IDW KNOWLEDGE PAPER

DATAGOVERNANCE

DIE BEDEUTUNG EINER GUTEN GOVERNANCE FÜR DEN UMGANG MIT DATEN IM UNTERNEHMEN

STAND 16.03.2022

IDW
INSTITUT DER WIRTSCHAFTSPRÜFER

INHALT

Management Summary 3

Vorbemerkung 4

1. Bedeutung von Data Governance 6

2. Einordnung des Begriffs der Data Governance 8
- 2.1. Definition, Ein- und Abgrenzung 8
- 2.2. Verständnis als Management System 9
- 2.3. Anknüpfung an bestehende Management Systeme / Ordnungsrahmen 11

3. Vorschläge zum Aufbau von Data Governance-Strukturen 12
- 3.1. Mögliche Vorgehensweise zum Aufbau von Data Governance-Strukturen 12
- 3.2. Teil I – Anforderungsebene 13
- 3.3. Teil II – Organisatorische Ebene 15
  - 3.3.1. Strategischer Gestaltungsrahmen / Unternehmensstrategie und Einordnung des Wertbeitrages von Daten für das eigene Geschäftsmodell 15
  - 3.3.2. Aufbauorganisation 16
- 3.4. Teil III – Operative Ebene 18
  - 3.4.1. Metadaten und Klassifizierung 18
  - 3.4.2. Richtlinien 19
  - 3.4.3. Technologische Unterstützung / Automatisierbarkeit und Werkzeugeinsatz 20

4. Beratung und Prüfung im Kontext Data Governance 23

5. Fazit und Ausblick 24

Fußnoten 26

MANAGEMENT SUMMARY

Die zunehmende Bedeutung von Daten und die für Unternehmen daraus resultierenden Chancen und Risiken zeigen die Wichtigkeit, sich mit dem ganzheitlichen und strategischen Management der Lebenszyklen von Daten (Data Governance) zu befassen. Die erfolgreiche Umsetzung aktueller Digitalisierungsvorhaben, die Entwicklung neuer datenbasierter Geschäftsmodelle oder der Einsatz von Technologien wie Machine Learning und Künstliche Intelligenz sind ohne die strukturierte und strategische Nutzung von Daten unvorstellbar. Gleichzeitig bergen diese neuen Vorhaben und Technologien auch Risiken, insbesondere im Hinblick auf Datensicherheit und -schutz.

Für die Einführung eines Data Governance Management Systems bzw. die Fortentwicklung bestehender Strukturen lässt sich auf bewährte Ansätze und Ordnungsrahmen aus anderen Bereichen der Governance zurückgreifen, die um die Fragestellung des sicheren und vertrauensvollen Umgangs mit Daten erweitert werden können. Anknüpfungspunkte bieten bspw. die *IDW Prüfungsstandards: „Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen“ (IDW PS 980)* bzw. *„Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen“ (IDW PS 981)*. Eine gute Orientierung stellen zudem Rahmenwerke wie COBIT oder ITIL dar.

Bei der Einrichtung von Data Governance Strukturen empfiehlt sich ein projekthaftes Vorgehen. Zunächst sind alle relevanten Stakeholder und regulatorische wie unternehmensinterne Ansprüche an die Data Governance-Organisation zu identifizieren und durch Data Governance-Strukturen zu adressieren (Anforderungsebene). Auf der organisatorischen Ebene ist die Einbindung von Data Governance in die Unternehmensstrategie zu gewährleisten und durch die Zuordnung von Rollen und Verantwortlichkeiten angemessen zu unterstützen. Die ge-

schaffenen Strukturen gilt es auf der operativen Ebene erfolgreich anzuwenden und in die Geschäftsabläufe zu integrieren. Von zentraler Bedeutung sind hier die Datenklassifizierung, die Definition, Kommunikation, Einhaltung und Überwachung geeigneter Richtlinien zur Generierung, Verarbeitung bis hin zur Vernichtung von Daten sowie eine angemessene technische Unterstützung von Data Governance.

Aus der Sicht der Wirtschaftsprüfer*innen ist der vertrauensvolle Umgang mit Daten ein zentrales Element der Governance in Unternehmen. Der Berufsstand kann das Vertrauen der Öffentlichkeit und anderer relevanter Stakeholder in den regelkonformen Umgang mit Daten in Unternehmen in Form von Beratungs- und Prüfungsleistungen außerhalb von Abschlussprüfungen stärken.

VORBEMERKUNG

Das Thema Daten und der Umgang mit ihnen gewinnen einen immer höheren Stellenwert in der Öffentlichkeit und in Unternehmen. Vor dem Hintergrund der fortschreitenden Digitalen Transformation ist es für viele Unternehmen unerlässlich, Daten auszuwerten und nutzbar zu machen, um selbst wettbewerbsfähig zu bleiben. Daten dienen hierbei sowohl als Basis für Prozessverbesserungen als auch als Grundlage neuer Geschäftsmodelle. Daneben nehmen auch die Möglichkeiten zur Erhebung, Speicherung und Verarbeitung von Daten und großen Datenmengen massiv zu.

Wurden im Jahre 2018 weltweit noch 33 Zettabyte[1] an Daten generiert, so prognostizieren verschiedene Studien und Publikation für das Jahr 2025 ein Datenaufkommen von mehr als 180 Zettabyte[2] (vgl. Abb. 1).

Die Datenwirtschaft ist ein Thema mit großem Wertschöpfungspotenzial. Anwendungen aus den Bereichen Big Data, Künstliche Intelligenz (KI) oder Internet of Things (IoT) bieten Unternehmen und Nutzern das Potenzial, bestehende Prozesse und Systeme disruptiv zu verändern. Daneben entstehen komplett neue Wertschöpfungsmodelle und Märkte, welche sich exklusiv mit der Erhebung, Analyse, Bereitstellung oder der Monetarisierung von Daten befassen.

Die Nutzung von sehr großen Datenmengen erfolgt bereits in vielen Bereichen, z.B. bei den Produktempfehlungssystemen der Online-Shops, sensorbasierten Smart Watches mit der Möglichkeit der Analyse des Schlafrhythmus oder Predictive Analytics zu Wartungsintervallen und Ausfallrisiken bei Maschinen im Produktionsprozess. Insbesondere für Anwendungen von KI und Machine Learning ist es unerlässlich, auf große Datenmengen für das Anlernen und Verbessern der Modelle zugreifen zu können. Das IoT wird mit der Verbreitung von bspw. 5G zu einem weiteren Anstieg von erhobenen Daten führen, von denen viele auch unter datenschutzrechtliche Kriterien fallen.

Ein erwartetes jährliches Wachstum der Datenmengen von mehr als 27%[3] und der bereits erhebliche Anteil der Datenwirtschaft am BIP (2,4% in der EU im Jahr 2018 mit einem erwarteten Anstieg auf 5,8% im Jahr 2025)[4], welcher auf die monetäre Nutzung von Daten zurückzuführen ist, zeigen Einfluss und Potenzial der Nutzung von Daten heute und für die kommenden Jahre.

Daraus ergeben sich steigende Anforderungen an den Umgang mit Daten und die Erkenntnis, dass Daten ein selbstständiges und wichtiges Gut sind, das entsprechende Beachtung erfordert. Dies unterstreicht die Wichtigkeit von Data Governance.

Das IDW Knowledge Paper „Data Governance“ hat zum Ziel, die Bedeutung eines Data Governance Management Systems (DGMS) für Unternehmen, insbesondere aus dem Mittelstand, darzustellen und Hilfestellung zur Einführung oder zur zielgerechten Erweiterung bestehender Strukturen zu geben. Öffentlichkeit und relevante Stakeholder haben ein Interesse, dass Unternehmen mit Daten vertrauensvoll umgehen. Aus der Sicht von Wirtschaftsprüfer*innen ist der vertrauensvolle Umgang mit Daten ein zentrales Element der Governance in Unternehmen. Mit diesem Papier möchte das IDW einen Beitrag zur notwendigen, laufenden Debatte über den vertrauensvollen Umgang mit Daten leisten. Es richtet sich daher auch an die interessierte Öffentlichkeit, vor allem an Unternehmensleitung, Aufsichtsorgane und Politik. Welchen Beitrag der Berufstand zur Stärkung dieses Vertrauens in Form von Beratungs- und Prüfungsleistungen bieten kann, stellt dieses Knowledge Paper am Ende dar.

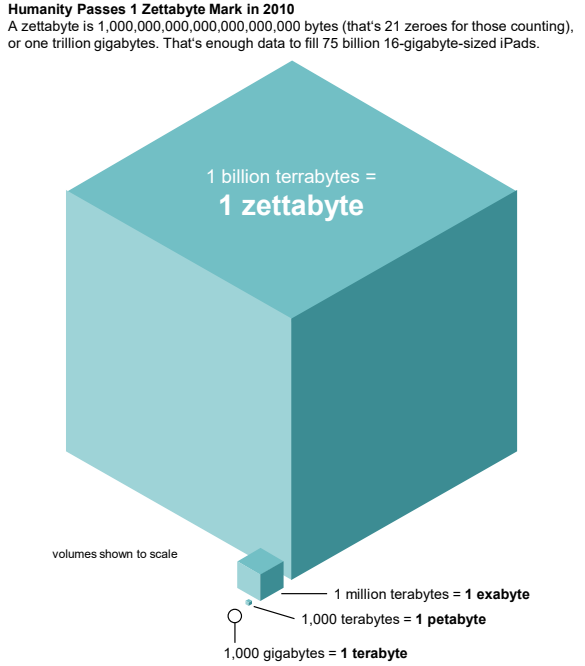


Abb. 1: Vergleich zwischen einem Zettabyte und einem Terabyte, Quelle: TechNewsDaily, Karl Tate; vgl.: https://twitter.com/schmarzo/status/1075863920517115904

1. BEDEUTUNG VON DATA GOVERNANCE

Mit steigenden Datenmengen wachsen zugleich die Risiken aus deren Nutzung. In den vergangenen Jahren häufen sich Berichte über Datenmissbrauch oder den unsachgemäßen Umgang mit Daten. Neben Skandalen wie die Geschehnisse um Cambridge Analytica, die in der öffentlichen Wahrnehmung Fragen zum verantwortungsvollen Umgang mit Daten aufwerfen, steigen auch Cyber-Risiken, wie der Diebstahl von Daten oder Ransomware-Attacken, die den Betrieb von Unternehmen oder Behörden gefährden. Nicht selten sind diese Fälle auf Schwächen in Data Governance-Strukturen zurückzuführen. Solche Berichte haben darüber hinaus die Themen Datennutzung, Datenweitergabe und vor allem Datenschutz in den Fokus gerückt.

Daneben bestehen rechtliche Risiken im Umgang mit Daten, wie z.B. die Einhaltung der Datenschutzgrundverordnung (DSGVO), die für die Aufsichtsgremien und die Unternehmensleitung als verantwortliche Organe von Belang sind. Neben übergreifenden rechtlichen Anforderungen gibt es zahlreiche branchenspezifische Regularien, wie bspw. im Finanzsektor oder der Telekommunikationsbranche.

Somit treibt nicht nur die Anforderung an Datenqualität die Wichtigkeit einer ganzheitlichen Data Governance, sondern auch Anforderungen aus Datensicherheit und Datenschutz, sowie gestiegene Compliance Anforderungen machen eine Data Governance unerlässlich.

Trotz der Risiken einer unzureichenden Implementierung von Data Governance stellen die Offenlegung und somit die vielfältige Nutzung von Daten eine strategische Notwendigkeit dar (siehe auch Open-Data-Initiative der EU). Der Grund besteht im erzielbaren gesamtgesellschaftlichen Nutzen. Zusätzliche Daten erlauben immer mehr und detailreichere Einblicke, die zu einem multiplikativen Effekt beim Erkenntnis- und dem daraus resultierenden Effizienzgewinn führen.

Ein institutioneller Hinweis auf die Notwendigkeit einer Data Governance ist der Data Governance Act der Europäischen Kommission. Der Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Data Governance stellt eine der ersten Maßnahmen vor, die in der 2020 veröffentlichten europäischen Datenstrategie[5] angekündigt wurden. Diese Maßnahme zielt auf den vermehrten Austausch von Daten zur gemeinsamen Nutzung ab, im privaten wie im öffentlichen Sektor.

Die zahlreichen Themen, Risiken, nationalen Regularien, ethischen Fragestellungen, aber auch Potenziale sowie die Vielfältigkeit der beteiligten und betroffenen Stakeholder zeigen auch, dass dieses komplexe Thema nicht von verschiedenen Fachabteilungen separat und individuell bearbeitet werden sollte. Eine Institutionalisierung und ganzheitliche Betrachtung im Rahmen einer Data Governance wird für Unternehmen zu einer Notwendigkeit. Diese umfasst die Einführung bzw. Weiterentwicklung von Strukturen und Prozessen für einen verantwortungsbewussten Umgang mit Daten.

Vorteile eines effektiven Data Managements für Unternehmen:

- Einhaltung der geltenden Compliance-Vorgaben
- Schutz wesentlicher Informationen
- Sicherstellung des Datenschutzes
- optimale Unterstützung der Unternehmensprozesse
- Erschließung neuer Geschäftspotenziale
- effizientere Verwaltung großer Datenmengen
- optimierter Zugriff auf Informationen

Unternehmen stehen vor der Herausforderung, dass von unterschiedlichen Stakeholdern (Kunden, Mitarbeiter, Lieferanten, Investoren, Öffentlichkeit etc.) unterschiedliche Anforderungen an Daten, Datenqualität und Datenhaltung gestellt werden. Diese Anforderungen umfassen u.a.:

- Zweckbindung von Daten
- Nachvollziehbarkeit der Datenverarbeitung
- Datensicherheit, Datenschutz
- Mehrwertschaffung durch Daten (Kunde möchte das beste Angebot „Google-Ad“-Prinzip)
- Prozesssicherheit (Datenqualität, Datenaktualität)
- Transparenz (Reportingfunktionen, Auswertbarkeit)
- Rechtliche Anforderungen, bspw. Aufbewahrungsfristen

Entsprechend ist eine Data Governance entlang der gesamten Wertschöpfungskette inklusive des Datenökosystems von Bedeutung, um den Interessen aller Stakeholder gerecht zu werden. Unter anderem aus diesem Grund muss Data Governance Teil der unternehmensweiten Governance-Strategie sein.

Zur Umsetzung der Data Governance sollte ein einheitliches und klares Verständnis des Begriffes Daten in einem Unternehmen etabliert sein. Nur so kann der Datenfluss und die Datenverarbeitung innerhalb eines Unternehmens vollständig nachvollzogen und die Grundlage für Data Governance geschaffen werden.

Es ist notwendig, neben digital vorliegenden Daten auch nicht digital vorliegende Daten zu berücksichtigen. Daten können sowohl bereits systematisiert als auch unstrukturiert sein. Um aussagekräftige Kennzahlen und Analysen zu ermöglichen, sollten alle dafür verwendeten Daten mit einem geeigneten "tag“ versehen werden.

2. EINORDNUNG DES BEGRIFFS DER DATA GOVERNANCE

Zur weiteren Begriffsbestimmung bietet der folgende Abschnitt Informationen zur Definition, Ein- und Abgrenzung des Begriffs Data Governance und illustriert das eng damit verbundene Verständnis als Management System. Zusätzlich werden Anknüpfungspunkte zu bereits bestehenden Management Systemen/Ordnungsrahmen aufgezeigt.

2.1. Definition, Ein- und Abgrenzung

Aufgrund der fortschreitenden Digitalisierung von Geschäftsprozessen haben sich Unternehmen bereits oftmals mit dem Umgang mit Daten beschäftigt. Dementsprechend bedarf es einer Abgrenzung des Begriffs der Data Governance von anderen Begriffen, deren Ziele und Schwerpunkte zwar Anknüpfungsmöglichkeiten bieten, jedoch davon zu unterscheiden sind. Trotz der steigenden Bedeutung von Daten und dem sich daraus ergebenden Bedarf einer gezielten, systemübergreifenden Steuerung für den erfolgreichen und rechtlich zulässigen Einsatz von Daten existiert bislang keine klare und einheitliche Definition des Begriffs Data Governance.

In Anlehnung an die Definition der deutschen Organisation DEMAND (Data Economics and Management of Data Driven Business)[6] wird für den Zweck dieses Knowledge Papers unter dem Begriff **Data Governance** ein Rahmenwerk zur strategischen und übergeordneten Steuerung der Datenlebenszyklen verstanden. Die Strategie, Ziele und Richtlinien für den Umgang mit Unternehmensdaten stehen dabei im Mittelpunkt. Hinzu kommen die Orchestrierung der Teilprozesse von Datenlebenszyklen (d.h. von der Datenakquisition bzw. -generierung über die Analyse, Speicherung, Bereitstellung, Nutzung bis hin zur Löschung von Daten) sowie die klare Definition von Rollen und Verantwortlichkeiten.

Die Bezeichnung **Data Management** wird allgemein für die Verwaltung von Informationen, die von Unternehmen genutzt oder generiert werden, verwendet. Dieser Begriff wird häufig für Tätigkeiten im Umfeld der Nutzung von Daten in einzelnen Systemen genutzt, bspw. im Kontext des sog. „Stammdatenmanagements". Data Governance bildet für diesen Teil des Themenkomplexes den organisatorischen Rahmen und behandelt den Aspekt der strategischen und übergreifenden Steuerung von Aktivitäten in Zusammenhang mit der effektiven und zulässigen Nutzung von Daten.

Unter dem häufig genutzten Sammelbegriff **Datenschutz** wird die Einhaltung von Gesetzen zum Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung ihrer Daten wie bspw. der DSGVO verstanden. Hierbei handelt es sich um einen Katalog aus rechtlichen Anforderungen, die an die Verarbeitung von sogenannten „personenbezogene Daten" gestellt werden und deren Nichteinhaltung bußgeldbewehrt ist. Bei „personenbezogenen Daten" handelt es sich im Sinne der DSGVO um „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen"[7]. Im Rahmen von Data Governance werden im Gegensatz dazu alle Daten betrachtet, die von Unternehmen generiert oder genutzt werden, unabhängig davon, ob diese Personenbezug aufweisen oder nicht.

2.2. Verständnis als Management System

Unter einem Management System werden die auf der Grundlage der von der Unternehmensleitung vorgegebenen Ziele eingeführten Grundsätze und Maßnahmen eines Unternehmens verstanden, die auf die Erreichung eines konkreten Ziels (z.B. die Sicherstellung eines regelkonformen Verhaltens bei Compliance Management Systemen) gerichtet sind[8].

Ein Management System im Sinne des *IDW Prüfungsstandards: „Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen" (IDW PS 980)*, welches man auf den Themenkomplex Data Governance überträgt, zeichnet sich durch die Berücksichtigung der folgenden Grundelemente aus:

1. Grundsätzlich haben alle Führungsebenen eine Kultur der ganzheitlichen und strategischen Nutzung von Daten zu schaffen und zu fördern.

2. Unter Berücksichtigung der strategischen Ausrichtung des Unternehmens sind eindeutige und messbare Ziele für die Datennutzung festzulegen.

3. Auf der Basis dieser Ziele sind auch Risiken für den ganzheitlichen und strategischen Umgang mit Daten fortlaufend in einem geordneten Verfahren zu identifizieren.

4. Das Programm enthält angemessene Maßnahmen, um Risiken zu vermeiden und die Ziele der Data Governance Organisation zu erreichen.

5. Im Rahmen der Organisation werden Rollen und Verantwortlichkeiten sowie Aufbau- und Ablauforganisation in einem angemessenen Ausmaß festgelegt.

6. Durch geeignete Verfahren zur Überwachung und Verbesserung werden fortlaufend Angemessenheit und Wirksamkeit aller Strukturen und Maßnahmen überprüft.

7. Durch fortlaufende Kommunikation werden Mitarbeiter wie ggf. Dritte über Vorgaben sowie deren Rollen und Verantwortlichkeiten informiert, so dass diese in der Lage sind, die ihnen zugewiesen Aufgaben bestmöglich zu erfüllen.

Die Grafik fasst die wesentlichen Elemente zusammen:

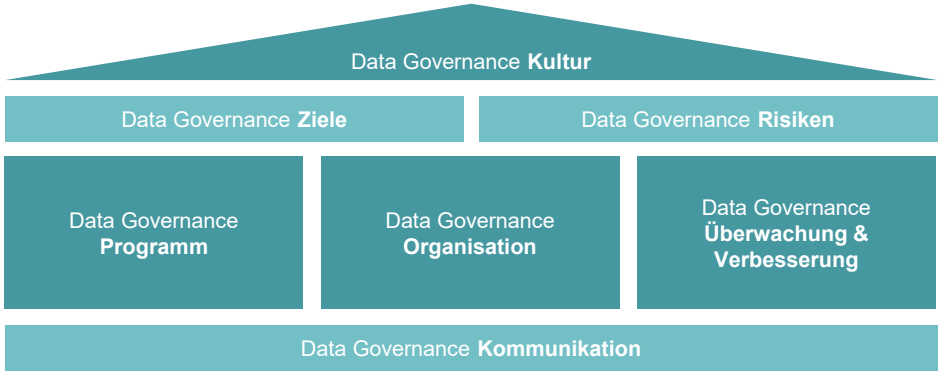


Abb. 2: Die Grundelemente einer Data Governance

Vor allem mittelständische Unternehmen können von der Einrichtung eines Management Systems für Data Governance profitieren. Der Aufbau entsprechender Strukturen kann die Erschließung neuer Geschäftsfelder beschleunigen und unterstützt Digitalisierungsprojekte für eine zukunftsfähige Aufstellung.

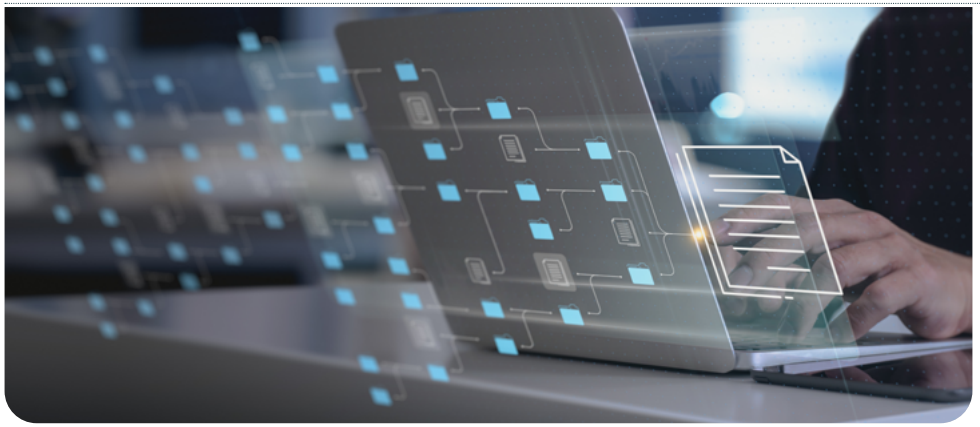
2.3. Anknüpfung an bestehende Management Systeme / Ordnungsrahmen

Unter Berücksichtigung der Definition und der inhaltlichen Schwerpunkte von Data Governance ergeben sich vielfältige Anknüpfungspunkte zu bereits bestehenden Management Systemen oder anderen Ordnungsrahmen. Daher kann es für Unternehmen, die sich erstmalig mit den Anforderungen an einen ganzheitlichen und strategischen Umgang mit Daten befassen, sinnvoll sein, auf anderweitig verfügbare Erfahrungswerte zurückzugreifen.

Ein im Unternehmen bereits eingerichtetes Compliance Management System nach *IDW PS 980* oder ein Risikomanagementsystem nach *IDW Prüfungsstandard: „Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen" (IDW PS 981)* beschreibt bspw. Anforderungen an die zugrundeliegenden Grundelemente (siehe Abschn. 3.2.). Beim Aufbau eines entsprechenden Management Systems zu Data Governance können Unternehmen von Erfahrungen aus der Implementierung der Grundelemente aus den zuvor genannten Management Systemen profitieren bzw. diese sogar integrieren.

Eine gute Orientierung stellen Rahmenwerke wie COBIT[9] oder ITIL[10] dar. Zwar handelt es sich dabei um IT-Governance-Standards, welche sich auf den Bereich Data Governance nicht 1:1 übersetzen lassen. Dennoch stellt eine Orientierung an den Schlüsselprinzipien der Frameworks eine wertvolle Basis dar.

Weiterhin relevant ist der Themenkomplex der Informationssicherheit. Als gängigste Zertifizierung dazu findet häufig die ISO/IEC 27000er-Reihe Anwendung. Diese Standards bieten Unternehmen einen Rahmen zur Absicherung von Informationssicherheits-Risiken durch entsprechende Kontrollen.



3. VORSCHLÄGE ZUM AUFBAU VON DATA GOVERNANCE-STRUKTUREN

Dieses Kapitel gibt zunächst einen Überblick über prozessuale Vorgehensweisen zur Einführung einer Data Governance. Ein besonderer Fokus wird dabei auf die Erhebung der Anforderungen gelegt. In den folgenden beiden Abschnitten werden die Dimensionen Aufbauorganisation und Umsetzung thematisiert.

3.1. Mögliche Vorgehensweise zum Aufbau von Data Governance-Strukturen

Aufgrund der Notwendigkeit, Data Governance unternehmensweit zu denken, erfordert der Aufbau von entsprechenden Strukturen das Zusammenspiel unterschiedlicher Fachbereiche und Führungskräfte. Um der Herausforderung in einem angemessenen Ausmaß und Zeitrahmen gerecht zu werden, empfiehlt sich ein projekthaftes Vorgehen bei der Einrichtung.

Zunächst ist es wichtig, alle relevanten Stakeholder zu ermitteln. Neben internen Bereichen können dies auch Ansprechpartner außerhalb des Unternehmens, wie Kunden oder Geschäftspartner, sein. Unter Einbezug dieser Stakeholder sind zunächst die strategische Bedeutung und der Umfang der Nutzung von Daten zu identifizieren bzw. zu ergänzen. Dies stellt die Grundlage dar für die Erhebung der Anforderungen, die durch das Data Governance System adressiert werden sollen.

Im Anschluss wird mit der Definition eines Zielbildes eine eindeutige Vorstellung für die zukünftige Data Governance-Organisation erarbeitet. Zusammen mit den als kritisch eingestuften Stakeholdern werden die zukünftigen Strukturen in Form eines Soll-Zustands entwickelt und abgestimmt. Dabei erfolgt stets ein Abgleich mit den strategischen Zielen des Unternehmens, um die Vereinbarkeit der zukünftigen Organisation im Gesamtkontext der Wertschöpfungsprozesse zu gewährleisten.

Dieser Handlungsbedarf wird bei einer Maßnahmenplanung aufgearbeitet und in konkrete Aufgaben übersetzt. Unter Berücksichtigung der im Unternehmen verfügbaren Ressourcen und Kompetenzen werden die Aufgaben in Umsetzungsschritte unterteilt und jeweils einem Verantwortlichen zugewiesen.

Diese Aufgaben werden anschließend während der Umsetzung bearbeitet. Dabei kann es sowohl zur Implementierung neuer Strukturen oder Prozesse sowie zu möglichen Restrukturierungen kommen.

Auch agile Projektmanagementmethoden wie bspw. SCRUM[11] eignen sich zur Umsetzung.

Zugleich bietet eine systematische Data Governance die Möglichkeit, Synergien vorhandener Prozesse zu heben und Doppelstrukturen zu vermeiden.

3.2. Teil I – Anforderungsebene

Zunächst sind im Kontext der sogenannten „Anforderungsebene“ (Teil I) regulatorische wie interne Ansprüche aus dem eigenen Risikomanagement an die Data Governance-Organisation zu identifizieren.

Dabei handelt es sich sowohl um extrinsisch motivierte Anforderungen, die bei der regulatorischen Compliance auf das Unternehmen einwirken als auch um unternehmensinterne Interessen, die zumeist aus dem Risikomanagement resultieren. Beide Aspekte sind durch angemessene Data Governance-Strukturen zu adressieren.

Das wachsende gesellschaftliche und politische Bewusstsein für die Bedeutung der Datennutzung bringt es mit sich, dass Unternehmen fortlaufend mit neuen, rechtlichen Anforderungen konfrontiert werden. Auch wenn die Anzahl an gesetzlichen Regelungen in manchen Branchen und Industrien bereits vermeintlich hoch ist, so entstehen mit der fortschreitenden Digitalisierung fortlaufend neue Szenarien, die der Gesetzgeber wahrscheinlich adressieren wird.

Beispiel:

Als Beispiel kann hier aktuell der Entwurf zum „EU AI Act“ vom 21. April 2021 genannt werden, aus dem sich schon bald konkrete Anforderungen z.B. hinsichtlich das Umgangs mit Daten zum Trainieren von KI-Systemen ergeben, die zudem auch die Fragestellung des Umgangs mit von externen Dritten bezogenen Daten mit einschließen könnte

Zusätzlich lässt sich beobachten, dass gerichtliche Entscheidungen dazu führen, dass Vorgaben anders angewendet oder gar neu interpretiert werden müssen, um rechtskonform zu handeln.

Um die zielgerichtete und strategische Nutzung von Daten im Sinne einer erfolgreichen Data Governance bestmöglich zu steuern, ist daher eine kontinuierliche Überwachung notwendig, um zeitnah auf neue Anforderungen angemessen reagieren zu können.

Die Vorgaben, die unter dem Begriff regulatorische Compliance zusammengefasst werden können, sind vielfältig, wie die folgenden Beispiele aufzeigen:

- Die DSGVO schützt alle personenbezogenen Daten. Unternehmen müssen viele gesetzliche Anforderungen erfüllen, bspw. das Führen eines „Verzeichnisses für Verarbeitungstätigkeiten”. Darin muss eine umfangreiche Dokumentation zu allen Prozessen vorgehalten werden, im Rahmen derer personenbezogene Daten, z.B. von Kunden oder Mitarbeitern, verarbeitet werden. Die Nichteinhaltung der Anforderungen ist mit hohen Bußgeldern bewehrt.

- Seit dem Inkrafttreten des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) am 26. April 2019 stehen viele Unternehmen vor der Herausforderung, dass das Know-how nicht mehr per se geschützt wird, sondern lediglich in den Fällen, in denen die Unternehmen aktiv angemessene Geheimhaltungsmaßnahmen ergreifen. Dies erfordert eine Identifikation und Klassifizierung der schützenswerten Informationen über alle Fachbereiche hinweg. Die daraus gewonnenen Erkenntnisse über erforderliche Schutzmaßnahmen müssen zusammengefasst und dokumentiert werden, um sich im Falle eines Rechtsstreits auf deren Status als Geschäftsgeheimnis berufen zu können.

- Zudem gibt es zahlreiche industrie- oder produkt- bzw. dienstleistungsspezifische regulatorische Anforderungen, wie bspw. das Telekommunikationsgesetz (TKG) für Unternehmen, die Telekommunikationsdienstleistungen anbieten, oder zur Sicherheit der Informationstechnik von Betreibern sogenannter kritischer Infrastrukturen (sog. „KRITIS”). Diese haben zusätzlich oftmals großen Einfluss auf den rechtlich zulässigen Umgang mit Daten und müssen unter Androhung von Bußgeldern oder gar persönlicher Haftung von den Unternehmen eingehalten werden.

Neben Anforderungen, die von außen an die Organisation herangetragen werden, entstehen auch innerhalb des Unternehmens neue Herausforderungen. Dank der wachsenden Bedeutung für den Unternehmenserfolg und einer kontinuierlich steigenden Anzahl an möglichen Bedrohungsszenarien sollte die Nutzung von und Umgang mit Daten auch im Risikomanagement – bspw. unter Berücksichtigung der Kriterien aus dem *IDW PS 981* – berücksichtigt werden:

- Bei der Risikoidentifikation sind potenzielle Hindernisse und Herausforderungen für die zuverlässige und zielgerichtete Nutzung und Verfügbarkeit von Daten entsprechend aufzunehmen.

- Bei der Risikobewertung sind die Auswirkungen auf den Umgang mit Daten zu analysieren und zu beurteilen.

- Bei der Festlegung von Maßnahmen zur Risikosteuerung sind auch relevante Aspekte zum Umgang mit Daten zu beachten.

Bei der Identifikation möglicher Risiken können auch Ansätze für neue Geschäftschancen entstehen, wie bspw. neue Geschäftsmodelle oder Dienstleistungen.

3.3. Teil II – Organisatorische Ebene

Neben der Erfüllung der oben genannten Anforderungen ist auf der organisatorischen Ebene die Einbindung von Data Governance in die Unternehmensstrategie zu gewährleisten und durch die Zuordnung von Rollen und Verantwortlichkeiten angemessen zu unterstützen.

3.3.1. Strategischer Gestaltungsrahmen / Unternehmensstrategie und Einordnung des Wertbeitrages von Daten für das eigene Geschäftsmodell

„Daten sind das Öl des 21. Jahrhunderts“[12] – Nicht erst seit diesem Slogan sind Daten branchenübergreifend für Unternehmen von zentraler Bedeutung.

Modernste Verfahren und Methoden nebst mittlerweile verfügbaren technischen Lösungen (z.B. fortgeschrittene KI-basierte Datenanalysen) erlauben über die Verwendung dieser Daten für die Optimierung von bestehenden Geschäftsprozessen hinaus die Entwicklung neuer Geschäftsmodelle – Stichwort „New Insights“. Hierbei werden

- unternehmensintern gewonnene Daten,
- am Markt käufliche Daten (bspw. über Marktmitbewerber) und
- Daten, welche Nutzer bereitstellen,

in komplexen Modellen miteinander vernetzt und so Muster und letztlich Möglichkeiten für neuartige Leistungsangebote entwickelt.

Daher finden sich zunehmend Formulierungen in den Unternehmensstrategien, die diesen sog. datenzentrierten Ansatz aufgreifen und explizit thematisieren.

Der Wert von Daten lässt sich bspw. entlang folgender Wirkungskette ableiten:

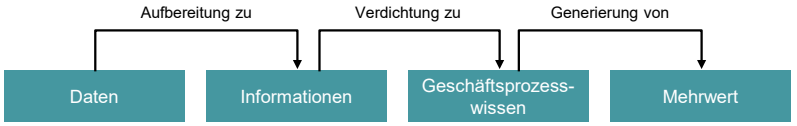


Abb. 3: Wirkungskette der Mehrwertgenerierung durch Daten

Die Entwicklung und Fortschreibung einer Datenstrategie ist daher wie die anderen Strategiedimensionen (z.B. Produkt-, Kommunikations- oder Vertriebsstrategie) ein fester Bestandteil des unternehmerischen Strategiebildungsprozesses.

3.3.2. Aufbauorganisation

Als wichtiger Erfolgsfaktor für die erfolgreiche Umsetzung der Strategie muss die Data Governance in der Organisation verankert werden. Diese sollte sich möglichst nahtlos in bestehende Strukturen einfügen.

Eine entsprechende Compliance und Risikobehandlung kann im Bereich der Data Governance dem sog. „Three Lines Model" folgen, welches sich in den vergangenen rund zehn Jahren bereits in vielen Unternehmen bewährt hat. Gemäß des Institute of Internal Auditors (IIA) stellt sich dieses wie folgt dar[13]:

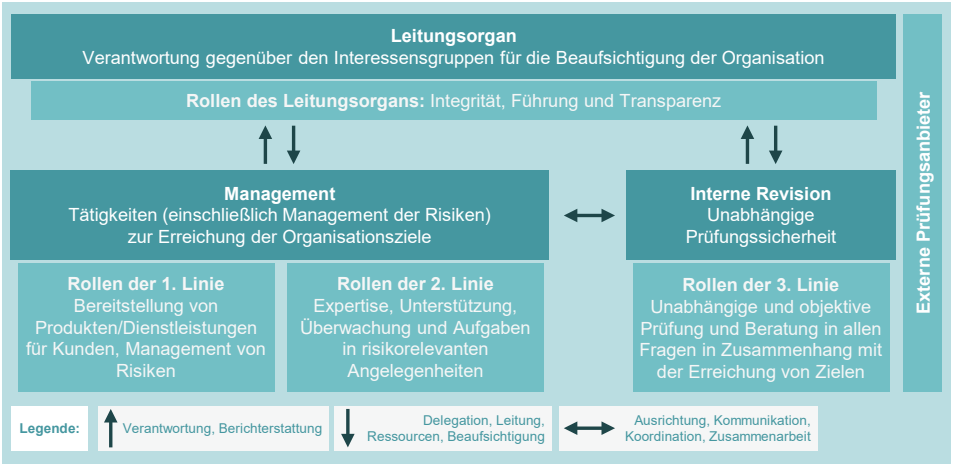


Abb. 4: Three Lines Model; Quelle: DIIR, 2020

Für die Umsetzung der Data Governance bedeutet das, die Dimension der Daten in die operativen Fachbereiche und das Management zu integrieren und bestehende Governance-Strukturen wie Risikomanagement und Interne Revision zu nutzen. Darüber hinaus kann die zentrale Funktion eines Chief Data Officers (CDO, nicht zu verwechseln mit dem Chief Digital Officer), sofern vorhanden, eingebunden werden.

Zur Wahrnehmung der Aufgaben sollten entsprechende Rollen und Verantwortlichkeiten definiert und dokumentiert werden. Neben der oben angesprochenen Rolle der operativen Fachbereiche sowie der Governance-Funktionen können noch die folgenden Rollen unterschieden werden:

- Application Owner (AO)
- System Owner (SO)
- Information Owner (bei elektronischer Speicherung von Informationen „Data Owner" – IO)

Der AO stellt sicher, dass die betreffende Applikation die erforderlichen fachlichen Funktionen anwendbar bietet, die das Business benötigt und ist für den fachlich-funktionalen Lebenszyklus verantwortlich. Bezogen auf das Beispiel „Benutzer- und Berechtigungsmanagement" gibt diese Rolle die sachlich-fachlichen Vorgaben (welche Rolle wird benötigt, Vergabe-/Entzugsprozesse für Nutzerrollen etc.) und achtet in der fachlichen Nutzung darauf, dass die Anwendung gemäß dem Rollenkonzept genutzt wird.

Der SO, welcher, verkürzt formuliert, für den (auch unter Compliance-Aspekten) ordnungsgemäßen technischen Betrieb verantwortlich zeichnet, ist i.d.R. in der IT-Abteilung verortet.

Eine weitere, exemplarische Aufgabe ist sicherzustellen, dass angemessene technische Vorgaben für die Realisierung und Bereitstellung eines Benutzer- und Berechtigungsmechanismus beachtet und umgesetzt werden.

Der IO wiederum ist für die in seinem Verantwortungsbereich verarbeiteten Informationen (Daten) verantwortlich. Da Daten, wie bspw. ein Kundenname, oftmals in mehr als einer Applikation verarbeitet und gespeichert werden, ist unmittelbar ersichtlich, dass der IO i.d.R. mit mehreren AO und damit auch mit mehreren SO zusammenwirkt.

Ergänzt werden kann diese Struktur durch die Rolle des „Process Owners" (PO, dt. oft „Prozesseigner/-verantwortlicher"). Der PO verantwortet einen (oder auch mehrere, ggf. vernetzte) Geschäftsprozesse in seinem Unternehmen. Aufgaben des PO sind insb. die Ausgestaltung des jeweiligen Prozesses durch dessen fortlaufende Optimierung, die Prozessplanung und -steuerung. Der PO interagiert stark mit dem AO und dem IO.

Es wird empfohlen, die Zuständigkeiten dieser Rollen sowie das Zusammenspiel mit den übergeordneten Compliance-Rollen in einer sog. „RACI" (oder „RACI-VS" [14])-Systematik[15] angemessen zu dokumentieren, wonach folgende Verantwortlichkeiten unterschieden werden:

- **Responsible** (Durchführungsverantwortung): Die Person, die die Verantwortung im disziplinarischen Sinne für die jeweilige Durchführung trägt. Von ihr geht üblicherweise auch die Initiative für die Durchführung (auch durch andere) aus.

- **Accountable** (rechenschaftspflichtig / Kosten- bzw. Gesamtverantwortung): Der eigentliche Genehmiger, der im rechtlichen oder kaufmännischen Sinne die Verantwortung trägt.

- **Consulted** (konsultiert): Eine Person, die relevante Informationen für die Umsetzung von Projekten besitzt und als Experte befragt werden soll oder muss.

- **Informed** (zu informieren / Informationsrecht): Eine Person, die die Berechtigung besitzt, Informationen über den Verlauf von entsprechenden Projekten und/oder Vorgängen zu erhalten.

- **Verify** (überprüfen): Eine Person, welche das/die Projektergebnis(se) auf der Basis verabredeter Kriterien qualitätssichert und eine Empfehlung über Freigabe/Ablehnung erteilt.

- **Sign-Off** (freigeben): Die Person, die die endgültige Freigabe für eine Auslieferung des Projektergebnisses erteilt.

Abhängig von Unternehmensspezifika und Geschäftsmodell kann eine weitere Differenzierung notwendig sein.

3.4. Teil III – Operative Ebene

Auf operativer Ebene gilt es, die geschaffenen Strukturen erfolgreich anzuwenden und in die Geschäftsabläufe zu integrieren, um sowohl identifizierte Ansprüche zu erfüllen als auch Mehrwert für das Unternehmen zu generieren. Während einige Aspekte den üblichen Vorgehensweisen aus der Organisationslehre folgen, greift dieser Abschnitt drei wichtige Aspekte auf: die zentrale Bedeutung der Datenklassifizierung als Grundlage, die Relevanz von Richtlinien sowie Ansätze für die technische Unterstützung von Data Governance.

3.4.1. Metadaten und Klassifizierung

Die Entwicklung einer Datenklassifikation hat eine zentrale Bedeutung zur Sicherstellung der Compliance, aber auch der effizienten Nutzung. Exemplarisch lässt sich das anhand personenbezogener Daten im Kontext der DSGVO erläutern.

Die Klassifikation beinhaltet Aussagen u.a. zu den folgenden Punkten:

- Festlegung des Nutzungsbereichs
- „Eigentümer" im Sinne von Verantwortlicher für die Korrektheit (zeitlich, inhaltlich) von Daten/Dokumenten
- Bezeichnung
- Semantische Bedeutung („Inhalt")
- Strategische Bedeutung für das Unternehmen
- Quellen- und Artenfestlegung: interne Quellen, externe Datenquellen
- Qualitätsbewertung der Datenherkunft/Quellen
- Vertraulichkeitsgrad
- Aktualisierungshäufigkeit/-bedarf
- Datentypen (aggregiert, atomar)
- Aufbewahrungsfristen
- Separierung
- Anzuwendende Regularien (unternehmensintern, extern, bspw. DSGVO)
- Kreis der Verarbeitenden/Zugriffsberechtigten

Da Daten außer strukturiert bspw. in Form von Datenbanken auch unstrukturiert und gebündelt in „Dokumenten" (bspw. Verträge) gespeichert werden, ist aufbauend auf der Datenklassifizierung eine ergänzende „Dokumentenklassifikation" sinnvoll.

Das Ergebnis ist in einem Daten-/Dokumentenkatalog zu hinterlegen und idealerweise für maschinelle Auswertungs- und Verwendungsprozesse zugänglich[16].

3.4.2. Richtlinien

Aufbauend sind geeignete Richtlinien (sog. „Policies") für die Generierung, die Verarbeitung/den Umgang und schließlich die Entfernung/Vernichtung von Daten/Dokumenten zu definieren, zu kommunizieren und die Einhaltung dieser Richtlinien mithilfe eines Compliance-Systems zu überwachen und durchzusetzen.

Teilprozesse der Data Governance

Richtlinien für die Generierung, die Verarbeitung/den Umgang und schließlich die Entfernung/Vernichtung von Daten/Dokumenten bilden den regulatorischen Rahmen, in welchem sich die Teilprozesse der Data Governance wiederfinden. Es sind daher Richtlinien zu entwickeln für

- Erhebung und Speicherung von Daten („Gewinnung")
- Qualitätsbewertung und -sicherung von Daten („Vollständigkeit", „Korrektheit", „Aktualität")
- Verarbeitung/Korrektur und Weitergabe von Daten
- Aufbewahrung/Vertraulichkeit/Geheimhaltung/ordnungsgemäße Vernichtung von Daten
- Data Compliance („gesetzlichen Standards", „Branchenstandards", „ethisch-moralische Standards", firmenspezifisch)
- Verlust von Daten („Datenpannen")

Eine besondere Bedeutung kommt aus Compliance-Sicht dem strukturierten, effizienten Umgang mit sog. Datenpannen zu. Hierbei sind nicht nur solche aus dem Kontext der DSGVO zu betrachten, sondern insgesamt der ungewollte, unautorisierte Abfluss von Daten. Präventive Maßnahmen, frühzeitige Erkennung, abgestimmte interne (und im Bedarfsfall auch externe) Kommunikationsprozesse (z.B. Information des betrieblichen Datenschutzbeauftragten, ggf. der Datenschutzbehörde) sowie Maßnahmen zur Eindämmung und Folgenabminderung sind exemplarische Prozessschritte in einem steuernden Governance-Modell.

Dieses Beispiel verdeutlicht zugleich, dass sich Data Governance-Prozesse einfügen (müssen) in bestehende Governance-Prozesse wie bspw. zum Datenschutz (bspw. Grundsatz der Datenminimierung), branchenbezogene Prozesse, des Informationssicherheitsmanagements insgesamt sowie spezifischen Unternehmensregelwerken (z.B. „Need-to-know“).

3.4.3. Technologische Unterstützung / Automatisierbarkeit und Werkzeugeinsatz

Ein effizienter Umgang mit Data Governance erfordert nicht zuletzt geeignete Werkzeugunterstützung und einen möglichst hohen Standardisierungs- wie Automatisierungsgrad bzgl. der abzubildenden Prozesse.

Data Governance-Werkzeuge bilden eine prozessural-operative Schnittstelle zwischen mit generellen Compliance-Aufgaben betrauten Organisationseinheiten wie Risikomanagement, Informationssicherheitsmanagement und der IT und sind damit Teil einer übergreifenden IT-Anwendungslandschaft. Diese Werkzeuge ermöglichen den involvierten Anwendern unterschiedliche Sichtweisen auf identische Basisdaten. Nach modernem Verständnis sollten Daten als eigenständiges Gut aufgefasst und entsprechend strukturiert behandelt werden.

Die Auswahl des einzusetzenden Werkzeugs ist an den umzusetzenden (Soll-)Governance-Prozessen und den zuvor erhobenen Anforderungen der zukünftigen Nutzer/Stakeholder auszurichten. Die Komplexität der angebotenen Werkzeug-Suiten ist mitunter beträchtlich und erfordert daher neben fachlicher Expertise auch Schulung im Umgang mit den angebotenen Werkzeugen.

Da die Einführung von Data Governance und Data Governance-Systemen zu (teilweise erheblichen) Veränderungen im Unternehmen führen kann, ist es sinnvoll, hier auf den „Werkzeugkasten“ des Change-Managements zurückzugreifen. Für eine hohe Akzeptanz und Unterstützung im Unternehmen bedarf es eines Veränderungsmanagements. Dazu gehört bspw. auch, die Mitarbeiter durch entsprechende Weiterbildungen mitzunehmen.

Aufgrund des Fehlens einer international einheitlichen Definition von Data Governance stellt die Suche und die Auswahl geeigneter Tools eine große Herausforderung für Unternehmen dar. Oftmals sind einzelne Definitionen an das Portfolio von Dienstleistern angepasst, was eine sinnvolle Eingrenzung der Anbieter zusätzlich erschwert. Die Grafik stellt dar, mit welchen Schritten sich Unternehmen und deren Verantwortliche einer Tool-Auswahl annähern können:

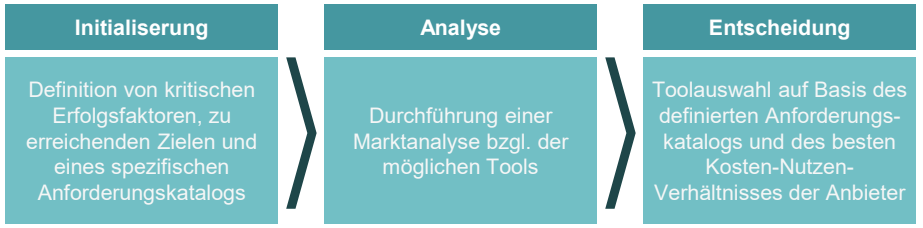


Abb. 5: vereinfachte Darstellung zur Annäherung an eine Toolauswahl

Lösungen aus den folgenden Bereichen können zur Unterstützung der Data Governance in Betracht kommen:

- Datenarchitektur und -modellierung
- Datenbanksystem
- Automatisierungs-/Workflowmanagementlösungen
- Lösungen für interne Kontrollsysteme (IKS)
- Asset-Verwaltungssysteme, z.B. nach ITIL für eine Configuration Management Database (CMDB)
- Informationssicherheits-Management-Systeme („ISO/IEC 27001“)
- Master Data Management (MDM)
- Data Warehouse (DWH), Business Intelligence (BI) & Analytics
- Dokumentenmanagementsysteme (DMS)

Wichtige Erfolgsfaktoren sind die saubere Definition der Anforderungen als Grundlage für die Auswahl einer Lösung und die Erkenntnis, dass es vermutlich mehr als eine technische Lösung zur Unterstützung des Management Systems benötigt. Dabei kann aber auch auf teilweise bereits im Unternehmen existierende Lösungen zurückgegriffen werden, welche in jedem Fall in die Selektion mit einbezogen werden sollten (z.B. Systeme zu Risikomanagement und IKS).

4. BERATUNG UND PRÜFUNG IM KONTEXT DATA GOVERNANCE

Wirtschaftsprüfer*innen sind aufgrund ihrer Kenntnisse und Erfahrungen in besonderem Maße zur Beratung und Unterstützung bei der Einrichtung von Management Systemen befähigt. Als vertrauensschaffende und unabhängige Partei sind sie zudem bestens dafür positioniert, Prüfungs-, Assurance- und andere Beratungsleistungen in diesem Zusammenhang zu erbringen.

Ein dedizierter Standard existiert noch nicht. Passender Anhaltspunkt für die Beratung bei der Einführung oder Prüfung des DGMS ist jedoch der *IDW PS 980* zur Prüfung von Compliance Management Systemen. Die Anforderungen lassen sich, wie unter Abschn. 3.3. dargestellt, gut übertragen.

Gegenstand der Prüfung sind die in einer DGMS-Beschreibung enthaltenen Aussagen über das eingerichtete System. Als Systemprüfung ist diese Prüfung nicht auf das Erkennen einzelner Verstöße gegen regulatorische Vorschriften (z.B. gegen DSGVO) oder interne Vorgaben (z.B. falsche Klassifizierung von Daten im Datenkatalog) ausgerichtet, sondern vielmehr auf das Managementsystem als Governance des Unternehmens. Dabei können verschiedene Prüfungsumfänge festlegt werden:

- Angemessenheitsprüfung
- Wirksamkeitsprüfung

Das Ergebnis wird in einer Berichterstattung festgehalten, welche bei Bedarf auch ggü. Dritten verwendet werden kann.

Zusätzlich kann es sinnvoll sein, den Einsatz von Daten in KI-Systemen regelmäßig von Wirtschaftsprüfer*innen nach *IDW Entwurf eines Prüfungsstandards: „Prüfung von KI-Systemen" (IDW EPS 861)* prüfen zu lassen und bei Bedarf anzupassen bzw. neue Strukturen zu implementieren.

Im Umfeld von Data Governance können Wirtschaftsprüfer*innen ihr Know-how und Better Practices einfließen lassen und somit Entwicklungs- und Implementierungsprojekte effizient und effektiv unterstützen. Die Beratung kann sich hier von der Entwicklung einer Data Governance-Strategie, über die Entwicklung und Implementierung von Data Governance-Prozessen, Master- und Meta-Data-Management-Lösungen oder der Konzeptionierung, Entwicklung und Implementierung von Compliance Management Systemen erstrecken. Aufgrund der Erfahrungen und dem Wissensstand von Wirtschaftsprüfer*innen können diese den Unternehmen bei der Umsetzung von Data Governance auch als Sparringspartner zur Seite stehen.

5. FAZIT UND AUSBLICK

Die steigende Bedeutung von Daten und die daraus möglichen Chancen, aber auch Risiken für Unternehmen zeigen die Wichtigkeit, sich mit ganzheitlicher Data Governance zu befassen. Das Angehen als eine interdisziplinäre und gesamtunternehmerische Aufgabe hilft, effizienter regelkonform (compliant) zu werden und Potenziale besser zu erschließen. Dabei lässt sich auf bewährte Ansätze aus anderen Bereichen der Governance zurückgreifen, welche um die Fragestellung des sicheren und vertrauensvollen Umgangs mit Daten erweitert werden können. Die Aufgabe ist also lösbar, bedarf aber einer Konkretisierung auf die jeweiligen Unternehmensverhältnisse sowie einer Unterstützung durch die Unternehmensleitung.

Auch die Gesetzgeber sowohl auf europäischer als auch auf nationaler Ebene beschäftigen sich mit vergleichbaren Fragestellungen. Data Governance wurde durch die EU-Kommission bereits 2019 als führendes Thema – neben KI, Big Data, Cloud Computing und Open Data – eingestuft. Im Rahmen der Strategie „Shaping Europe's Digital Future"[17] wurde im November 2020 ein Entwurf für den „EU Data Governance Act"[18] vorgestellt. Dieser soll den Austausch von Daten zur Förderung von Innovation ermöglichen. Der Entwurf des „EU-AI Act" vom 21. April 2021[19] befasst sich mit der Regulierung von KI-Systemen. Dabei wird die Wichtigkeit von Data Governance und Data Management im Hinblick auf die Verwendung von Daten bei KI-Systemen betont sowie damit verbundene ethische Fragestellungen zur Erhebung, Speicherung und Verwendung von Datenthematisiert. Für Unternehmen, die KI vertreiben oder einsetzen, ergeben sich hieraus schon bald konkrete Anforderungen, z.B. zum Umgang mit Daten zum Trainieren von KI-Systemen.

Auf nationaler Ebene gibt bspw. der „Kriterienkatalog für KI-Cloud-Dienste – AIC4"[20] des Bundesamts für Sicherheit in der Informationstechnik (BSI) Mindestanforderungen für eine sichere Verwendung von KI vor, die auch ein strategisches Datenmanagement umfasst.

Es ist festzuhalten, dass eine erfolgreiche Umsetzung aktueller Digitalisierungsvorhaben oder der Einsatz von Technologien wie Machine Learning und KI ohne die strukturierte und strategische Nutzung von Daten unvorstellbar ist. Um in einem immer stärker technologie- und datengetriebenen Wettbewerb zu bestehen, sollten Unternehmen sich zeitnah mit einer strategischen Herangehensweise an die Datengenerierung und -nutzung auseinandersetzen.

Data Management und damit auch Data Governance sind geostrategische Zukunftsthemen vor dem Hintergrund der Nutzung von KI-Systemen und weiteren Algorithmus-basierten Geschäftsmodellen. Die Nutzung von Daten als „Rohstoff" für diese Systeme setzt auch in der Politik Maßnahmen und Regulierungen voraus. Der Zugang zu und der Besitz von Daten hat bereits heute einen hohen strategischen Stellenwert für Unternehmen, der weiter an Wichtigkeit gewinnen und einen wachsenden Anteil an der Wertschöpfung ganzer Volkswirtschaften repräsentieren wird. Auf der anderen Seite stehen die Bürger*innen als „Datengeber" mit ihren Privatsphären- und Sicherheitsbelangen. Der verantwortungsbewusste Umgang mit Daten und dessen Belegbarkeit können für Unternehmen einen entscheidenden Marktvorteil bieten.

FUSSNOTEN

[1] Zur Einordnung: 33 Zettabyte entspricht einer Speicherkapazität von 660 Milliarden Blu-rays oder 33 Millionen menschlichen Gehirnen, https://de.statista.com/infografik/17739/speicherplatz-bedarf-im-zettabyte-zeitalter/ (Abruf: 05.01.2022)

[2] Vgl. https://www.statista.com/statistics/871513/worldwide-data-created/ (Abruf: 05.01.2022)

[3] Vgl. www.iwd.de/artikel/datenmenge-explodiert-431851/ (Abruf: 05.01.2022)

[4] Vgl. https://www.kowi.de/Portaldata/2/Resources/fp/2020-COM-IPR-Action-Plan_de.pdf (Abruf: 05.01.2022)

[5] Vgl. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066 (Abruf: 05.01.2022)

[6] Vgl. https://www.iwkoeln.de/fileadmin/user_upload/Studien/Gutachten/PDF/2019/Gutachten_Data_Governance_DEMAND_Template.pdf (Abruf: 17.02.2022).

[7] Vgl. Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung), Art. 4 Abs. 1.

[8] Vgl. *IDW PS 980*, Tz. 5

[9] Vgl. https://www.isaca.de/de/veroeffentlichungen/cobit (Abruf: 05.01.2022)

[10] Vgl. https://www.axelos.com/certifications/itil-service-management (Abruf: 05.01.2022)

[11] Vgl. https://www.scrum.org/ (Abruf: 05.01.2022)

[12] Vgl. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156 (Abruf: 05.01.2022)

[13] THE IIA'S THREE LINES MODEL – An update of the Three Lines of Defense, Juli 2020, S. 4; Übersetzung gem. Deutsches Institut für Interne Revision (DIIR), vgl. https://www.diir.de/fileadmin/fachwissen/downloads/Three-Lines-Model-Updated-German.PDF (Abruf: 05.01.2022)

[14] „RACI-VS" leitet sich aus den Anfangsbuchstaben der englischen Begriffe Responsible, Accountable, Consulted, Informed, Verify, Sign-Off ab.

[15] Oftmals wird die Form RACI angewendet; bei größeren Unternehmen mit einer (sehr) hohen Prozessreife kommt auch die Erweiterung „VS" zum Einsatz.

[16] Dies ist nicht gleichbedeutend mit dem Begriff des "Data Dictionary" aus den 70er und 80er Jahren des vorigen Jahrhunderts, sondern stellt eine erhebliche qualitative Erweiterung dar.

[17] https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf (Abruf: 05.01.2022)

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767 (Abruf: 05.01.2022)

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (Abruf: 05.01.2022)

[20] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/AIC4/aic4.html (Abruf: 05.01.2022)

Ihre Notizen:

Ihre Notizen:

Dieses Knowledge Paper wurde von der IDW Arbeitsgruppe „Datenmanagement/Data Governance“ entwickelt.

Wir freuen uns über Ihre Anmerkungen. Sie können diese direkt an Frau Valerie Wachter, Institut der Wirtschaftsprüfer in Deutschland e.V., Postfach 320580, 40420 Düsseldorf oder an valerie.wachter@idw.de senden.

INSTITUT DER WIRTSCHAFTSPRÜFER IN DEUTSCHLAND E.V.
WIRTSCHAFTSPRÜFERHAUS

Tersteegenstr. 14
40474 Düsseldorf

Postfach 32 05 80
40420 Düsseldorf

Telefon: +49 (0) 211/4561-0
Telefax: +49 (0) 211/4561097

E-Mail: info@idw.de
Web: www.idw.de

IDW
INSTITUT DER WIRTSCHAFTSPRÜFER