



Data Governance und AI Governance

DER WEG ZUM VERANTWORTUNGSVOLLEN UND SICHEREN EINSATZ VON KI



Von Industrie und Dienstleistung über Finanzen und Versicherungen bis hin zu Handel und öffentlicher Hand – in Zeiten des demografischen Wandels, Fachkräftemangels und sich stetig verändernder Marktbedingungen stehen viele Organisationen vor der gleichen Frage: Wie lassen sich Arbeitsprozesse optimieren sowie Arbeitsmethoden und Ressourcen effizient einsetzen, um wettbewerbsfähig zu bleiben, Kosten zu sparen oder Verwaltungsaufgaben, Staats- und Bürgerdienste mit weniger Personal zu bewältigen? Dabei liegt die Hoffnung vermehrt auf künstlicher Intelligenz, insbesondere generativer KI. Organisationen entwickeln deshalb immer häufiger Ideen, ihre Prozesse mithilfe einer eigenen KI-Lösung zu automatisieren.

Elementar dabei: Neben geeigneten Use Cases muss die KI sicher, vertrauenswürdig und rechtskonform sein. Und das geht nur mit fundierter Governance für die zugrundeliegenden Daten und eingesetzten KI-Lösungen. Diese unabdingbaren Voraussetzungen einer sicher nutzbaren KI-Lösung innerhalb einer Organisation gehen Computacenter und IBM strukturiert, regelkonform und auf Basis langjähriger Erfahrung an.

Für Organisationen steht häufig ein geeigneter Use Case am Anfang ihrer KI-Reise. So können KI-Lösungen beispielsweise in der IT dabei unterstützen, eine Vielzahl komplexer Dokumente wie Serviceverträge, Verordnungen, Erlässe oder Bedienungsanleitungen zu sichten und zu überprüfen, während Personalabteilungen Bewerbungsdokumente oder Angaben in Bewerbungsportalen schnell und sicher analysieren können. In der Fertigung lassen sie sich für Qualitätskontrollen, den effizienten Einsatz von Ressourcen oder in der Landwirtschaft für die Auswertung von Satellitenbildern einsetzen, um den Einsatz von Düngemitteln oder Wasser zu optimieren. Nicht zuletzt können KI-Lösungen Behörden dabei helfen, ihren Bürgerservice oder die Kommunikation zwischen Bürger:innen und Behörde zu verbessern.

In all diesen Anwendungsszenarien setzen KI-Tools sinnvollerweise auf bereits bestehende Strukturen auf und greifen auf vorliegende Datensätze zu. Jedoch müssen Organisationen gewährleisten, dass sensible Unternehmensdaten, die von einer KI genutzt werden, geschützt sind und die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gewahrt ist. Auch und vor allem rund um den Einsatz von Künstlicher Intelligenz wissen Unternehmen darum, dass sie das Vertrauen von Mitarbeitenden, Kunden und Partnern in die Organisation nicht leichtfertig aufs Spiel setzen dürfen. Damit scheitern Consumer-KI-Lösungen wie ChatGPT aus. Stattdessen sind maßgeschneiderte KI-Fähigkeiten notwendig, die sich in firmeneigene Applikationen integrieren lassen und den genannten Anforderungen gerecht werden.

Ziel ist es, mit KI die Effizienz und Effektivität der Organisation nachhaltig zu steigern und dabei cybersicher zu agieren, das Vertrauen von Kunden und Mitarbeitenden in die KI zu stärken und durch die gezielte Auswertung und Nutzbarmachung von Daten die eigene Wettbewerbsfähigkeit zu erhöhen.

DAS RICHTIGE MINDSET VOR DEM START: DIE KI „LEBT“ – UND ERFORDERT MANAGEMENT

Vor dem Einsatz einer KI-Lösung müssen sich Organisationen darüber im Klaren sein, dass KI-Systeme nicht nur leistungsfähige Werkzeuge sind, um Entscheidungen zu treffen oder Aufgaben zu automatisieren, sondern auch Risiken und Herausforderungen im Bereich Sicherheit und Governance sowie hinsichtlich der zugrundeliegenden Daten mit sich bringen. Denn KI ist keine Technologie wie andere, die – einmal beschafft – in vielen Fällen nach dem Einsatz nur hin und wieder aktualisiert wird. KI erfordert ein kontinuierliches Management. Und das aus zwei Gründen, die sich mitunter gravierend auswirken können: Regulatorische Anforderungen und die Risiken hinsichtlich der Qualität einer KI.

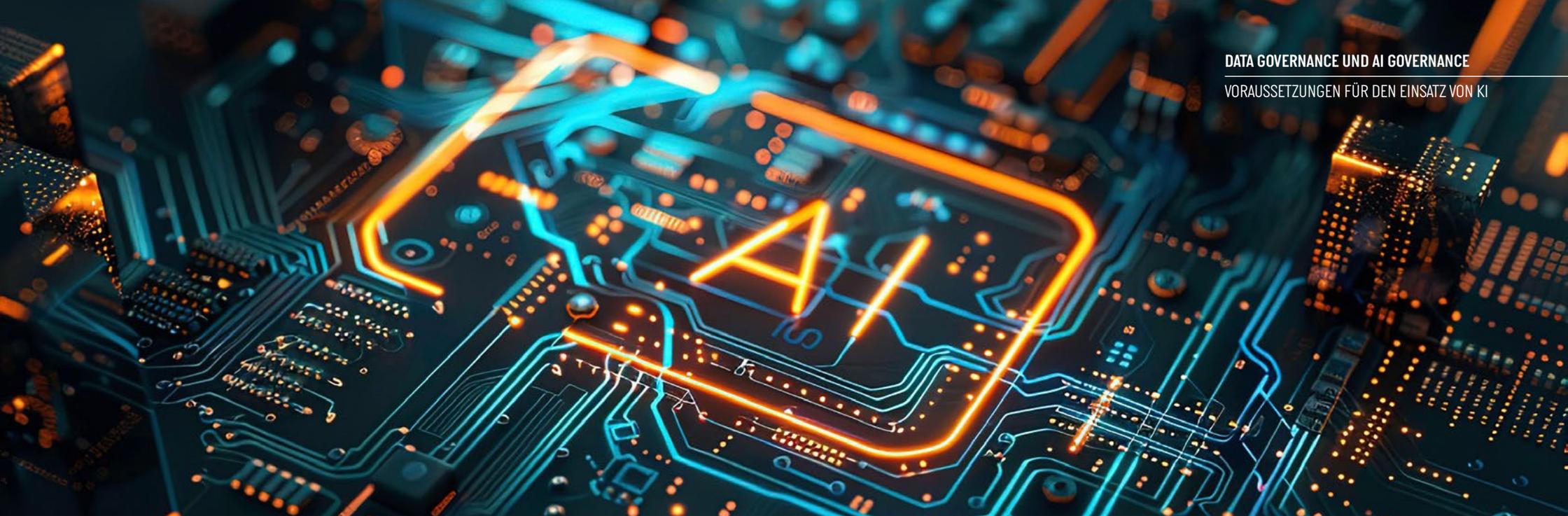
REGULATORISCHE ANFORDERUNGEN

Im August 2024 ist der EU AI Act in Kraft getreten, der den Einsatz von KI regeln soll. Für bestehende und neue KI-Lösungen ist im ersten Schritt die Einstufung nach EU AI Act Pflicht. Es drohen hohe Geldbußen, die sich an den Sanktionen der Datenschutzgrundverordnung orientieren, wenn Unternehmen oder Behörden gegen die Anforderungen des EU AI Acts verstoßen. Hinzu kommen langfristige Reputationsschäden.

Die Einteilung von KI erfolgt dabei in drei Risikoklassen: KI-Lösungen mit unannehmbarem Risiko sind verboten. KI-Tools mit begrenztem Risiko müssen nur geringe Anforderungen erfüllen, während KI-Systeme mit minimalem Risiko keine Anforderungen erfüllen müssen. Dagegen erfordern KI-Lösungen mit hohem Risiko ein professionelles Risikomanagementsystem, eine Data Governance, technische Dokumentation, Monitoring, menschliche Aufsicht und Cybersicherheitsmaßnahmen.

RISIKOKLASSE	BEISPIELE	ANFORDERUNGEN
Unannehmbares Risiko	<ul style="list-style-type: none"> • Unterschwellige Verhaltensmanipulation • Social Scoring 	<ul style="list-style-type: none"> • Verboten
Hohes Risiko	<ul style="list-style-type: none"> • Betrieb Straßenverkehr • Bewerbungstools • Kreditwürdigkeit 	<ul style="list-style-type: none"> • Risikomanagementsystem • Data Governance • Technische Dokumentation • Monitoring und menschl. Aufsicht • Cybersicherheit
Begrenztes Risiko	<ul style="list-style-type: none"> • Chatbots • Bild-, Video-, Tonerzeugung 	<ul style="list-style-type: none"> • Transparenz und Offenlegung
Minimales Risiko	<ul style="list-style-type: none"> • Spamfilter • AI-Videospiele 	<ul style="list-style-type: none"> • Keine Anforderungen

Viele Organisationen, ob sie KI-Modelle nun bereits im Einsatz haben oder dies erst planen, wissen, dass sie handeln müssen – jedoch nicht, wie sie den Einstufungsprozess und den daraus folgenden Handlungsbedarf strukturiert angehen.



RISIKEN HINSICHTLICH DER QUALITÄT EINER KI

Neben den regulativen Anforderungen birgt KI auch Risiken, die nicht unterschätzt werden dürfen. Drei der bedeutendsten sind BIAS, Drift und Halluzination.

- BIAS, oder Verzerrung, tritt auf, wenn KI-Systeme auf Grundlage von voreingenommenen Daten trainiert werden. Dies kann zu diskriminierenden Ergebnissen führen, die bestimmte Gruppen benachteiligen. Ein Beispiel hierfür ist die Gesichtserkennung, die bei Menschen mit dunkler Hautfarbe oft weniger genau ist.
- Drift bezieht sich auf die Veränderung der Daten oder der Umgebung, in der die KI operiert. Ändern sich die Bedingungen, kann die Leistung der KI nachlassen, da sie auf veralteten Informationen basiert. Dies ist besonders kritisch in dynamischen Umgebungen wie der Finanzwelt oder im Gesundheitswesen.
- Halluzinationen in KI-Systemen treten auf, wenn diese Informationen ohne Bezug zur Realität generieren. Dies kann zu Problemen führen, wenn die KI in sicherheitskritischen Anwendungen eingesetzt wird, wo falsche Informationen schwerwiegende Konsequenzen nach sich ziehen.

DIE RICHTIGEN DATEN FÜR DIE GEWÜNSCHTEN ERGEBNISSE

Eine hohe Datenqualität und der verantwortungsbewusste Umgang mit sensiblen Daten bilden die Grundlage jeder erfolgreichen KI-Lösung. Denn nur so kann diese wertvolle Erkenntnisse und Mehrwerte schaffen sowie menschliche Fähigkeiten wie Hören, Sehen, Sprechen und große Datenmengen analysieren und bewältigen.

Eine mangelhafte Datenqualität kann im Umkehrschluss dazu führen, dass KI-Modelle falsche oder ungenaue Ergebnisse liefern. Dies führt zu Fehlentscheidungen und potenziellen Schäden. Sind sensible Daten nicht ordnungsgemäß geschützt, riskieren Organisationen Datenschutzverletzungen. Diese ziehen nicht nur rechtliche Konsequenzen nach sich, sondern beeinträchtigen auch das Vertrauen der Kunden und die eigene Reputation.

Ein weiteres Problem ist die fehlende Konsistenz und Auffindbarkeit der Daten. Ohne klare Richtlinien und Prozesse kann es schwierig sein, die für einen Use Case benötigten Daten schnell und effizient zu finden, wodurch sich Entwicklung und Implementierung von KI-Lösungen verzögern. Zudem kann der unkontrollierte Zugriff auf Daten zu Missbrauch und Verlust führen, was die Sicherheit und Integrität der Daten gefährdet.

Regulatorik und Risiken zeigen, dass der Einsatz von KI sorgfältig überwacht und reguliert werden muss. Nur so lässt sich erreichen, dass dieser auch verantwortungsvoll und sicher ist. Wollen Organisationen KI-Tools und -Plattformen nutzen, müssen sie daher nicht nur regulativen Anforderungen gerecht werden, sondern auch für Datensicherheit und -qualität, Risikomanagement, Transparenz und ein Rollenmanagement sorgen. Für Verantwortliche sind die sogenannte „Data Governance“ und „AI Governance“ deshalb von entscheidender Bedeutung. Beide Bereiche sind eng miteinander verzahnt, da Datensätze die Grundlage für KI-Modelle bilden.



DATA GOVERNANCE UND AI GOVERNANCE – WICHTIGE VERBÜNDETE

Data Governance konzentriert sich auf das strategische und umfassende Management der Daten, auf die die KI zugreift. Ohne eine solide Data Governance können schwerwiegende Vorfälle auftreten, die den Erfolg von KI-Projekten gefährden. Data Governance stellt sicher, dass diese Risiken minimiert werden, indem sie klare Richtlinien und Verantwortlichkeiten festlegt. Sie gewährleistet, dass Daten qualitativ hochwertig, gut strukturiert und sicher sind, sodass sie effektiv für KI-Anwendungen genutzt werden können. Durch die Einhaltung von Datenschutz- und Compliance-Anforderungen wird das Risiko von Vorfällen reduziert und die Grundlage für erfolgreiche KI-Projekte geschaffen.

Der Bereich AI Governance fokussiert sich auf die Steuerung, die Dokumentation und das Monitoring der genutzten KI-Modelle – und ist somit unter anderem für die Qualitätsanforderungen an die KI

verantwortlich. Deshalb macht AI Governance den effektiven Einsatz von KI überhaupt erst möglich.

AI Governance und Data Governance sind keine „lästige Pflicht“, sondern angesichts geltender Regularien wie dem EU AI Act oder der DSGVO essenzielle und rechtlich bindende Grundlagen, um Risiken zu minimieren, Innovation zu fördern und ethisch verantwortungsvoll zu agieren. Sie bilden das Fundament für den langfristigen Erfolg und das Vertrauen in neue Technologien sowie für die eigene Reputation. Sie sichern die Qualität für fundierte KI-basierte Voraussagen. Wollen Organisationen also verantwortungsvolle KI-Lösungen erstellen, ist ein strukturiertes Vorgehen unverzichtbar. Was wie eine unlösbare Aufgabe wirken kann, lässt sich Schritt für Schritt und mit der richtigen Unterstützung strukturiert und erfolgreich angehen.

DATA GOVERNANCE

Verwaltung und Kontrolle von Daten

Data Governance bezieht sich auf die Richtlinien, Prozesse, Standards und Verantwortlichkeiten, die festgelegt werden, um sicherzustellen, dass Daten korrekt, sicher und nutzbar sind.

Die Hauptziele der Data Governance sind Datenqualität, Datensicherheit und Datenschutz durch Einhaltung gesetzlicher Vorschriften wie DSGVO, Datenverantwortlichkeit und Datenverfügbarkeit.

AI GOVERNANCE

Steuerung der Nutzung von KI

AI Governance bezieht sich auf die Implementierung und Überwachung von Prozessen, die darauf abzielen, potenzielle Risiken im Einsatz von AI-Systemen zu minimieren, um deren Sicherheit und ethische Integrität zu gewährleisten.

DATA GOVERNANCE ALS BASIS DER EIGENEN KI

Qualitativ hochwertige Daten stellen die Grundlage jeder erfolgreichen KI-Lösung dar. Innerhalb der Organisationen liegen die relevanten Daten für den jeweiligen Use Case in der Regel bereits vor. Planen Organisationen, diese Daten für eine eigene KI-Lösung einzusetzen und KI-Modelle mit diesen Daten zu trainieren, besteht eine der ersten Herausforderungen darin, die notwendigen Daten zu identifizieren und diese sicher und verantwortungsvoll nutzbar zu machen.

Hier kommt die Data Governance ins Spiel: Sie stellt sicher, dass die Daten Anforderungen wie Zugriffskontrolle, Auffindbarkeit, Konsistenz und Verständlichkeit erfüllen und Regulatorien wie der EU AI Act und die DSGVO eingehalten werden. Die Daten müssen zudem gut strukturiert, vollständig, für den KI-Einsatz repräsentativ und qualitativ hochwertig sein. Darüber hinaus muss die Nutzung zum Zweck des Use Cases überhaupt grundsätzlich erlaubt sein, beispielsweise aus Datenschutzgründen. Ohne klare Datenrichtlinien, Verantwortlichkeiten und Prozesse zur Sicherstellung der Datenqualität könnte KI nicht nur keinen Mehrwert bieten, sondern auch gefährlich für die Unternehmensreputation werden.

Zu den größten Herausforderungen im Bereich Data Governance gehören:

QUALITÄT UND VERTRAUEN

- **Sicherstellung der Datenqualität**
[Sind die Daten geprüft, bereinigt und korrekt?]
- **Wem gehören die Daten?**
- **Art und Qualität der Trainingsdaten für das KI-Modell**
- **Sind die Daten klassifiziert?**

SENSIBILITÄT DER DATEN

- **Personenbezogene sensible Daten**
- **Datenverantwortlichkeit**

WERT DER DATEN

- **Art der gespeicherten Informationen**
- **Sicherstellen von Datenverfügbarkeit und -zugriff**

DATENSICHERHEIT UND -SCHUTZ

- **Schutz vor Missbrauch**
- **Cybersicherheit von Plattformen und Daten**



DATA GOVERNANCE: UNSER SERVICE

Für Daten und KI-basierte Workflows bietet Computacenter eine umfassende Lösung zur Integration von Data Governance in das bestehende Information Security Management System (ISMS) einer Organisation an. Im Rahmen einer Bestandsaufnahme und Analyse auf Basis des bestehenden ISMS identifizieren wir relevante Daten und Verantwortlichkeiten. Wir prüfen, wie dies im Hinblick auf die KI, den geplanten Use Case sowie relevante Regulierungen und bestehende Richtlinien unter dem Aspekt der Datennutzung für KI zusammenpasst. Es erfolgt ein Abgleich und eine Ergänzung mit datensicherheitsrelevanten Regulatorien wie DSGVO, EU AI Act, EU Data Act oder DORA. Wir geben Empfehlungen, wie der Datenzugriff von allen Mitarbeitenden gemäß festgelegter Standards und Richtlinien erfolgen kann. Auf diese Weise minimiert Data Governance das Risiko von Datenmissbrauch und -verlust und trägt zur Einhaltung von Datenschutz- und Compliance-Anforderungen bei.

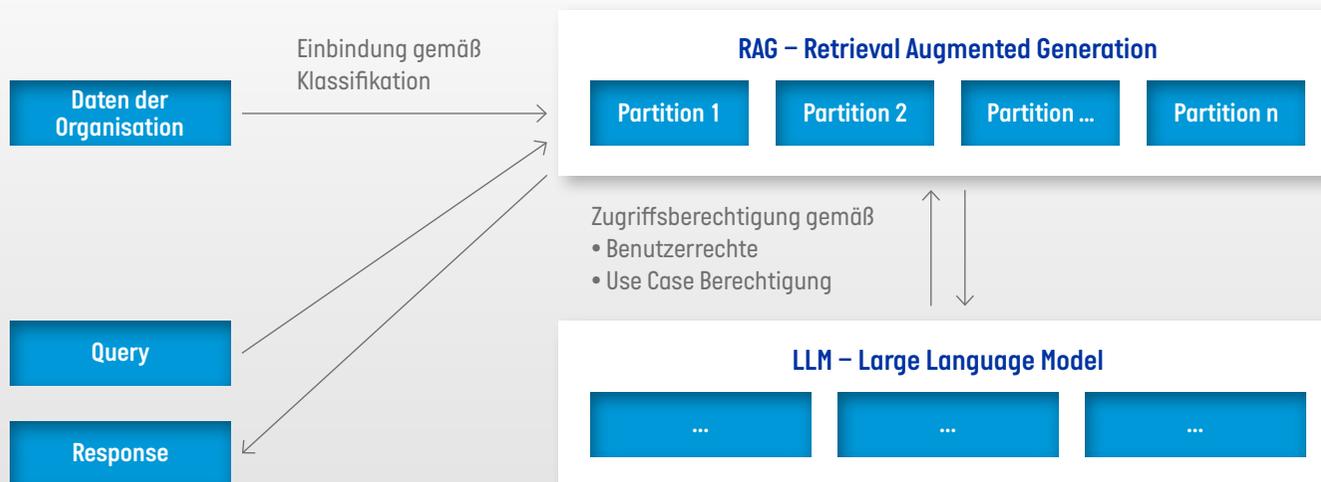
Ziel ist es, die gesetzlichen Vorschriften einzuhalten und Datenmissbrauch- und Verlustrisiken zu reduzieren. Darüber hinaus erarbeiten wir konkrete Empfehlungen für Data und KI-Plattformen.

Beispielsweise dazu, wie der Datenzugriff und die Teilung von Daten zu definieren ist, wie sich die Verwendung der Daten nachvollziehbar dokumentieren lässt oder wie sich die vorliegenden Daten klassifizieren lassen, um Datenqualität und -sicherheit zu erhöhen – und wie sich all dies auf einer Plattform umsetzen lässt.

UNSER VORGEHEN

Eine Daten- und KI-Plattform besteht unter anderem aus einer Benutzerschnittstelle oder Applikation, dem KI-Modell und Datenbanken. Bei der Verwendung der Daten für das Training als auch bei der späteren Anwendung des Modells muss sichergestellt werden, dass jede:r Nutzer:in nur auf die Daten Zugriff hat, für die er oder sie berechtigt ist. Dies erfordert, dass Daten klassifiziert sind und der Zugriff geregelt ist. Mit der Lösung Data Fabric und watson.x unseres Partners IBM wird über eine Klassifizierung sichergestellt, dass nur diejenigen Nutzer:innen auf Daten zugreifen dürfen, die dazu berechtigt sind. Des Weiteren kann es bei personenbezogenen Daten auch notwendig sein, bestimmte Teile der Daten zur weiteren Verwendung zu maskieren.

REGELUNG DES DATENZUGRIFFS AM BEISPIEL EINER RETRIEVAL AUGMENTED GENERATION (RAG)-ARCHITEKTUR

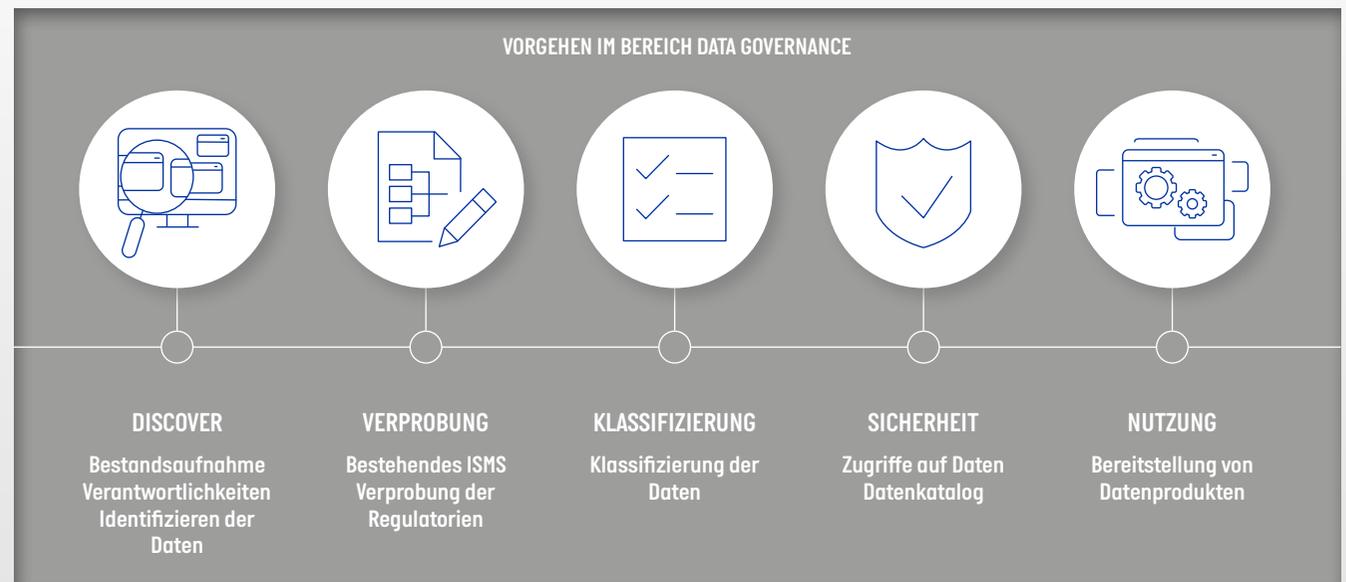




Darüber hinaus halten wir die Datenaufbereitung und -verwendung nachvollziehbar fest. Ein Datenkatalog kann helfen, die Datenbestände zu dokumentieren sowie die Herkunft und die Nutzung der Daten zu verfolgen. So wird sichergestellt, dass die Daten für zukünftige Zwecke leicht zugänglich sind. Dies schafft die Voraussetzung, den Wert der Daten auszuschöpfen und dabei nachvollziehbare, verlässliche Daten für das Training einer KI bereitzustellen. Hat man die Daten einmal aufbereitet und für die KI-Anwendung vorbereitet, ist es möglich, diese Daten auch für andere Use Cases wiederzuverwenden. Durch die Bereitstellung solcher Datenprodukte wird die Effizienz erhöht und die Auffindbarkeit der Daten innerhalb des Unternehmens verbessert. Ein einmal erstelltes Datenprodukt kann allen Mitarbeitenden im Unternehmen zugänglich gemacht werden.

BENEFITS

Durch die Integration von Data Governance in das bestehende ISMS gewährleisten wir, dass das Management jederzeit in der Lage ist, einen Überblick über die Daten zu haben, die den KI-Workflows zugrunde liegen. Dies minimiert einerseits das Risiko rechtlicher Konsequenzen und schützt Ihre Unternehmensreputation. Andererseits führt der sichere, effiziente und effektive Einsatz von Daten zu einem nachhaltigen Wettbewerbsvorteil. So können unsere Kunden ihre Geschäftsziele besser verfolgen.



AI GOVERNANCE: EINE RUNDUM VERTRAUENSWÜRDIGE UND SICHERE KI

Stimmt die Data Governance, muss im nächsten Schritt dafür gesorgt werden, dass die KI auch vorschriftsgemäß, sicher und verantwortungsvoll genutzt wird – und dies gewissenhaft geprüft wird. KI-Technologie soll die Effizienz und Effektivität der Organisation steigern. Ohne eine systematische AI Governance bleibt das Potenzial von KI jedoch ungenutzt – schlimmer noch, es gibt hohe Risiken. Deshalb ist es entscheidend, AI Governance von Beginn an im gesamten Lebenszyklus der Lösung zu berücksichtigen.

Es ist notwendig, die Qualitätsanforderungen an KI-Systeme klar zu definieren und umzusetzen. Diese Anforderungen erstrecken sich über den gesamten Lebenszyklus der KI, beginnend bei der Einstufung von KI in Bezug auf den EU AI Act und dem Training mit den erforderlichen Datensätzen bis hin zum Einsatz und dem Monitoring geeigneter KPIs.

Organisationen müssen ihre KI vor dem Hintergrund der folgenden Überlegungen kontinuierlich managen.



REGULATIVE ANFORDERUNGEN

- Einstufung nach EU AI Act
- Datenschutz [Bundesdatenschutzgesetz oder DSGVO]

RISIKOMANAGEMENT

- AI-Drift
- BIAS
- Ethik
- Monitoring

AI GOVERNANCE: UNSER SERVICE

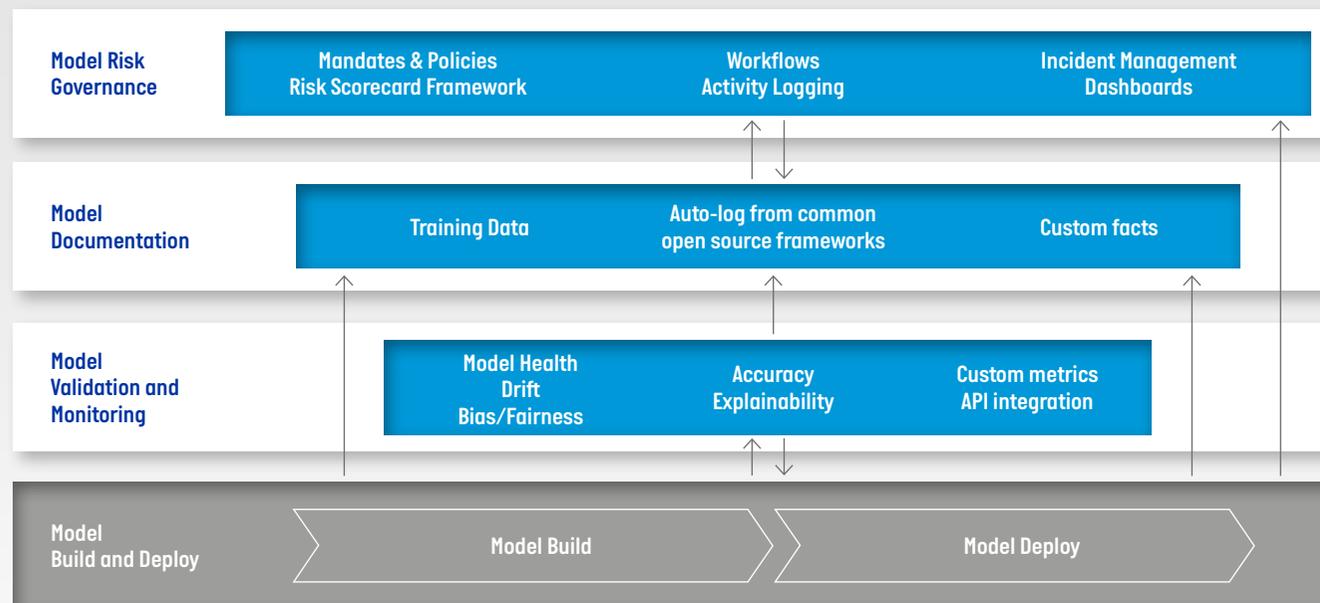
Computacenter bietet eine umfassende Lösung zur Integration von AI Governance in das bestehende ISMS. Wir stellen sicher, dass die KI-Systeme den regulatorischen Anforderungen entsprechen und kontinuierlich überwacht werden.

Die internationale Norm ISO/IEC 42001 spielt dabei eine zentrale Rolle. Sie stellt sicher, dass alle relevanten Aspekte bei der AI Governance berücksichtigt werden. Mit einer strukturierten Herangehensweise ermöglicht sie es, KI-Systeme über ihren gesamten Lebenszyklus hinweg zu managen und ihr Potenzial optimal auszuschöpfen. Um die AI Governance auf den Weg zu bringen, setzen wir gemeinsam mit den Verantwortlichen in der Organisation ein Projekt auf, das die AI Governance mit dem internen ISMS verknüpft. Auf Grundlage der so gewonnenen Konzepte soll eine möglichst hohe Automatisierung aufgebaut werden, um Workflows zur Governance, Dokumentation der Modelle und zum Monitoring der KI-Systeme zu erzielen.

UNSER VORGEHEN

Dafür implementieren wir Lösungen wie watsonx.governance unseres Partners IBM, um die Steuerung, Verwaltung und Überwachung von KI vollumfänglich umzusetzen. Eine Vielzahl von skalierbaren Governance-, Risiko- und Compliance-Funktionen berücksichtigt zudem gezielt die Anforderungen des EU AI Act. Die Lösung vereinfacht die Dokumentation, Bewertung und Überwachung von KI-Tools und ihren Modellen über den gesamten Lebenszyklus hinweg.

AUTOMATISIERUNG ÜBER IBM WATSONX.GOVERNANCE



Mit Tools wie diesem setzt Computacenter AI Governance während des gesamten Lebenszyklus der KI auf drei Ebenen um:

- **Model Risk Governance:** Auf dieser Ebene wird der KI Use Case entwickelt und es werden Leitplanken gesetzt, gegen die dieser evaluiert werden kann. Hier stehen entsprechende Workflows, Dashboards und Risikoanalysen für das Management bereit, die manuell eingegeben werden.
- **Model Documentation:** Auf dieser Dokumentationsebene lassen sich unter anderem Autologgings durchführen oder große Datenmengen automatisch speichern. Dazu gehören beispielsweise Trainingsdaten oder Daten, mit denen die KI verbessert wird. Verlangt eine Regulierungsbehörde Einsicht, um den EU AI Act entsprechend durchzusetzen, stehen diese Aufzeichnungen bzw. automatisierten Berichte zur Verfügung.

- **Model Validation and Monitoring:** Auf dieser Ebene geht es um das Monitoring der KI im laufenden Betrieb – Prompts, Antworten und Kontexte in der Kommunikation zwischen Nutzer:innen und der KI – sowie ihre Performance. Dies ist aus technischer Sicht besonders spannend, denn hier wird deutlich, ob die Daten qualitativ hochwertig sind und die Data Governance funktioniert. Das Monitoring Tool lässt sich an die KI anschließen, woraufhin über entsprechende Schnittstellen (APIs) Anforderungen zur Überwachung gestellt werden. Zeigt das Monitoring Auffälligkeiten, sind Remediationsmaßnahmen wie zum Beispiel ein weiteres Fine Tuning zu initiieren.

BENEFITS

Durch die Integration automatisierter AI Governance in das bestehende ISMS stellen wir sicher, dass das Management jederzeit in der Lage ist, die KI vollumfänglich zu steuern. Durch kontinuierliches Monitoring und die Erhebung von KPIs werden Risiken durch eine unerwünschte Drift oder kritische Parameter frühzeitig erkannt und behoben. Dies gewährleistet die langfristige Stabilität und Sicherheit der KI-Systeme, minimiert das Risiko rechtlicher Konsequenzen und schützt die Unternehmensreputation. Regelmäßige Audits und Fragebögen bieten zusätzliche Sicherheit und helfen dabei, potenzielle Risiken frühzeitig zu identifizieren und zu adressieren. Umfassende Dokumentation ermöglicht eine Auditierung des Betriebs.



WARUM COMPUTACENTER?

Computacenter verfügt über umfangreiche Erfahrung und Expertise im Bereich ISMS, Integration verschiedener Security-Lösungen und Data Governance. Durch moderne Technologien und bewährte Methoden bieten wir Ihnen eine maßgeschneiderte Lösung, die auf Ihre spezifischen Anforderungen zugeschnitten ist.

Wir unterstützen Sie dabei, KI-Technologien verantwortungsvoll und erfolgreich zu implementieren und zu nutzen. Wir setzen ein Projekt auf, mit dem wir Sie durch den Dschungel an Regularien und Vorgaben lotsen, Rollen definieren sowie Leitplanken und Policies festlegen. Unser engagiertes Team aus Sicherheitsexpert:innen arbeitet eng mit Ihnen zusammen, um sicherzustellen, dass Ihre KI-Systeme sicher und konform betrieben werden. Erfordert Ihr KI-Anwendungsszenario eine spezielle Expertise, greifen wir zur Unterstützung auf unser Netzwerk professioneller Servicepartner zurück.

Ihre Ansprechpartner für Data & AI Governance:

Ralf Becker

Solution Manager Data & AI Platforms
Fon +49 1728356339
ralf.becker@computacenter.com

Ralf Nemeyer

Solution Manager IT GRC [Governance, Risk, Compliance]
Fon +49 173 8929293
ralf.nemeyer@computacenter.com

Unternehmensprofil

Computacenter ist ein führender, unabhängiger Technologie- und Servicedienstleister, dem große Unternehmen und öffentliche Auftraggeber vertrauen. Wir helfen unseren Kunden bei der Beschaffung, der Weiterentwicklung und dem Betrieb ihrer IT-Infrastruktur, um eine digitale Transformation zu ermöglichen, die Anwender und deren Geschäft erfolgreich macht.

Computacenter ist ein an der Londoner Börse notiertes Unternehmen und beschäftigt über 20.000 Mitarbeitende weltweit.



Computacenter AG & Co. oHG
Computacenter Park 1, 50170 Kerpen

computacenter.de
+49 (0)2273 5970