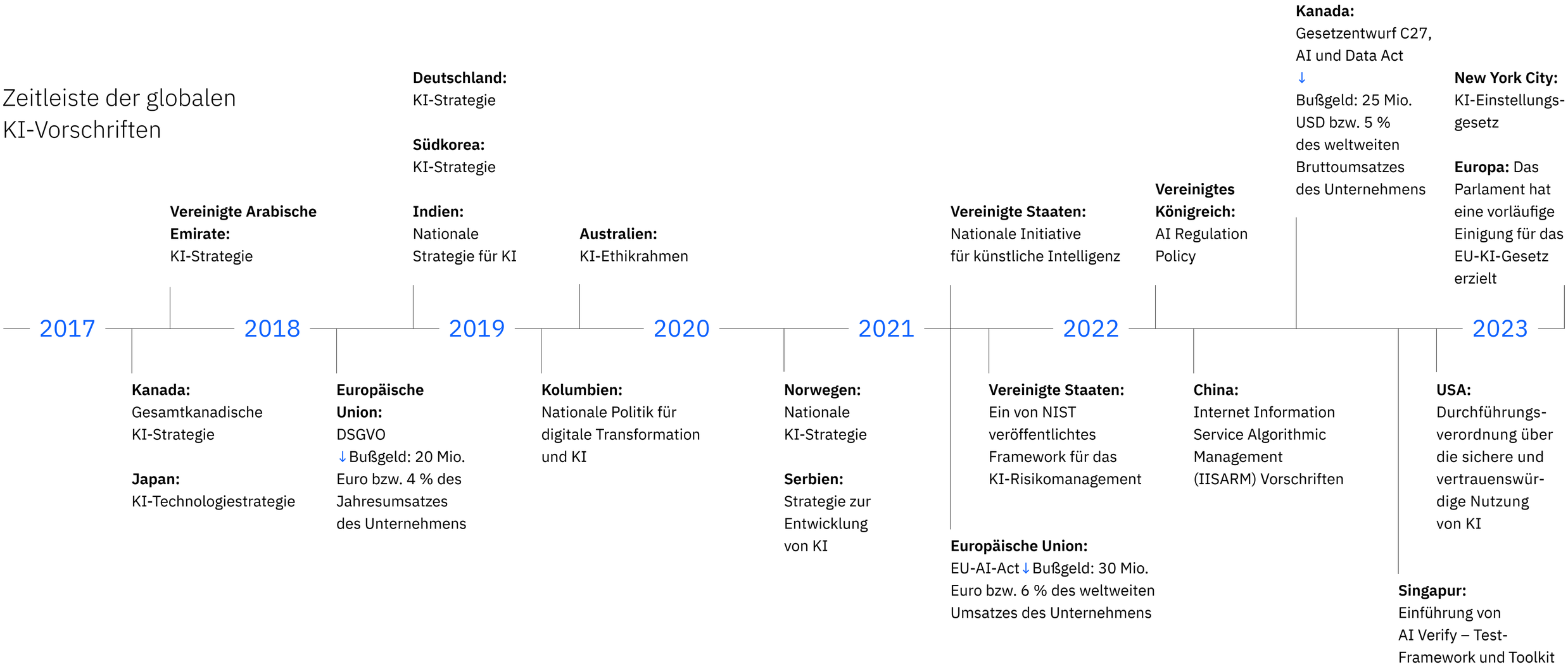
Ergreifen Sie Maßnahmen, um KI-Systeme aufzubauen, die transparent, erklärbar, fair und inklusiv sind. Damit tragen Sie dazu bei, Privatsphäre, Sicherheit, Kundentreue und Vertrauen zu wahren.

**Die KI-Vorschriften werden ständig weiterentwickelt**
Erfolgreiche KI erfordert die Einhaltung von Gesetzen und Vorschriften – auf lokaler, regionaler und nationaler Ebene –, deren Zahl in rasantem Tempo zunimmt. Die Nichteinhaltung könnte Ihr Unternehmen Bußgelder in zweistelliger Millionenhöhe kosten, wie einige der strengsten KI-Vorschriften zeigen, die derzeit weltweit diskutiert werden. Dazu gehört auch das vorgeschlagene KI-Gesetz der EU. Dessen aktueller Entwurf sieht Bußgelder von bis zu 30 Millionen Euro oder 6 % des weltweiten Umsatzes eines Unternehmens vor.

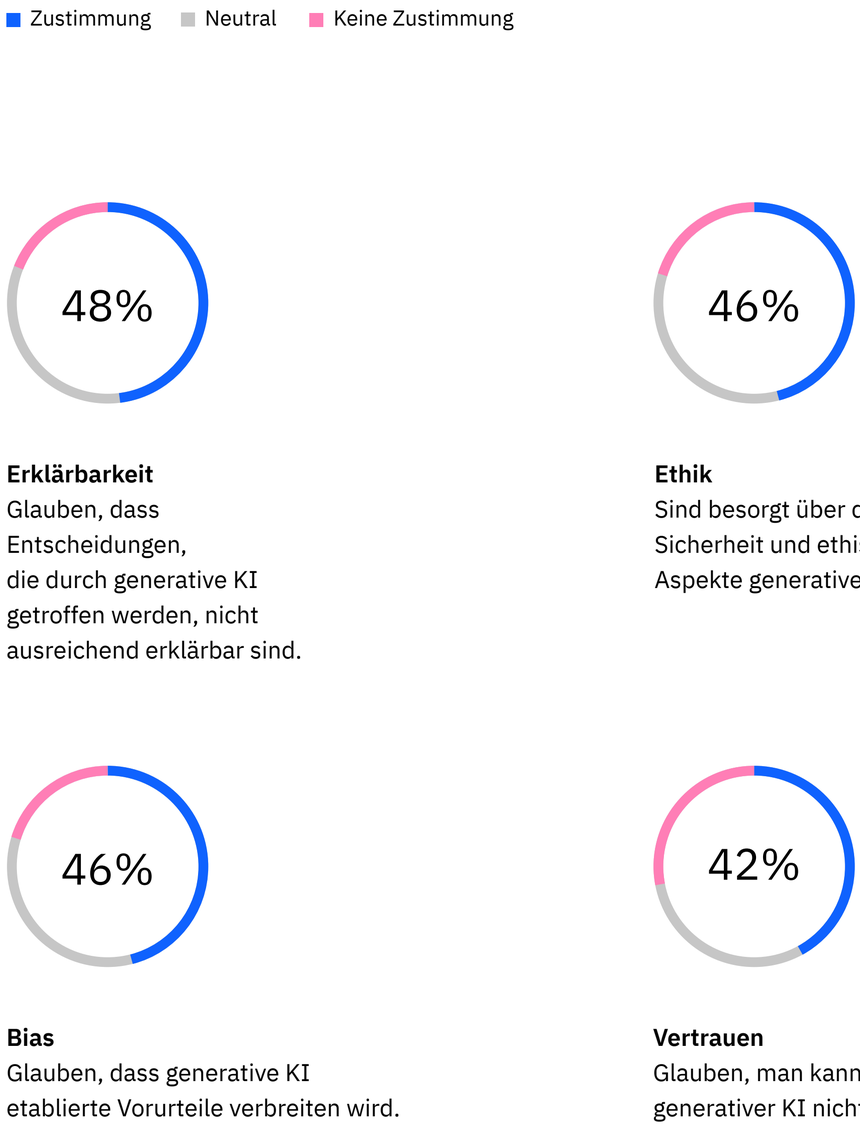
Die Modelldokumentation ist von entscheidender Bedeutung – und ein Bereich, der von einem unter Zeitdruck stehenden Data Scientist, dessen Unternehmen keine klaren Anforderungen vorgibt, leicht übersehen werden kann.

Lassen Sie diesen Schritt nicht außer Acht: Die neuen Vorschriften verlangen eine Modelldokumentation für Metadaten und Abstammung.

# Zeitleiste der globalen KI-Vorschriften



# 80 % der Führungskräfte in der Wirtschaft sehen mindestens eine dieser ethischen Fragen als großes Problem an[3]




**Erklärbarkeit**
Glauben, dass Entscheidungen, die durch generative KI getroffen werden, nicht ausreichend erklärbar sind.

**Ethik**
Sind besorgt über die Sicherheit und ethische Aspekte generativer KI.

**Bias**
Glauben, dass generative KI etablierte Vorurteile verbreiten wird.

**Vertrauen**
Glauben, man kann generativer KI nicht vertrauen.

03

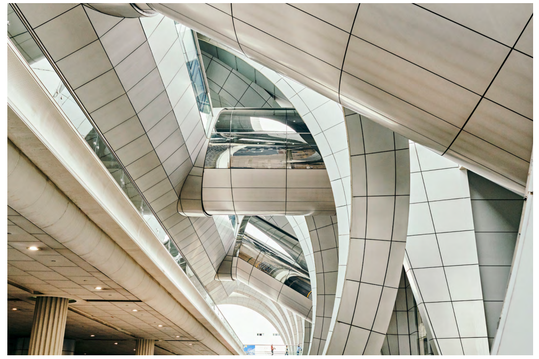
# Alle Modelle benötigen Governance

Nicht alle KI-Modelle werden auf die gleiche Weise erstellt. Aber alle Modelle brauchen Governance.

Die meisten Unternehmen setzen ab 2023 traditionelles maschinelles Lernen ein, und ihre Führungskräfte beginnen mit dem Einsatz generativer KI.

**Modelle für maschinelles Lernen**
ML-Modelle nutzen prädiktive Analysen, um Trends und Muster in Daten zu erkennen. Sie lernen aus Erfahrungen, um ihre Fähigkeiten zu verbessern und genauere analytische Entscheidungen treffen zu können. Diese Modelle werden aus Algorithmen erstellt, die entweder mit klassifizierten, unklassifizierten oder gemischten Daten trainiert werden. Durch maschinelle Lernverfahren können Modelle automatisch und ohne menschliches Eingreifen lernen.

Verschiedene Algorithmen des maschinellen Lernens eignen sich für unterschiedliche Zwecke, z. B. für die Klassifizierung oder die Vorhersagemodellierung, sodass Data Scientists verschiedene Algorithmen als Grundlage für verschiedene Modelle verwenden. Wenn Daten in einen bestimmten Algorithmus eingegeben werden, wird dieser so verändert, dass er eine bestimmte Aufgabe besser erfüllen kann, und wird zu einem maschinellen Lernmodell.



**Generative Modelle**
Diese KI-Modelle umfassen sowohl Basismodelle (FMs) als auch große Sprachmodelle (LLMs). Sie haben das Potenzial, wirtschaftliche Werte in Billionenhöhe freizusetzen, da ihre bemerkenswerte Leistungsfähigkeit die Produktivität steigert und sie für eine Vielzahl von Aufgaben eingesetzt werden können.

Solche Modelle sind hochgradig anpassbar, skalierbar und kosteneffizient. Sie können extrem große Datenmengen verarbeiten – und lernen dabei ständig dazu. Generative Anwendungen „von der Stange“ erfordern wenig Fachwissen und haben das Potenzial, viele mühsame und zeitaufwändige Aufgaben zu eliminieren.

In der Statistik werden generative Modelle seit Jahren zur Analyse numerischer Daten eingesetzt. In jüngster Zeit ist es durch Deep Learning möglich geworden, diese Modelle zu erweitern, um Bilder, Musik, Sprache, Videos, Text und sogar Code zu generieren. Anwendungsfälle können Marketing, Kundendienst, Einzelhandel und Bildung umfassen.

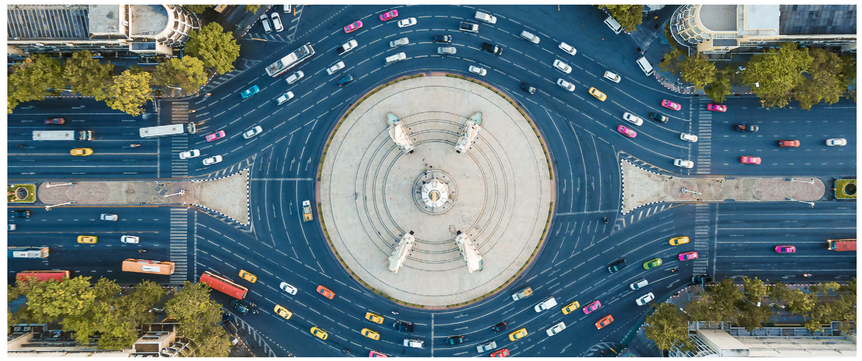
Während generative Modelle die KI für die meisten Führungskräfte ganz oben auf die Tagesordnung gesetzt haben, bringen ihre Fähigkeiten eine neue Komplexität mit sich, die sowohl für Unternehmen als auch für die Gesellschaft Risiken bergen kann.

Erfahren Sie, wie Sie KI verantwortungsvoll skalieren.

Blog lesen →

# 04
# Ganzheitliche KI-Governance

Wie jede andere Initiative hängt auch eine erfolgreiche KI-Governance vom Zusammenspiel von Menschen, Prozessen und Technologie ab.



Um KI richtig zu implementieren, bedarf es eines starken, funktionsübergreifenden Teams. KI ist für viele Führungskräfte ein strategischer Imperativ, und die Liste der Stakeholder wird gefühlt täglich länger. Für einige ist das Konzept des KI-Lebenszyklus neu, für andere gibt es neue Gründe, sich für KI zu engagieren.

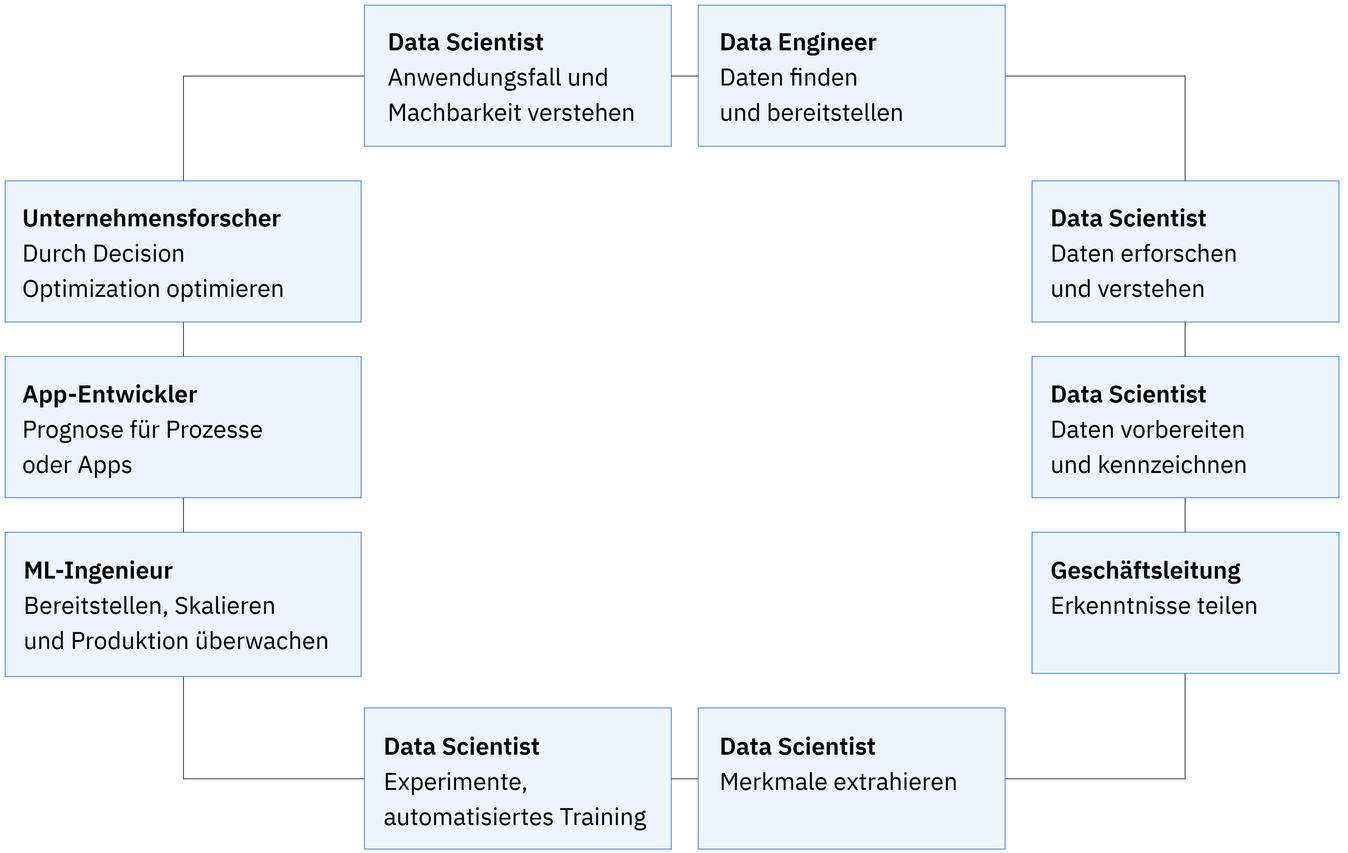
Versuchen Sie, den Anforderungen all dieser Gruppen gerecht zu werden, ohne Ihre Data Scientists zu überfordern, die nur wenig Zeit haben, Genehmigungen und Informationsanfragen weiterzuleiten oder zu verwalten.

Ihre Stakeholder in Einklang zu bringen, ist ein guter Start. Holen Sie sich die Zustimmung der richtigen Stakeholder und ermutigen Sie sie, sich an der Ideenfindung zu beteiligen, sich an den Ergebnissen zu orientieren und verantwortungsvolle KI einzuführen. Ergreifen Sie dann Maßnahmen, um sicherzustellen, dass die richtigen Metriken, KPIs und Ziele in Übereinstimmung mit den Geschäftskontrollen und -vorschriften Ihres Unternehmens definiert werden. Sie sollten auch die spezifischen Metriken überwachen, die für KI-Modelle identifiziert wurden.

Erfahren Sie, wie Sie einen ganzheitlichen Ansatz für die KI-Governance entwickeln

Blog lesen →

# Rollen im gesamten KI-Lebenszyklus




Förderung der Zusammenarbeit mit den wichtigsten Stakeholdern und Kenntnis ihrer Hauptanliegen:

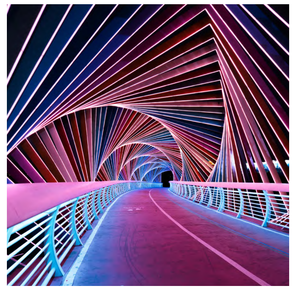
- CFO – Risiken für die Rentabilität
- CMO – Risiken für die Marke
- CRO – Risiken für das Unternehmen
- CDO – effiziente Datenverarbeitung
- CHRO – potenzielle Auswirkungen auf Talente
- CEO – organisatorische Verantwortlichkeit
- CPO – regulatorische Verantwortlichkeit

**Prozess**
Die KI-Governance verfolgt und dokumentiert den Ursprung von Daten, die zugehörigen Modelle und Metadaten sowie die gesamten Datenpipelines für die Prüfung. Die Dokumentation sollte die für jedes Modell verwendeten Trainingstechniken, die verwendeten Hyperparameter und die Metriken der Testphasen enthalten. Dadurch erhalten die Stakeholder einen besseren Einblick in das Verhalten des Modells während seines gesamten Lebenszyklus, einschließlich der Daten, die bei seiner Entwicklung eine Rolle gespielt haben, und der potenziellen Risiken des Modells.

Zunächst sollten Sie die aktuellen KI-Technologien und -Prozesse in Ihrem Unternehmen vergleichen und bewerten. Einige Prozesse und Stakeholder sind möglicherweise bereits aufeinander abgestimmt und können erweitert werden, während andere möglicherweise ersetzt werden müssen. Erstellen Sie dann eine Reihe von automatisierten Governance-Workflows, die den Compliance-Anforderungen entsprechen. Neue und bestehende KI-Modelle können diese Workflows unterstützen, die so gestaltet sein sollten, dass die oben genannten Prozessverzögerungen vermieden werden. Schließlich sollte ein Framework eingerichtet werden, um Eigentümer und Nutzer zu warnen, wenn die Metriken eines Modells den akzeptablen Schwellenwert überschreiten.

**Technologie**
Der Aufbau einer gut geplanten, gut ausgeführten und gut kontrollierten KI erfordert spezifische technologische Bausteine. Suchen Sie nach einer Lösung, die den End-to-End-KI-Lebenszyklus abdeckt und über die folgenden Funktionen verfügt:

- Integration von Daten unterschiedlicher Art und Herkunft im Zuge verschiedener Bereitstellungen
- offenes und flexibles System, das arbeitet mit den vorhandenen Tools Ihrer Wahl arbeitet
- Self-Service-Zugriff mit Datenschutzkontrollen und der Möglichkeit, die Datenabstammung zurückzuverfolgen
- Automatisierung von Modellerstellung, Bereitstellung, Skalierung, Schulung und Überwachung
- Verbindung mehrerer Stakeholder durch einen anpassbaren Workflow
- Unterstützung beim Erstellen von benutzerdefinierten Workflows für verschiedene Personas mithilfe von Governance-Metadaten



# Ein Framework für verantwortungsvolle, kontrollierte KI

| | KI zuverlässig einsetzen | Risiko und Reputation verwalten | Compliance verbessern | Anforderungen der Stakeholder erfüllen |
|---|---|---|---|---|
| Plan | Messbare Leistungsmetriken für die KI-Nutzung in Ihrem Unternehmen definieren | Bestehende Prozesse zur Überwachung von Fairness und Erklärbarkeit überwachen | Eine Lückenanalyse in Bezug auf aktuelle und potenzielle KI-Vorschriften durchführen | Die vorhandenen Fähigkeiten und den Bedarf an verantwortungsvoller KI überprüfen und mit den Geschäftszielen abstimmen |
| Aufbauen | Nachvollziehbarkeit und Überprüfbarkeit aktueller Prozesse sicherstellen | Aktualisierte Prozesse und Kontrollpunkte während des gesamten KI-Lebenszyklus einsetzen | Sicherstellen, dass die Modelldokumentation zugänglich ist | Neue Rollen, Fähigkeiten und Lernprogramme, die für die Umsetzung verantwortungsbewusster KI erforderlich sind, spezifizieren |
| Erstellen | Automatische Dokumentation der Modellherkunft und Metadaten erstellen | Faire, erklärbare und qualitativ hochwertige KI-Modelle bereitstellen, Drift minimal halten und regelmäßige Richtlinienüberprüfungen durchführen | Maßnahmen zur Einhaltung gesetzlicher Vorschriften für Data-Science-Teams ohne Mehraufwand ergreifen | Einen wiederholbaren End-to-End-Workflow mit integrierten Genehmigungen der Stakeholder einrichten, um das Risiko zu senken und den Umfang zu erhöhen |

05

# watsonx.governance für verantwortungsvolle, transparente und erklärbare KI.

Lernen Sie das Toolkit für KI-Governance kennen. Der Ansatz von IBM watsonx.governance hilft Ihnen, die KI-Aktivitäten Ihres Unternehmens zu steuern, zu verwalten und zu überwachen.

Dieses Toolkit basiert auf der KI- und Datenplattform von IBM watsonx und nutzt Softwareautomatisierung, um Ihre Fähigkeit, regulatorische Anforderungen zu erfüllen und ethische Bedenken zu berücksichtigen, auszubauen.

Sie erhalten eine umfassende KI-Governance ohne die übermäßigen Kosten eines Wechsels von Ihrer aktuellen Data-Science-Plattform.

Bevor ein Modell in Produktion geht, wird es validiert, um Geschäftsrisiken zu bewerten. Sobald das Modell in Betrieb ist, wird es kontinuierlich auf Fairness, Qualität und Drift überwacht. Aufsichtsbehörden und Prüfer können auf die Dokumentation zugreifen, die das Verhalten und die Vorhersagen des Modells enthält.

Sie können Transparenz darüber bieten, wie das Modell funktioniert und welche Prozesse es durchlaufen hat und wie es trainiert wurde.

watsonx.governance erstreckt sich über den gesamten Lebenszyklus, und Ihre Teams erhalten Unterstützung beim Entwerfen, Erstellen, Bereitstellen, Überwachen und Zentralisieren von Fakten für die Erklärbarkeit durch KI.

Mit diesem Governance-Toolkit können Audits einfacher werden. Verfolgen und dokumentieren Sie die Herkunft der Daten, der Modelle und der zugehörigen Metadaten sowie der Pipelines.

Die Dokumentation sollte die für jedes Modell verwendeten Trainingstechniken, die verwendeten Hyperparameter und die Metriken der Testphasen enthalten.

Erwarten Sie mehr Transparenz über das Verhalten jedes Modells während seines gesamten Lebenszyklus, Wissen über die Daten, die bei seiner Entwicklung eine Rolle gespielt haben, und die Möglichkeit, potenzielle Risiken zu identifizieren.

# IBM Prinzipien einer verantwortungsvollen KI

Der Zweck von KI besteht darin, die menschliche Intelligenz zu erweitern

Daten und Erkenntnisse gehören ihrem Ersteller

KI-Systeme müssen transparent und erklärbar sein

# Beachten Sie diese Komponenten:

## Einhaltung von Vorschriften

Managen Sie KI so, dass diese weltweit die neuesten Sicherheits- und Transparenzvorgaben und -richtlinien erfüllt. Betrachten Sie es als eine Art „Inhaltsdeklaration“ für KI.

- Umsetzung externer KI-Vorschriften in Richtlinien zur automatischen Durchsetzung
- Bessere Einhaltung von Audit- und Compliance-Vorschriften
- Nutzung dynamischer Dashboards für die Einhaltung aller Richtlinien und Vorschriften

**Automatische Metadaten**
Datenkonvertierung und Abstammungserfassung durch Python-Notebooks.

## Risikomanagement

Erkennen und mindern Sie Risiken proaktiv, überwachen Sie Fairness, Verzerrung, Drift und neue LLM-Metriken.

- Automatisieren Sie Fakten und Workflows zur Einhaltung von Geschäftsstandards
- Identifizieren, verwalten, überwachen und berichten Sie über Risiken und Regelkonformität in großem Maß.
- Nutzen Sie dynamische Dashboards für klare, prägnante und anpassbare Ergebnisse
- Verbessern Sie die Zusammenarbeit über mehrere Regionen und Standorte hinweg

**Offen**
Unterstützung Sie die Verwaltung von Modellen, die in Tools von Drittanbietern erstellt und verwendet werden.

## Lebenszyklus-Governance

Verwalten, überwachen und steuern Sie KI-Modelle von IBM, Open-Source-Communitys und anderen Modellanbietern.

- Überwachen, katalogisieren und steuern Sie KI-Modelle von dort aus, wo sie sich befinden, in großem Maß.
- Automatisieren Sie die Erfassung von Modellmetadaten
- Erhöhung der Vorhersagegenauigkeit, indem Sie erkennen, wie KI eingesetzt wird und wo sie im Rückstand ist

**Umfassend**
Steuerung des gesamten End-to-End-Lebenszyklus der KI.

06

# KI-Governance in Aktion

## IBM Chief Privacy Officer ↷

**Skalierung der Automatisierung zur Erfüllung regulatorischer Anforderungen an KI**
Gestützt auf das KI-Framework des Unternehmens zur Erfüllung der regulatorischen Anforderungen an KI hat das Chief Privacy Office (CPO) von IBM wichtige Schritte zur Umsetzung branchenführender KI- und Datenfunktionen unternommen, die auf einer starken Kombination aus Datenschutz, Sicherheit, KI-Governance, Ethik, Prozessen, Technologie und Tools basieren.

Der IBM CPO hat mit Unterstützung des IBM AI Ethics Board eine Reihe verbesserter Prozesse entwickelt, die eine detailliertere Nachverfolgung der Einhaltung bestehender Standards und geltender gesetzlicher Anforderungen ermöglichen.

Durch die Nutzung des integrierten Governance-Frameworks und -Prozesses von IBM, mit dem Ziel, die Entwicklung und den Einsatz von KI im gesamten Unternehmen zu steuern und zu überwachen, sind die Teams jetzt in der Lage:

- einen robusten Workflow mit IBM Tools zur Erfassung, Konsolidierung, Anzeige und Überwachung des Workflows zu erstellen
- die Erfassung und Integration von Fakten aus dem KI-Lebenszyklus automatisieren, um die Pflege des globalen KI-Bestands zu beschleunigen

Mehr erfahren →

07

# Nächste Schritte

Sehen Sie, wie schnell Sie mit dem watsonx. governance-Toolkit verantwortungsvolle, transparente und erklärbare KI-Workflow erstellen können – ohne die Kosten für den Wechsel von Ihrer aktuellen Data-Science-Plattform.

- KI-Governance operationalisieren
- Risiko und Reputation verwalten
- Unterstützung der Einhaltung von Vorschriften

## Erste Schritte

Demo anfordern →
Mehr erfahren über das Governance-Toolkit →
Kostenlos selbst ausprobieren →

1. „How to capitalize on generative AI“, Harvard Business Review, 2023.

2. „Generative AI worldwide“, Statista, 2023.

3. „Generative AI: The state of the market”, IBM Institute for Business Value, 2023.



IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de
IBM Corporation
New Orchard Road
Armonk, NY 10504

Hergestellt in den Vereinigten Staaten von Amerika
November 2023



Das vorliegende Dokument ist ab dem Datum der Erstveröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle Angebote sind in allen Ländern verfügbar, in denen IBM tätig ist.

Alle angeführten oder beschriebenen Beispiele illustrieren lediglich, wie einige Kunden IBM Produkte verwendet haben und welche Ergebnisse sie dabei erzielt haben. Die tatsächlichen Umgebungskosten und Leistungsmerkmale variieren in Abhängigkeit von den Konfigurationen und Bedingungen des jeweiligen Kunden. Es können keine generell zu erwartenden Ergebnisse bereitgestellt werden, da die Ergebnisse jedes Kunden allein von seinen Systemen und bestellten Services abhängen. Es liegt in der Verantwortung der Anwender, die Nutzbarkeit anderer Produkte oder Programme neben den Produkten und Programmen von IBM zu evaluieren und verifizieren.



Erklärung zu bewährten Sicherheitsverfahren: Kein IT-System oder -Produkt sollte als vollkommen sicher angesehen werden, und kein einzelnes Produkt, kein Service und keine Sicherheitsmaßnahme kann eine missbräuchliche Nutzung oder einen missbräuchlichen Zugriff vollständig verhindern. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vor böswilligem oder rechtswidrigem Verhalten von Dritten geschützt sind oder Ihr Unternehmen davor schützen.

Die Einhaltung sämtlicher geltender Gesetze und Vorschriften liegt in der Verantwortung des Kunden. IBM bietet keine Rechtsberatung an und gewährleistet nicht, dass die Services oder Produkte von IBM die Konformität von Gesetzen oder Verordnungen durch den Kunden sicherstellen.