Fraunhofer ISST

Data Governance in der kollaborativen Wertschöpfung

Infrastruktur zur Realisierung industrieller Dienstleistungen in Wertschöpfungsnetzwerken im Kontext digitaler Integrität und Souveränität

Teil des Projektes:

SEALED SERVICES

Aus Gründen der besseren Lesbarkeit wird in diesem Whitepaper die Sprachform des generischen Maskulinums verwendet. Bei allgemeinen Aussagen bezieht sich die männliche Form explizit auf alle Geschlechter.

Inhalt

Zusammenfassung

Das vorliegende Whitepaper befasst sich mit dem Thema Data Governance in der kollaborativen Wertschöpfung anhand der SealedServices Infrastruktur. Dazu wird zunächst Data Governance als Rahmenwerk definiert und in vier Dimensionen aufgeteilt. Diese vier Dimensionen werden jeweils in ihren Auswirkungen auf die drei verschiedenen Infrastrukturebenen und die drei zugehörigen Subebenen beschrieben. Die dabei betrachteten Dimensionen lauten Datenmanagement, Datenqualitätsmanagement, Datensicherheit und regulatorische Vorgaben. Das Datenmanagement befasst sich hierbei insbesondere mit der Verteilung der Verantwortlichkeiten. Die Dimension des Datenqualitätsmanagement ist wiederum unterteilt in fünf Subdimensionen zur möglichst objektiven Einordnung der Datenqualität. Im Bereich der Datensicherheit werden Möglichkeiten zur Sicherung der Komponenten und der Verbindungen durch verschiedene Technologien aufgezeigt. Diese zielen insbesondere auf einen sicheren und souveränen Datenaustausch ab. In der letzten Dimension, den regulatorischen Vorgaben, werden verschiedene EU-Regularien und das deutsche Lieferkettengesetz hinsichtlich ihrer Einflüsse auf die SealedServices Infrastruktur und ihrer beteiligten Unternehmen untersucht und aufgezeigt. Dabei liegt der Fokus auf dem Data Governance Act, dem Digital Markets Act, dem Digital Services Act und dem Data Act. Insgesamt ergeben die Untersuchungen der einzelnen Ebenen und ihrer Subebenen der Infrastruktur sowohl eine Vielzahl an Implikationen für die weitere Entwicklung der SealedServices Infrastruktur, als auch die Ausrichtung der beteiligten Unternehmen unter Berücksichtigung der rechtlichen Vorgaben. Die Nutzung der beschriebenen Data Governance Facetten können in der Folge den beteiligten Unternehmen dahingehend Mehrwert verschaffen, dass unter anderem neue Geschäftsfelder entstehen oder aktuelle Geschäftsfelder wirtschaftlicher gestaltet werden können.

SealedServices: Das Projekt

Das Verbundsprojekt SealedServices ist auf die Förderung von Co-Produktion von industriellen Dienstleistungen fokussiert. Ziel des Projektes ist die Schaffung einer Plattform mit Marktplatz und App Store zur Bereitstellung, Koordination und Abwicklung physischer und datenbasierter (Teil-)Services im Kontext des Maschinen- und Anlagenbaus.

Grundlage dieser Services sind hierbei Rahmenbedingungen zur Wahrung der Integrität und Souveränität der unternehmenseigenen Daten. Ein Mehrwert wird hierbei unter anderem durch die Kombination verschiedener Einzellösungen zu Gesamtdienstleistungen geschaffen. Der bereits erwähnte Marktplatz bringt hierbei sowohl die Angebots- als auch die Nachfrageseite zusammen. In Bezug auf den App Store können Unternehmen Erweiterungen ihrer bestehenden Produkte und Dienstleistungen sowie eigenständige Dienstleistungen als digitale Services anbieten.

Auf der technischen Ebene wird beispielsweise durch die Einführung einer definierten Rollenhierarchie und Governance eine Integration der digitalen Lebenslaufakte ermöglicht, welche als zentrales Register servicespezifisch Zugriffsrechte bereitstellt. Unterstützt durch die Distributed Ledger Technologie wird eine transparente und nachvollziehbare Dokumentation der Leistungen sichergestellt.

1 Data Governance

Ein zentraler Aspekt innerhalb eines Unternehmens, aber auch unternehmensübergreifend, stellt die Organisation von Daten in Form eines Data Governance Konzeptes dar. Data Governance ist dabei definiert „als das Rahmenwerk, welches die Grundlage für den Umgang mit und die Bewirtschaftung von Daten in einem Unternehmen für alle internen und externen Stakeholder bildet". Ziel von Data Governance ist dabei die Schaffung des größtmöglichen Nutzens aus Daten sowie die Einhaltung gesetzlicher Regularien und die Erstellung neuer wertschöpfenden Angebote. [1, 2]

Data Governance konzentriert sich damit auf die Art und Weise, wie Entscheidungen über Daten getroffen werden sowie den Umgang mit Daten in Prozessen. Der Umfang und Fokus der Data Governance Aktivitäten eines Unternehmens oder zum Beispiel einer unternehmens-übergreifenden Infrastruktur hängen hierbei von den organisatorischen Anforderungen ab.[3]

Dabei hat Data Governance Auswirkungen sowohl auf das unternehmensinterne Handeln, als auch auf das unternehmensübergreifende Handeln. In der vorliegenden Abbildung 1.1 werden die verschiedenen Dimensionen von Data Governance dargestellt:

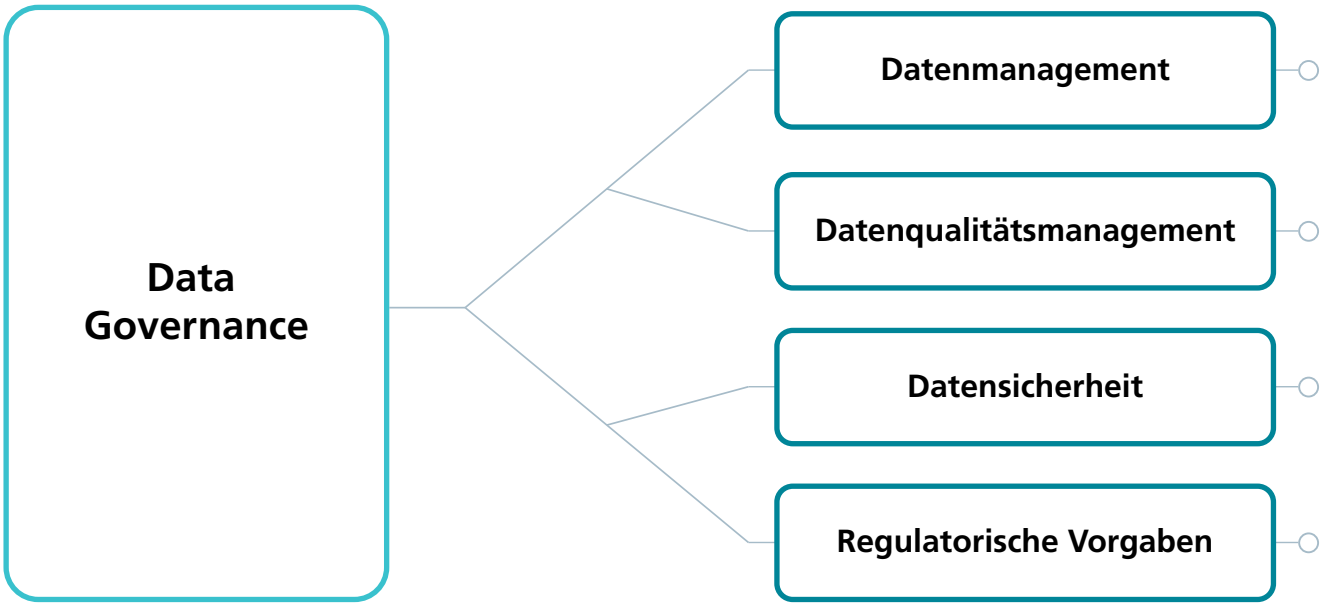


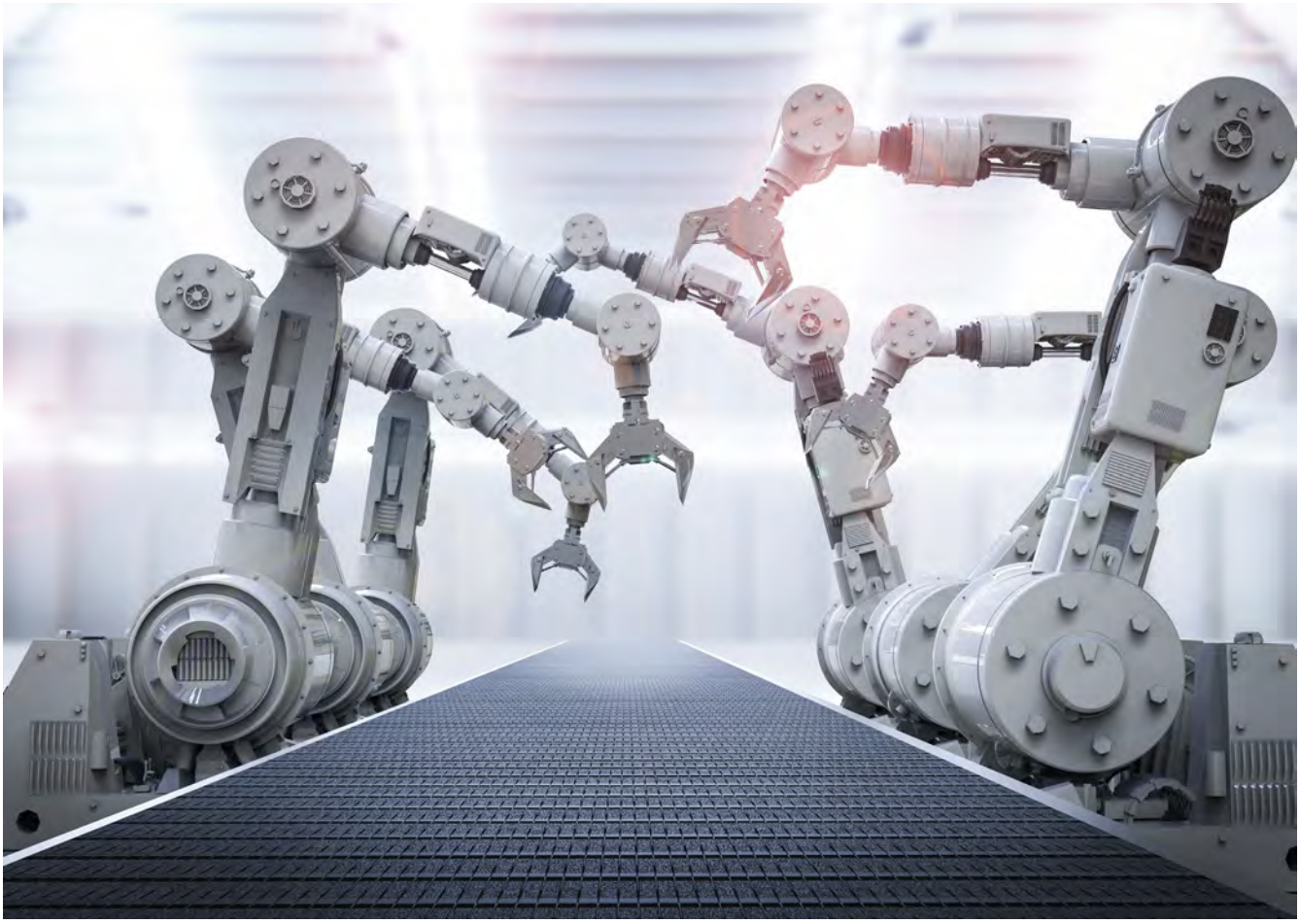
Abbildung 1.1: Dimensionen der Data Governance

Data Governance im SealedServices Ökosystem

Mit der Schaffung eines Ordnungsrahmens in Form von Data Governance wird die Grundlage für die Co-Produktion im SealdServices Ökosystem geschaffen. Durch eine einheitliche Betrachtung der Datenorchestrierung in der Co-Produktion werden die Daten durch einheitliche Standards im SealedServices Ökosystem auch unternehmensübergreifend nutzbar. Data Governance schafft hierbei die Rahmenbedingungen, um agile und bedarfsorientierte kooperative Wertschöpfungsnetzwerke unter Bedingungen eines sicheren und souveränen Datenaustauschs zu ermöglichen. Somit wird aktiv Insellösungen entgegengewirkt und eine einheitliche Sprache der digital vernetzten, industriellen Dienstleistung geschaffen. Zur Umsetzung muss in allen Bereichen der zugrunde liegenden Infrastruktur bei der Ausarbeitung Data Governance bedacht werden.

Praktische Anwendung in der SealedServices Infrastruktur

Die SealedServices Infrastruktur adressiert die nachhaltige Wertschöpfung des deutschen Maschinen- und Anlagenbaus mittels drei Ebenen. Hierbei stellt Data Governance die Grundlage für die drei Ebenen der SealedServices Infrastruktur dar.



1.1 Geschäftsstrategie

Die erste Ebene befasst sich mit der Geschäftsstrategie und ist in drei Subebenen unterteilt: Ziele, Co-Creation und Marktumfeld. Dabei lässt sich die Subebene der Ziele von Unternehmen im SealedServices Kontext in wirtschaftliche und strategische Ziele aufteilen. Die Subebene Co-Creation hingegen fokussiert sich auf die Darlegung der beteiligten Akteure im Ökosystem und die Subebene des Marktumfeldes konzentriert sich auf die Beobachtung und den Austausch mit benachbarten Sektoren. In dieser Ebene wird somit die Führungsebene der an SealedServices beteiligten Unternehmen angesprochen, um bereits im Planungsprozess die Spezifikationen des SealedServices Ökosystems zu integrieren.

1.2 Geschäftsprozess

Die Geschäftsprozesse werden in der zweiten Ebene dargestellt, welche zunächst einen Prozess zur Erbringung von Leistungen durch den Kallenberg-Prozess definiert[4]. Der Leistungsbedarf als erste Subebene beschreibt hierbei das nötige Leistungsprofil. Die zweite Subebene differenziert zwischen datenbasierten und physischen SealedServices. Das Matching Verfahren als dritte Subebene bringt Anbieter, Kunden, Partner und weitere Akteure zusammen. Dies ermöglicht die Zusammenarbeit und die Etablierung erfolgreicher Co-Produktionen für spezifische Anwendungsfälle. Hierbei werden die unterschiedlichen Angebote, Nachfragen, Ressourcen und Ziele der Akteure berücksichtigt. Data Governance bildet dabei die Grundfunktion der einheitlichen Darstellung über Unternehmensgrenzen hinweg, sodass die Geschäftsprozesse auch unternehmensübergreifend einfacher aufeinander abgestimmt werden können.

1.3 Informationstechnologie

Die dritte Ebene stellt die Informationstechnologie der SealedServices Infrastruktur dar. Dabei bilden die plattformbasierten Anwendungen, welche in Marktplatz und App Store unterteilt sind, die erste Subebene. Die zweite Subebene befasst sich mit der Plattformsicherheit insbesondere in Hinblick auf die Sicherung der Schnittstellen. Die Datenhaltung als dritte Subebene definiert insbesondere die Basis des Multi-Cloud Ansatzes als Grundlage für Datenhaltung und Datenaustausch. Data Governance spielt hierbei insbesondere hinsichtlich der Architektur der Informationstechnologie eine Rolle. Dabei ist die Integrierung des unternehmensübergreifenden Datenaustausches in die Strategie der Datenhaltung essenziell, um die Integrität und Souveränität der Daten zu erhalten.

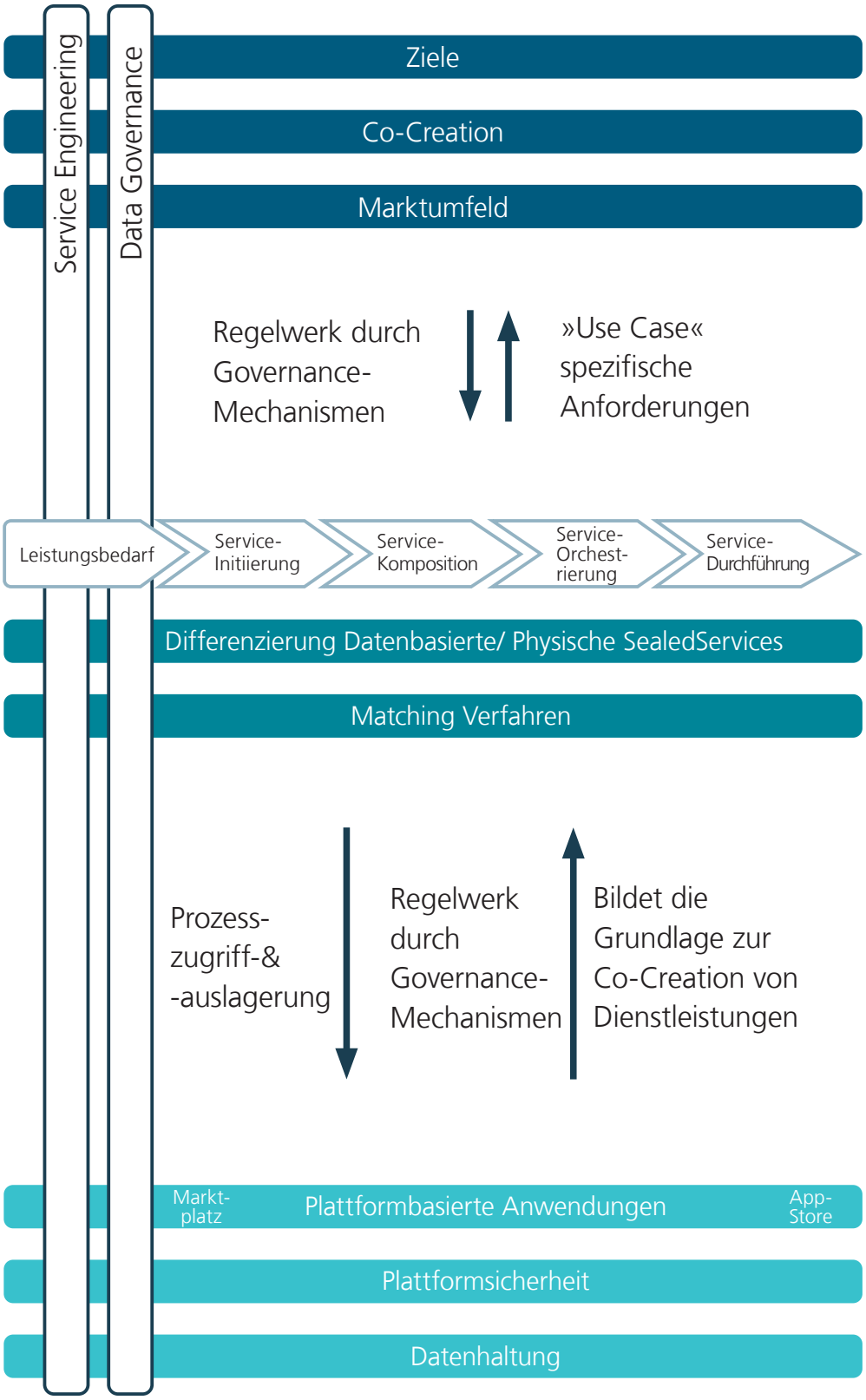


Abbildung 1.2: SealedServices Infrastruktur (SSI) Modell

2 Datenmanagement

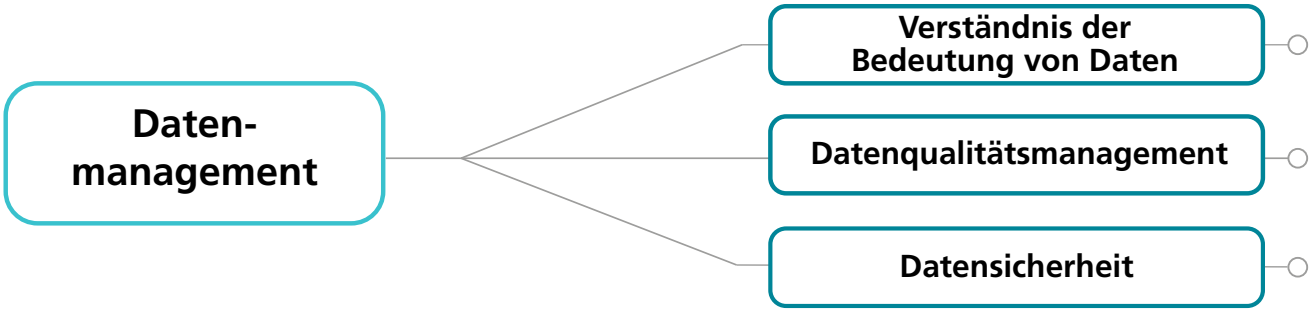


Abbildung 2.1: Unterteilung des Datenmanagements

Datenmanagement beschreibt die Entwicklung, Ausführung und Überwachung von Plänen, Richtlinien und Praktiken, die den Wert von Daten und Informationsbeständen während ihres gesamten Lebenszyklus liefern, kontrollieren, schützen und steigern.[3] Der Fokus dieses Whitepapers liegt hierbei auf der **organisatorischen Festlegung von Verantwortlichkeiten** der einzelnen Teilbereiche einer Organisationsstruktur für das Datenmanagement. Das Datenmanagement stellt dabei für Unternehmen ein Kernelement zur Generierung eines Wettbewerbsvorteiles dar. Der wichtigste Treiber für das Datenmanagement liegt dabei in der Möglichkeit, für Unternehmen aus ihren Datenbeständen Wert zu generieren. Analog zu anderen Vermögenswerten von Unternehmen ermöglicht das Datenmanagement die Schaffung eines Wertes. Dabei benötigen Unternehmen, die den Wert von Daten nutzen wollen, eine Architektur des Datenmanagements.[3] Zur Erstellung einer solchen Struktur und der Orchestrierung der damit verbundenen Aktivitäten in den jeweiligen Bereichen des Datenmanagements sind je nach Größe und Ausführung der Organisation und des Datenmanagements ein oder mehrere Personen nötig, um alle Aufgabenfelder abzudecken. Diese übernehmen **technische Aufgaben** wie Datenbank- und Netzwerkadministration, aber auch, wie bereits erwähnt, **strategische Funktionen** wie die Rolle des Chief Data Officers oder des Datenstrategen. In der Praxis ist dabei herauszustellen, dass nicht nur die Datenmanagementfachleute die Verantwortung für die Datenverwaltung tragen, sondern auch die Verantwortlichen im Bereich der Informationstechnologie. Die drei Ziele der Verantwortlichkeiten werden dazu in der vorliegenden Abbildung 2.1 dargestellt.

Hierbei muss zunächst die verantwortliche Person für Datenmanagement ein Verständnis über die Bedeutung von Daten erlangen. Daten dienen nicht nur der Schaffung eines neuen Vermögenswertes, sondern bilden auch die Grundlage für zukünftige Wettbewerbsvorteile. Diese können durch neue Geschäftsmodelle oder durch die Optimierung bestehender Prozesse erreicht werden. Dies ist beispielsweise mit der Schaffung einer digitalen Lebenslaufakte zu einer Maschine möglich. Diese digitale Lebenslaufakte ist dabei ein Instrument zur lückenlosen Dokumentation des Produktlebenszyklus. Die Schaffung dieses weiteren Angebotes ermöglicht sowohl für den Hersteller, als auch für den Kunden der Maschine die strukturierte und klar zugeordnete Darstellung der Daten zur entsprechenden Maschine. Die zweite Kategorie beschreibt unter anderem die Verantwortung für die Speicherung, die Gewährleistung der Integrität und Souveränität sowie den expliziten Wert von Daten unter dem Begriff Datenqualitätsmanagement. Hierbei wird die Verantwortlichkeit des Datenqualitätsmanagements definiert, sodass benötigte Daten anhand objektiver Kriterien gemessen und in ausreichender Qualität für die Anwendungsfälle erhoben oder erworben werden können. Diese Kategorie wird im weiteren Verlauf dieses Whitepapers genauer erläutert. Die Datensicherheit als weitere Kategorie beschreibt die genaue Zuständigkeit zur Prävention von unautorisierten Zugriffen, Manipulation, unangemessenem Zugriff oder Verwendung der Daten. Hierbei werden Verantwortlichkeiten definiert, um im Geschäftsprozess die Datensicherheit zu gewährleisten. Diese Kategorie und ihre verschiedenen Dimensionen werden auch im weiteren Verlauf näher erläutert. Im Hinblick auf das Datenmanagement liegt der Fokus im Folgenden daher auf der Orchestrierung und der Festlegung von Verantwortlichkeiten in der Data Governance. Data Governance bietet hierbei den Ordnungsrahmen für das Datenmanagement (Datenmanagementstrategie). Dabei müssen für die Festlegung dieser Strategie bestehende Strukturen und Steuerungselemente im Datenmanagement herausgestellt werden. Hierfür sind Verantwortlichkeiten innerhalb der Unternehmen zu bestimmen, aber auch unternehmensübergreifend erforderlich, um Verantwortlichkeiten zu definieren.[5]

Datenmanagement im SealedServices Ökosystem

2.1 Geschäftsstrategie

Innerhalb der Ebene Geschäftsstrategie wird das Datenmanagement administrativ adressiert. Dies startet auf der Subebene der Ziele. Hierbei wird durch die Definition von Zielen und der unternehmerischen Ausrichtung **Klarheit über Verantwortlichkeiten** geschaffen. Dazu zählen unter anderem die Sicherstellung der Bereitstellung der benötigten Daten für das Ziel oder auch die Schaffung eines Ansprechpartners für beispielsweise unternehmensübergreifenden Datenaustausch. Diese Zuordnung von Verantwortung ermöglicht hierbei eine stabile Organisation, da bei Problemen oder sonstigem Kommunikationsbedarf die entsprechenden Ansprechpartner ohne Organisationsbedarf ihr Anliegen herantragen können.

Die Subebene der Co-Creation adressiert explizit die unternehmensübergreifende Zusammenarbeit. Hierbei besteht für die Organisationen die Aufgabe darin, im Datenmanagement **klare Definitionen des Arbeits- und Datenbereitstellungsumfangs** zu erarbeiten. Dazu müssen beispielsweise Rollen wie Dienstleister, Plattformbetreiber, Dienstleistungsempfänger klar definiert werden und mit explizitem Leistungsprofil herausgearbeitet werden. Dies unterstützt die Teilnehmer im SealedServices Ökosystem über Unternehmensgrenzen hinweg, Probleme direkt an die richtige Organisation und die darin verantwortliche Person zu richten.

Auf der dritten Subebene der Geschäftsstrategie handelt es sich um die Beobachtung des direkten Marktumfeldes und benachbarter, weiter fortgeschrittener Sektoren zur frühzeitigen Adressierung von beispielsweise Dienstleistungserweiterungen. Hierzu ist, analog zu den beiden anderen Subebenen der Geschäftsstrategie, eine klare Zuordnung von Vorteil, um marktbezogene Daten über neue Entwicklungen durch eine Instanz aggregiert zu sammeln und daraus schließende Entwicklungen zu adressieren. Die klare Zuordnung verhindert hierbei, dass verschiedene Gruppen bzw. Personen in einem Unternehmen an den selben Marktdaten arbeiten oder das durch eine Zersplitterung der Aufgabe ohne klare Zuordnung nicht die benötigten Daten gesammelt werden können, um das ganzheitliche Marktbild zu schaffen.

Ein an der SealedServices Infrastruktur beteiligtes Unternehmen möchte über diese Infrastruktur physische Dienstleistungen anbieten. Hierbei stellt bereits die Zuordnung der Verantwortung, als Teil der Unternehmensstrategie, den Grundstein, um genügend Daten für das Matching Verfahren zu aggregieren. Alternativ, bei nicht ausreichender Bereitstellung von Daten, wäre keine Zuordnung zu Unternehmen, welche die Dienstleistung nachfragen möglich.

2.2 Geschäftsprozess

Die erste Subebene der Geschäftsprozessebene besteht aus dem Prozess nach Kallenberg. Dieser ist wiederum untergliedert in fünf Schritte und bietet eine Grundlage zur einheitlichen Erbringung von Dienstleistungen. Im ersten Prozessschritt (Leistungsbedarf) besteht die Aufgabe darin, Angebotslücken zu erkennen, um diese dann adressieren zu können. Hierzu ist Zugang zu externen Daten notwendig, aber auch beispielsweise die Nutzung eigener Kundendaten, um auch anfänglich neu entstehende Nachfragen bestehender Kunden anzusprechen. Zur Lösung dieser Aufgabe ist ein adäquates Datenmanagement und damit verbunden eine Zuordnung von Verantwortlichkeiten für die Datenerhebung, -aufbereitung und -auswertung erforderlich. Die darauffolgenden Schritte zwei bis fünf des Kallenberg-Prozesses basieren mit ihrer Datengrundlage auf den Erhebungen und Schlussfolgerungen der Daten des ersten Schritts, wodurch die Bedeutung des Datenmanagements in dieser Stufe besonders hervorzuheben ist.[4] Das Datenmanagement und damit einhergehend die Definition von Verantwortlichkeiten stellt damit die Grundlage zur Durchführung dieser Schritte.

Die zweite Subebene des Geschäftsprozesses beschreibt die Differenzierung zwischen datenbasierten und physischen SealedServices. In diesem Fall basiert die Entscheidung auf Grundlage der Daten der jeweiligen Verantwortlichen aus dem Schritt der Serviceinitiierung im Kallenberg-Prozess.[4] Auf Basis dieser Daten und der Zuordnung zu datenbasierten oder physischen SealedServices kann in der Folge auf Bausteine zurückgegriffen werden, welche die Umsetzung erleichtern.

Die dritte Subebene beschreibt das Matching Verfahren und ist damit stark abhängig vom Datenmanagement der einzelnen beteiligten Unternehmen in der SealedServices Infrastruktur. Um das passende Match zwischen Anbieter, Kunden und Partner zu schaffen, sind eine Vielzahl von Daten von allen beteiligten Unternehmen erforderlich, welche intelligent verknüpft die Basis für die Umsetzung des Matching Verfahrens und der daraus resultierenden Co-Produktion schaffen. Diese Aufgabe der Bereitstellung der nötigen Daten zur Verknüpfung

im Matching Verfahren stellen hierbei die Grundlage für die Co-Produktion und damit nachgelagerter Wertschöpfungsaufträge dar. Somit handelt es sich im Falle der Orchestrierung des Datenmanagements um eine zentrale Funktion, welche bei Nicht-Erfüllung alle weiteren wertschöpfenden Schritte durch mangelhaftes Matching oder ausbleibendes Matching an der Teilhabe der Co-Produktion hindert.

Die Orchestrierung der Bereitstellung der benötigten Daten ermöglicht die Schaffung neuer Absatzmöglichkeiten für produzierende Unternehmen, die an der SealedServices Infrastruktur teilnehmen. Dies bezieht sich nicht nur auf die Erweiterung des Kundenkreises, sondern ermöglicht weitere Services der Wertschöpfung, wie die digitale Lebenslaufakte einer Maschine.

2.3 Informationstechnologie

Innerhalb der Ebene Informationstechnologie steht das Datenmanagement besonders im Fokus. Die Subebene der plattformbasierten Anwendungen, lässt sich in zwei Bereiche unterteilen, den Marktplatz und den App Store. Im Falle des Marktplatzes handelt es sich um eine Handelsplattform, welche Anbieter und Käufer zusammenbringt. Diese Applikation stellt die Basis für das Matching Verfahren der Geschäftsprozessebene dar. Hierbei ist die **Datenorchestrierung** durch eine Instanz, welche den Marktplatz betreibt, essenziell, um auf dieser Grundlage automatisierte Matching Verfahren durchführen zu können. Analog dazu muss eine Instanz, welche den App Store betreibt, mittels Datenmanagements Applikationen einheitlich innerhalb des App Stores darstellen, um eine Vergleichbarkeit zu schaffen. Somit ist sowohl Datenmanagement in Form der Bereitstellung der nötigen Daten durch die Unternehmen essenziell, jedoch auch das Datenmanagement innerhalb der Applikationen der SealedServices Infrastruktur zu vergleichbaren Darstellungen der Angebote und Nachfrage auf dem Marktplatz und App Store. Hierbei ist der App Store eine Möglichkeit, für Unternehmen unternehmenseigene Applikationen anderen Unternehmen anzubieten. Die von den anbietenden Unternehmen beschreibenden Informationen zu den Applikationen muss der App Store Anbieter dahingehend managen, dass potenzielle Kunden benötigte Applikationen schnell und einfach finden können.

Die zweite Subebene bezieht sich auf die Sicherung der Plattform, welche durch die vielen Schnittstellen Risiken der unerlaubten Erlangung von Daten bieten. Diese Schwachstellen können jedoch durch Datenverschlüsselungen und Container-Technologien etc. adressiert werden. Hierbei ist innerhalb des Datenmanagements eines Unternehmens im Austausch mit einem anderen Unternehmen über die SealedServices Infrastruktur ein **Austausch mit den Verantwortlichen des Datenmanagements** des anderen Unternehmens von Vorteil. Dies ermöglicht die Etablierung eines **unternehmensübergreifenden Sicherheitsstandards**.

Auf der Subebene der Datenhaltung wird in der SealedServices Infrastruktur ein Multi-Cloud Ansatz verfolgt. Dies ermöglicht für die einzelnen beteiligten Unternehmen mehr Flexibilität in ihrem Datenmanagement, da diese für einen Austausch mit anderen Unternehmen nicht in einer spezifischen Cloud vorliegen müssen. Für die SealedServices Infrastruktur führt dies jedoch dazu, dass im Datenmanagement **innerhalb der Infrastruktur verschiedenste Schnittstellen** bereitgestellt und entsprechende Ansprechpartner geschaffen werden müssen, um einen Datenaustausch zu gewährleisten.

Ein an SealedServices beteiligtes Unternehmen kann sein Angebot auf dem Marktplatz verbessern, indem es Daten akkurat bereitstellt. Hierdurch wird die Grundlage geschaffen, dass das Angebot gefunden wird. Außerdem können die Vorteile gegenüber dem Wettbewerb von Kunden erkannt werden.

3 Datenqualitätsmanagement

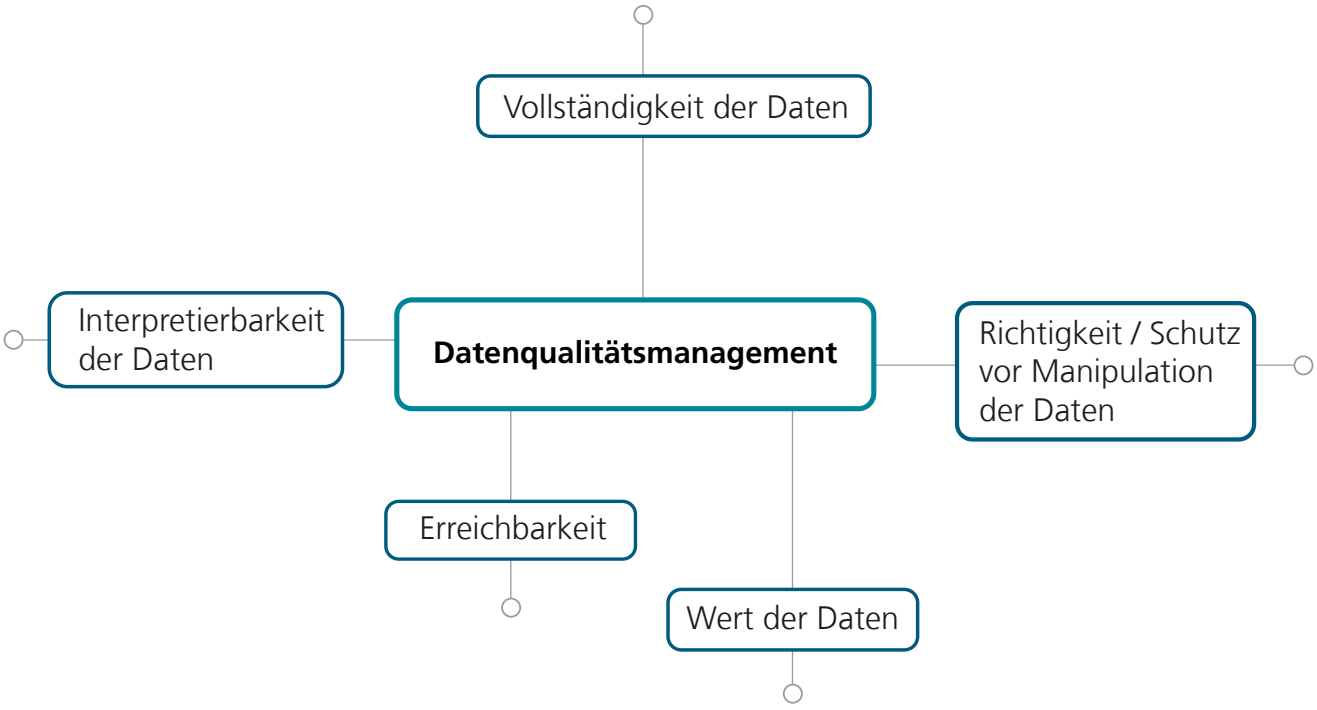


Abbildung 3.1: Dimensionen des Datenqualitätsmanagements

Das Datenqualitätsmanagement wird, angelehnt an Pipino in **fünf Dimensionen** unterteilt. Dies stellt die Grundlage für ein einheitliches Datenqualitätsmanagement innerhalb eines Unternehmens oder auch unternehmensübergreifend in einer Data Governance Strategie dar. Die erste Dimension beschreibt die **Erreichbarkeit von Daten**. Dieser Aspekt adressiert damit die Datenqualität hinsichtlich der Leichtigkeit und Schnelligkeit der Verfügbarkeit der benötigten Daten. Die zweite Dimension beschreibt die Menge beziehungsweise die **Vollständigkeit der Daten**, welche verfügbar sind. Der Fokus hierbei liegt in der Herausstellung, wie hoch die Datenbasis für einen spezifisch nachgefragten Aspekt ist und ob dies eine ausreichende Datenbasis darstellt, dies kann jedoch je nach Anwendungsfall unterschiedlich sein. Daher ist eine Definition der Nutzbarkeit der Daten durch Datenbreite und -tiefe von Vorteil, um den jeweiligen Nutzen anhand objektiver Messmethoden bestimmen zu können. Die **Richtigkeit und die Möglichkeit der Manipulation der Daten** stellt die dritte Dimension des Datenqualitätsmanagements dar. Dies bezieht sich auf die Richtigkeit bezogen auf z.B. Messfehler oder andere Fehler, aber auch auf die Aktualität der Daten und inwieweit diese weiterverwendbar sind. Darüber hinaus beinhaltet diese Dimension zur Beurteilung der Datenqualität die Einbeziehung von technischen Hürden für eine Manipulation sowie die allgemeine Zuverlässigkeit der Daten des entsprechenden Anbieters. Die vierte Dimension der Datenqualität besteht aus der Interpretierbarkeit beziehungsweise der **Verständlichkeit der Daten**. Dazu benötigt der Datenempfänger Dateneinheiten entsprechend dem Anwendungszweck sowie Daten in angemessener Sprache und Symbolen. Die letzte Dimension des Datenqualitätsmanagements beschreibt den **Wert der Daten**. Hierbei handelt es sich beispielsweise um den wirtschaftlichen Wert für das eigene oder auch andere Unternehmen.[5,6]

Datenqualitätsmanagement im SealedServices Ökosystem

3.1 Geschäftsstrategie

Auf der Subebene der Ziele werden die fünf Dimensionen des Datenqualitätsmanagements in den Unteraspekten Geschäftsvision, wirtschaftliche und strategische Ziele adressiert. Bezogen auf die Dimension der Erreichbarkeit wird sowohl die Geschäftsvision in Form einer erhöhten Transparenz in Unternehmensprozesse adressiert, als auch die wirtschaftlichen Ziele, sodass eine **automatisierte Erreichbarkeit von Daten** beispielsweise die Gesamtwirtschaftlichkeit eines Unternehmens erhöht. Als weiterer Aspekt kann dies zur strategischen Orientierung genutzt werden, um beispielsweise Kapazitätsengpässe etc. frühzeitig zu erkennen und aufgrund der Erreichbarkeit anderer Quellen durch die SealedServices Infrastruktur einen Ausgleich dieser Engpässe zu finden. Um die Geschäftsvision, als auch die wirtschaftlichen und strategischen Ziele auf Basis aktueller Gegebenheiten zu erstellen, ist somit eine ausreichende Menge bzw. **Vollständigkeit** der Datensätze notwendig. Hierbei muss das Ausmaß der Daten dargestellt und entsprechend klassifiziert werden, für welchen Zweck die Datentiefe ausreichend ist. Die Richtigkeit der Daten ist ein wichtiger Faktor bei der Erreichung der Ziele. Dies gilt insbesondere für extern einbezogene Daten, bei denen eine Manipulierbarkeit besteht. Die Verlässlichkeit der Daten muss daher bei der Erarbeitung der Geschäftsvision und wirtschaftlichen und strategischen Ziele berücksichtigt werden. Hierbei handelt es sich insbesondere um die richtige Darstellung des Status quo. Die **Interpretierbarkeit** und die Verständlichkeit der erhobenen oder bereitgestellten Daten haben dabei auch signifikante Auswirkungen auf die Zieldefinition und letztendlich die unternehmerische Ausrichtung eines jeweiligen Unternehmens. Dahingehend muss ein Standard geschaffen werden, um die Verständlichkeit sicherzustellen. Die **mögliche Wertschöpfung** durch gegebene oder bereitgestellte Daten stellt eine weitere wichtige Facette auf der Subebene der Ziele dar. Hierbei ist der Nutzen gegenüber dem Aufwand der eigenen Datensammlung im Unternehmen oder der monetäre Aufwand zur Akquirierung der benötigten Daten von externen Unternehmen entgegenzustellen.

Die zweite Subebene, in Form der Co-Creation, beschreibt die Akteure im Ökosystem, welche eine gemeinschaftliche Schaffung eines Wertes zum Ziel haben. Hierbei kann auf Basis des Datenqualitätsmanagements eine Zuordnung zu Akteuren wie Plattformbetreiber, Datentreuhänder etc. durchgeführt werden. Dabei ist die **Erreichbarkeit von Daten als Grundlage** für eine Co-Produktion wichtig. Hierfür sind auch **vollständige Daten von Vorteil**, um Nachfragen zu vermeiden. Um **Vertrauen** zu schaffen, ist zudem die Richtigkeit der von den Unternehmen angegebenen Daten essenziell. Auf Grundlage von interpretierbaren Daten in Form von beispielsweise eines **einheitlichen Standards der Datendarstellung** in einer Co-Produktion können für die gemeinschaftliche Wertschaffung ein Austausch spezifischer benötigter Daten vereinbart werden. Dies führt dazu, dass für alle beteiligten Unternehmen ein entsprechender **Wert geschaffen** wird.

Die dritte Subebene befasst sich mit dem Marktumfeld. Hierbei handelt es sich vorrangig um die Beobachtung anderer Akteure in eigenen, aber auch benachbarten Sektoren. Dabei dienen Schnittstellen der SealedServices Infrastruktur als Basis für einen vereinfachten Datenaustausch mit Unternehmen des eigenen und angrenzender Sektoren. Dabei ermöglicht die SealedServices Infrastruktur maßgeblich die **vereinfachte Erreichbarkeit** durch die Anbindung einer Vielzahl an Unternehmen mittels einer Vielzahl an Schnittstellen. Dies erhöht

maßgeblich die **Wahrscheinlichkeit der Zusammenstellung einer ausreichenden Menge an Daten**. Daraus folgt, dass ein Austausch mit Firmen aus anderen Sektoren oder ein Datenankauf entsprechend einen höheren Wert für das zu empfangende Unternehmen haben kann und der jeweilige Anbieter der Daten diese gewinnbringend ohne hohen Aufwand teilen kann. Zudem muss eingeschätzt werden, inwieweit entsprechende **Daten der Realität entsprechen** und nicht durch eine falsche Erhebungsmethode oder Manipulation zu falschen Schlussfolgerungen führen können. Darüber hinaus ist auch die **mögliche Wertschöpfung** dahingehend zu beurteilen, ob eine solche Marktumfeldanalyse für das Unternehmen den aufwandentsprechenden Mehrwert bietet und damit einhergehend, inwieweit die **Daten verständlich und interpretierbar** sind.

Ein produzierendes Unternehmen, das an der SealedServices Infrastruktur beteiligt ist, hat die Möglichkeit in der strategischen Ebene frühzeitig neue Erlösmöglichkeiten für Daten aus dem Produktionsprozess zu generieren. Zudem ist die Einstiegshürde aufgrund des Multi-Cloud-Ansatzes und der damit verbundenen Vielzahl an Schnittstellen der SealedServices Infrastruktur gering. Dies maximiert zudem die Erlösmöglichkeiten, da Käufer der Daten durch die aggregierte Akquirierung von Produktionsdaten auch von anderen Unternehmen in der SealdServices Infrastruktur einen höhere Wertschöpfung aufgrund von verlässlicheren Daten generieren können.

3.2 Geschäftsprozess

Die Adressierung des Datenqualitätsmanagements ist ein wichtiger Bestandteil der ersten Subebene der Geschäftsprozessebene. Der Kallenberg-Prozess als erste Subebene startet mit der Ermittlung des Leitungsbedarfs anhand von bestehender Nachfrage und Angebotslücken[4]. Dieser erste Schritt zeigt bereits die Wichtigkeit von Datenqualitätsmanagement. Da alle nachfolgenden Entwicklungsschritte nicht nur auf hohe Datenqualität der fünf verschiedenen Dimensionen angewiesen sind, sondern dass bei mangelnder Erreichbarkeit von Daten, mangelnder Menge und Vollständigkeit an Daten, falsch erhobener oder manipulierter Daten die **Grundlage für neue Geschäftsaktivitäten** bereits falsch dargestellt wird. Dies führt zu falschen Interpretationen von Daten und ggf. einem negativen Wert für beteiligte Unternehmen, da Aspekte adressiert werden, die in der Realität gar nicht existieren oder anders adressiert werden müssten.

Die zweite Subebene befasst sich mit der Differenzierung zwischen datenbasierten und physischen SealedServices. Im Falle des Datenqualitätsmanagements werden datenbasierte, aber auch physische SealedServices adressiert. Bei datenbasierten SealedServices handelt es sich um die primäre Aktivität des Handelns mit Daten. Somit ist hierbei Datenqualitätsmanagement der **Kern zur akkuraten Darstellung** anhand von Daten. Hierbei geht es um einen Informationsvorteil gegenüber der Konkurrenz und gegenüber dem eigenen Unternehmen in der Vergangenheit. Dafür sind die Dimensionen Erreichbarkeit von Daten, ausreichende Menge an Daten bzw. Vollständigkeit, Richtigkeit der Daten und Schutz vor Manipulation sowie Interpretierbarkeit und Verständlichkeit und Wertschöpfungsmöglichkeit der Daten essenziell. Bei den physischen SealedServices spielt das Datenqualitätsmanagement eine weniger zentrale Rolle als bei datenbasierten SealedServices. Nichtsdestotrotz ist auch hier durch die zunehmende digitale Begleitung physischer Produkte und Dienstleistungen Datenqualitätsmanagement in einer immer wichtiger werdenden Rolle. Dabei spielt insbesondere die Erreichbarkeit und Menge der Daten für ein adäquates Datenqualitätsmanagement eine zentrale Rolle. Primär befasst sich dies mit der Aufgabe beteiligten Unternehmen in der SealedServices Infrastruktur die entsprechenden **Datenquellen durch Digitalisierung zu erschließen** und damit erreichbar zu machen.

Im Rahmen der dritten Subebene der Geschäftsprozessebene, handelt es sich um eine der Kernfunktionen der SealedServices Infrastruktur, dem Matching Verfahren. In diesem Fall ist für die Infrastruktur essenziell, dass die Dimensionen Erreichbarkeit, Menge, Richtigkeit, Interpretierbarkeit gegeben sind, um die richtigen Unternehmen für Co-Creations zusammenzubringen. In diesem Fall hängen die Ergebnisse stark von den Daten ab, die von den Unternehmen zur Verfügung gestellt

werden. Daraus folgt, dass das Datenqualitätsmanagement innerhalb der Matching-Infrastruktur nur so gut sein kann wie das Datenqualitätsmanagement der Unternehmen. Der Multi-Cloud Ansatz unterstützt hierbei die Bereitstellung der Daten durch die Unternehmen, sodass keine Datenübertragungen auf ein zentrales Cloud System erfolgen müssen und somit der nötige Aufwand minimiert wird.

Ein an der SealedServices Infrastruktur beteiligter Anlagenbauer kann auf Basis eines guten Datenqualitätsmanagement weitere Services neben dem Kernprodukt, wie Condition Monitoring und Predictive Maintenance anbieten. Diese bieten neue Erlösfelder für das Unternehmen, ohne eine eigene Infrastruktur aufzusetzen und auch auf der Subebene das Datenqualitätsmanagement adressieren zu müssen.

3.3 Informationstechnologie

Die Subebene der plattformbasierten Anwendungen innerhalb der Informationstechnologieebene stellen die Grundlage für den Datenzugriff bzw. Datentransfer in der SealedServices Infrastruktur dar. Hierbei handelt es sich um den App Store und den Marktplatz, welche als plattformbasierte Anwendungen von der SealedServices Infrastruktur betrieben werden. Für **aussagekräftige Darstellungen von Daten** für die kollaborative Wertschöpfung ist hierfür ein hohes Maß an Datenqualität notwendig. Dazu gehören die Erreichbarkeit, Vollständigkeit und Richtigkeit der angegebenen Daten bei Angeboten auf dem Marktplatz. Darüber hinaus muss die Datenqualität dahingehend sichergestellt sein, dass die Richtigkeit und Interpretierbarkeit der Daten gewährleistet ist und durch die zielgenaue Angabe von Daten ein Wert geschaffen wird, welcher ohne die Daten nicht hätte erzielt werden können. Dafür ist eine **infrastrukturübergreifende, einheitliche Darstellung** von Daten hilfreich, um diese Qualitätsmerkmale erfüllen zu können. Analog gelten diese Datenqualitätsanforderungen auch für die Präsentation einer Applikation im App Store.

Die zweite Subebene der Informationstechnologie hat nur eine rekursive Schnittmenge mit dem Datenqualitätsmanagement, die sich auf die Verfügbarkeit der Daten bezieht. Diese Verfügbarkeit wird durch den Multi-Cloud-Ansatz und eine Vielzahl von Schnittstellen in der SealedServices Infrastruktur sichergestellt. Diese zahlreichen Schnittstellen erhöhen dabei die Anforderungen an die Plattformsicherheit.

Die Datenhaltung als dritte Subebene spielt in Hinblick auf das Datenqualitätsmanagement dahingehend eine Rolle, dass mit dem Multi-Cloud Ansatz den Unternehmen, welche an der SealedServices Infrastruktur angeschlossen sind, eine niedrigere Einstiegshürde und auch geringeren Aufwand in der Nutzung der Infrastruktur haben. Zudem kann durch eine **intelligente Datenhaltung** eine automatische Zusammenstellung der Daten eine Verbesserung der Interpretierbarkeit und damit der Nutzbarkeit der Daten hervorrufen. Diese Datenhaltung hat jedoch keine direkten Auswirkungen auf die anderen Dimensionen des Datenqualitätsmanagements.

Ein produzierendes Unternehmen kann die unternehmensinterne Dateninfrastruktur mit der SealedServices Infrastruktur mittels deren Schnittstellen verknüpfen. Dies ermöglicht durch eine niedrige Einstiegshürde einen automatisierten Datenaustausch entlang der Wertschöpfungskette, sodass durch einen geringen Etablierungsaufwand Transparenz geschaffen werden kann. Der messbare Wert, welcher mittels der Schnittstellen erhöht werden kann, ist die Qualität des Endproduktes.

4 Datensicherheit / Datensouveränität

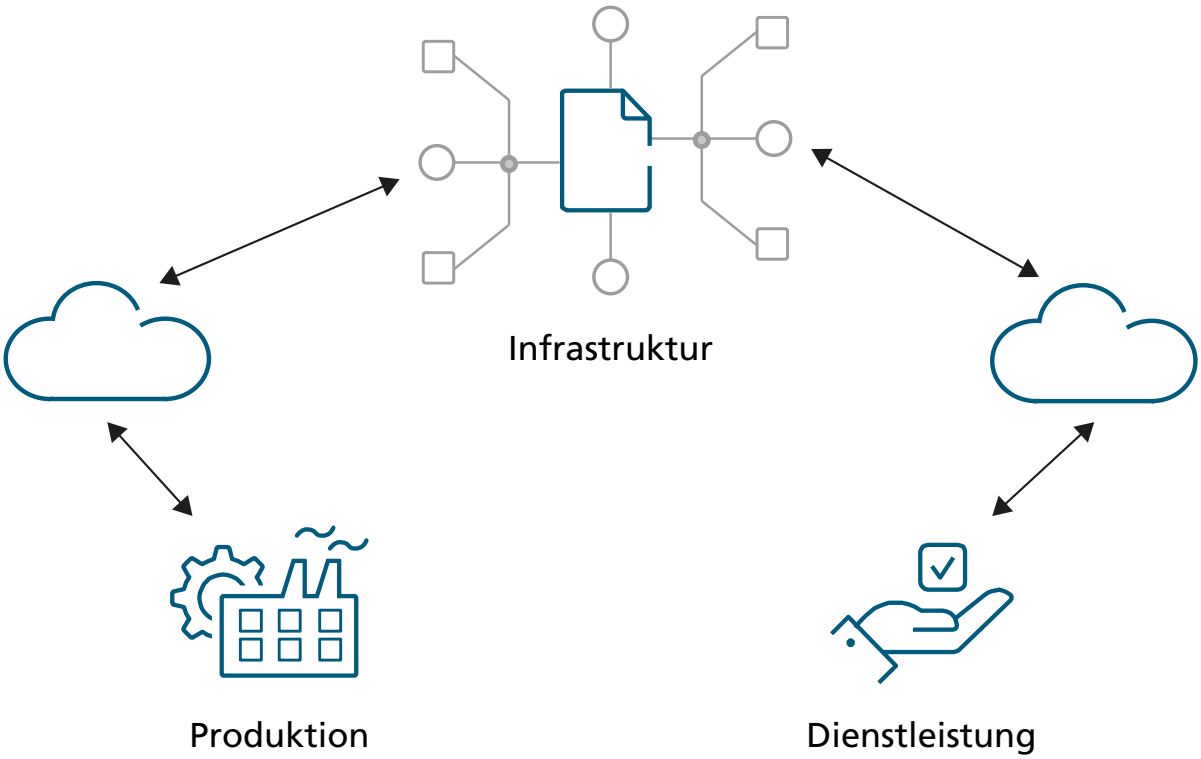


Abbildung 4.1: Architektur der unternehmensübergreifenden Datenübertragung

Datensicherheit spielt für alle Teilnehmer einer Infrastruktur eine zentrale Rolle und muss daher auf allen Subebenen adressiert werden. Da die Datensicherheit aufgrund des wachsenden Wertes von Daten immer wichtiger wird, muss dies auch insbesondere bei unternehmensübergreifendem Datenaustausch, aufgrund der größeren Angriffsmöglichkeiten, adressiert werden. Dies bildet in der Folge die Grundlage für eine vertrauensvolle Co-Produktion. Der Startpunkt ist dabei bereits die Datenübertragung von zum Beispiel einer Produktionsmaschine in eine Cloud. Daran anschließend muss eine sichere Verbindung von der jeweiligen Cloud zur Infrastruktur geschaffen werden. Diese wiederum muss eine sichere Verbindung zum Beispiel an die Cloud eines Dienstleisters (siehe Abbildung 4.1) herstellen. Hierbei ist nicht nur die **Sicherheit der jeweiligen Verbindungen** beziehungsweise Schnittstellen relevant, sondern auch die **generelle Absicherung der Komponenten** gegen unbefugten Zugriff und Manipulation.
Daraus ergeben sich verschiedene Anforderungen für die verschiedenen Bereiche entlang dieser Co-Produktionskette, welche zur Sicherstellung der Datensicherheit erfüllt werden müssen. Angelehnt an Manogaran und Chang bedarf es verschiedener Sicherheitsvorkehrungen aufgrund der verschiedenen Angriffspunkte der Subebenen innerhalb des Datenaustausches über eine Infrastruktur:[7,8]

Tabelle 4.1: Darstellung der verschiedenen Sicherheitsbedrohungen & Lösungen der verschiedenen Ebenen für einen sicheren unternehmensübergreifenden Datenaustausch in Anlehnung an Manogaran et al. (2017) und Chang et al. (2015) [7,8]

Komponenten Ebene	Schwachstellen	Arten von Bedrohungen und Angriffen	Sicherheitsanforderungen und Lösungen
Physisches Objekt (z.B. Produktionsmaschine mit Edge Device)	■ Begrenzte Kommunikation ■ Berechnungs- und Speicherressourcen ■ In verschiedenen Regionen verteilt	■ DoS/DDoS-Angriffe ■ Physische Angriffe ■ Integration von WSNs ■ Einbindung von RFID ■ Unbefugte Zugangskontrolle und Datenzugriff	■ Verschlüsselung / Kryptographie Techniken ■ Scannen der Prozesse auf Unstimmigkeiten ■ Authentifizierung ■ Autorisierung ■ Zugangskontrolle ■ Identifizierung durch Identitätsmanagement
Cloud / Server	■ Datenabdeckung ■ Cloud Computing ■ Sicherheitsfragen in Webanwendungen ■ Sichere Kommunikation	■ DoS ■ XSS-Angriff ■ CSRF-Angriff ■ SQL-Einschleusung ■ Schutz der Daten ■ Datenzugriff ■ PHRs Angriffe ■ Böswilliger Benutzer ■ Gemeinsame Nutzung verschiedener Umgebungen ■ Echtzeitverarbeitung ■ Gemeinsame Nutzung durch mehrere Anwendungen	■ Datentrennung (Informationsinhalt / -quelle) ■ Verschlüsselung / Entschlüsselung ■ Sicherer Datenzugriff ■ Vertraulichkeit der Daten ■ Plan zur Datensicherung, verteilte Datenbank-Technologie ■ Zeitplanung für Zugriff ■ Identifizierung ■ Authentifizierung ■ Firewall und Antivirus ■ Erkennung von Eindringlingen ■ Sicherheitsprotokolle ■ Isolierter Benutzerspeicher
Infrastruktur	■ Dynamisches Netzwerk ■ Infrastruktur ■ Probleme mit der Stromversorgung ■ Netzwerkprobleme ■ Auswahl der Sicherheitstechnik und ihre Herausforderungen Technik und ihre Herausforderungen	■ Drahtloses WAN ■ Kommunikation ■ Drahtlos LAN / PAN ■ Kommunikation ■ Sichere IoT ■ Kommunikation ■ Protokolle in ■ eingeschränkten ■ Ressourcen ■ Umgebung ■ Sichere Übertragung von Daten	■ Sicherheitsalgorithmus und -protokolle der Verbindungen ■ Verschlüsselung / Entschlüsselung mit z.B. zero-knowledge system ■ Starke Authentifizierung ■ Backup-Lösung ■ IoT-Kommunikationsprotokolle ■ Autorisierter Zugriff und Verfügbarkeit

Im Folgenden fokussieren wir uns in Bezug auf die Datensicherheit auf der Stufe der Infrastruktur des unternehmensübergreifenden Datenaustausches. Hierbei greifen wir auf die definierten Standards des Gaia-X als sichere und vertrauenswürdige europäische Dateninfrastruktur zurück, als auch auf die International Data Spaces (IDS) zur Gewährleistung eines interoperablen, sicheren und souveränen Datenaustausch.

Gaia-X ist eine europäische Initiative, die eine **Softwarearchitektur für Kontrolle und Governance** entwickelt, um diese auf Basis von europäischen Werten Richtlinien und Regeln zu implementieren. Diese Softwarearchitektur kann hierbei auf jeden bestehenden Cloud- / Edge-Technologie-Stack angewendet werden. Dies schafft Transparenz, Kontrollierbarkeit, Portabilität und Interoperabilität von Daten und Diensten. Dieses Framework soll auf jeder bestehenden Cloud-Plattform eingesetzt werden, die sich für den Gaia-X-Standard entscheidet.[8]

Die **International Data Spaces** haben das Ziel der Schaffung eines **globalen Standards für sichere und vertrauenswürdige Datenräume**. Auf Basis dieses Standards wird in der Folge ein sicherer, interoperabler und souveräner, unternehmensübergreifender Datenaustausch ermöglicht. Hierfür hat die IDS Initiative eine Referenzarchitektur für einen formalen Standard zur Erstellung von Datenräumen geschaffen. Diese IDS Architektur gewährleistet die digitale Souveränität der Dateneigentümer und erleichtert die gemeinsame Nutzung von Daten und deren Austausch. Somit bildet dies die Grundlage für die vereinfachte Entwicklung intelligenter unternehmensübergreifender Dienstleistungen anhand des definierten IDS Standards.[9]

Gaia-X und IDS arbeiten dabei nicht an konkurrierenden oder sich ausschließenden Standards, sondern sind kompatibel, beziehungsweise agieren ergänzend. Die Verbindung zwischen Gaia-X und IDS besteht dabei darin, dass die **IDS die Basis für den Datenaustausch in der Gaia-X-Infrastruktur** darstellen. Das genaue Zusammenspiel zwischen Gaia-X-Infrastruktur und IDS Anwendungen ist in der folgenden Abbildung dargestellt:[10]

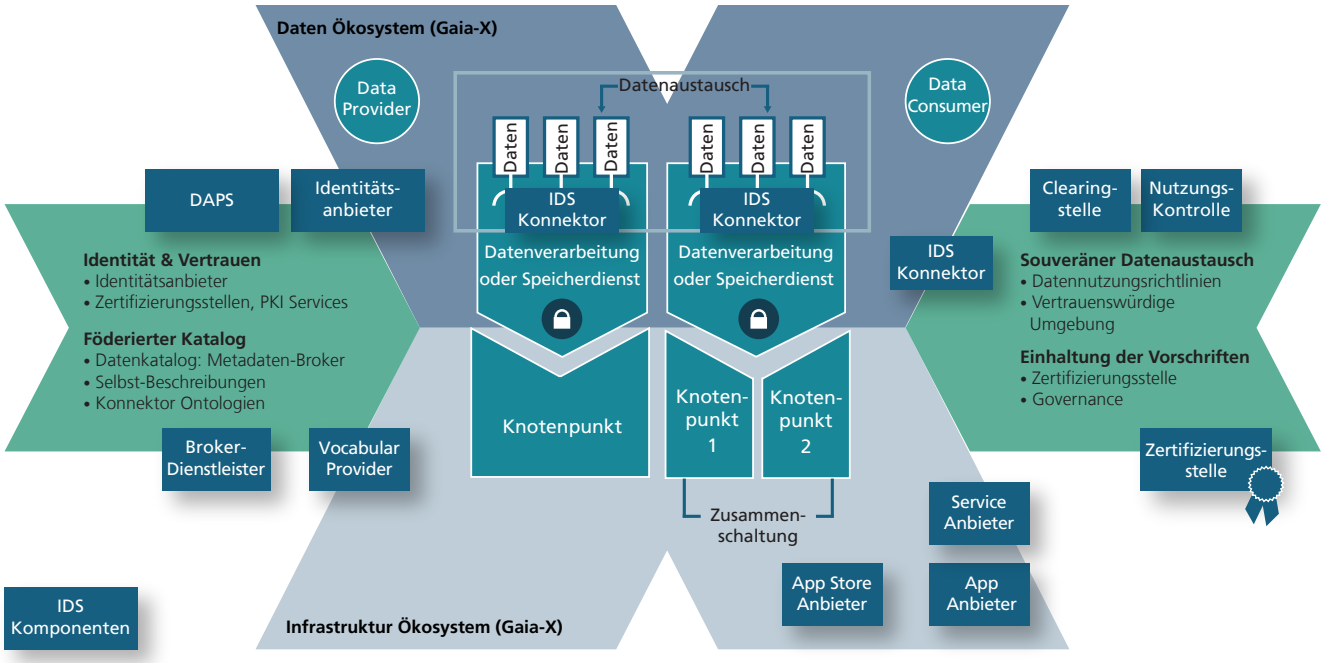


Abbildung 4.2: Integration und Zusammenspiel von IDS und Gaia-X (eigene Darstellung in Anlehnung an Otto et al. 2021) [11]

International Data Spaces

Die IDS Referenzarchitektur enthält eine Sicherheitsarchitektur für den unternehmensübergreifenden Datenaustausch. Diese Architektur ist unterteilt in sieben Dimensionen:[12]

Sichere Kommunikation

Die erste Dimension besteht aus der **sicheren Kommunikation**, welche innerhalb des IDS mittels Punkt-zu-Punkt-Verschlüsselung und Ende-zu-Ende-Autorisierung gewährleistet wird. Hierzu kommunizieren IDS Konnektoren über einen verschlüsselten Tunnel und können mittels geeigneten Protokolls die Kommunikation darstellen (z.B. IDSCP, https, mqtt). Das **Protokoll** unterstützt und ermöglicht mehrere Kommunikationsaspekte, darunter Identifizierung und Authentifizierung, Fernbescheinigungen, Austausch von Metadaten und Datenaustausch mit angehängten Nutzungsbestimmungen.[12]

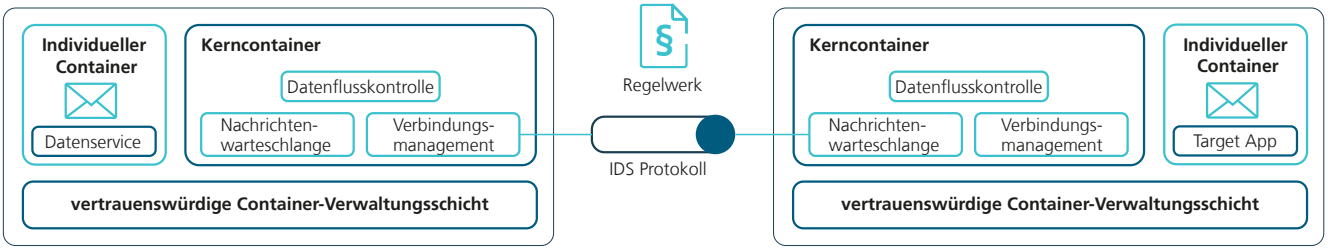


Abbildung 4.3: IDS Kommunikation (eigene Darstellung in Anlehnung an Otto et al. 2019) [12]

Identitätsmanagement

Die zweite Dimension stellt das **Identitätsmanagement** dar. Hierbei geht es im ersten Schritt um die Identifizierung durch das Präsentieren einer digitalen Identität. Daran anknüpfend beginnt die Authentifizierung der präsentierten Identität, sodass sichergestellt wird, dass die Identität verifiziert ist. Abschließend erfolgt der Schritt der Autorisierung, wobei eine Zugriffsentscheidung auf Basis der verifizierten Identität entschieden wird. Dieser Identitätsmanagementprozess als Teil der Datensicherheitsarchitektur wird orchestriert durch eine **Zertifizierungsstelle**, welche die benötigten **Zertifikate zur Authentifizierung und Verschlüsselung** zwischen den Konnektoren bereitstellt. Darüber hinaus enthält die IDS Architektur einen Dynamic Attribute Provisioning Service (DAPS) (Nähere Erläuterungen zu den Prozessen und Spezifikationen finden sich im Referenzarchitekturmodell des IDS). Dieser wird verwendet, um dynamische, aktuelle Attributinformationen über Teilnehmer und Konnektoren bereitzustellen.[12]

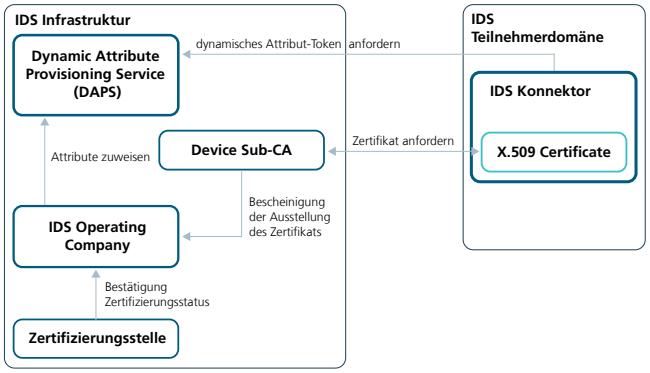


Abbildung 4.4: Einbetten des Konnektor-Zertifikats (eigene Darstellung in Anlehnung an Otto et al. 2019) [12]

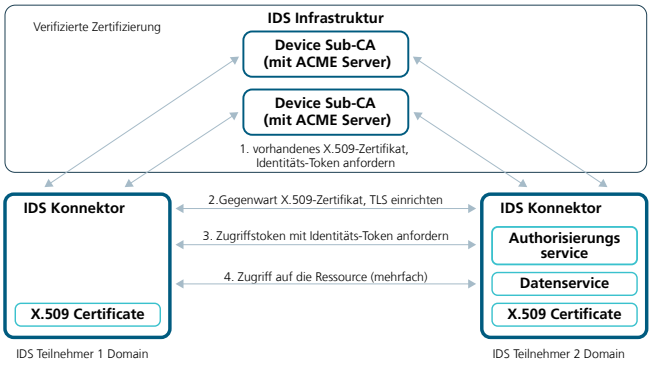


Abbildung 4.5: Arbeitsablauf beim Ressourcenzugang (eigene Darstellung in Anlehnung an Otto et al. 2019) [12]

Vertrauensmanagement

Die dritte Dimension der Sicherheitsarchitektur der IDS ist das **Vertrauensmanagement mittels kryptografischer Methoden** (z.B. Public Key-Infrastruktur (PKI)). Dadurch wird eine Hierarchie geschaffen, wobei der Identitätsanbieter an der Spitze, Zertifikate an die anderen Einheiten ausstellt, die wiederum ihrerseits Zertifikate an andere Einheiten ausstellen können.[12]

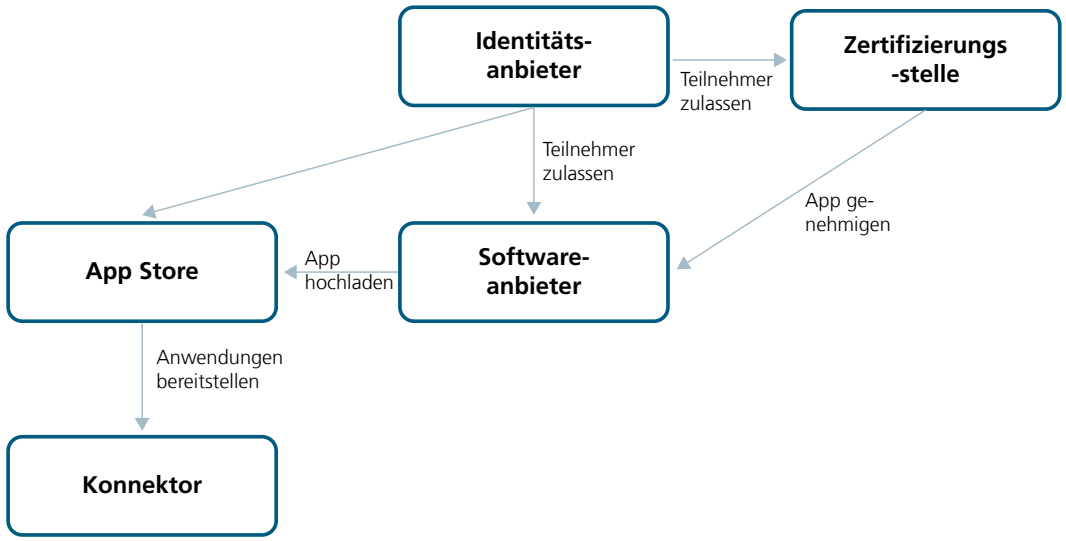


Abbildung 4.6: Technische Rollen in den International Data Spaces (eigene Darstellung in Anlehnung an Otto et al. 2019) [12]

Vertrauenswürdige Plattform

Im IDS gibt es mehrere Erscheinungsformen der Konnektor-Architektur und somit bedarf es weiterer Anforderungen zur Sicherstellung einer **vertrauenswürdigen Plattform**. Hierzu wurden drei Anforderungen in den International Data Spaces definiert. Zunächst muss ein gemeinsames Verständnis über die Sicherheitsprofile der anderen Teilnehmer geschaffen werden, um den Datenaustausch entsprechend zu gestalten. Zudem ist eine **Systemintegrität** zu gewährleisten, welche eine starke Isolierung der Komponenten notwendig macht. Des Weiteren ist für einen vertrauenswürdigen Datenaustausch eine **Remote-Integritätsverifizierung** erforderlich, womit Eigenschaften beziehungsweise explizit die Hard- und Software des Konnektors überprüft werden können.[12]

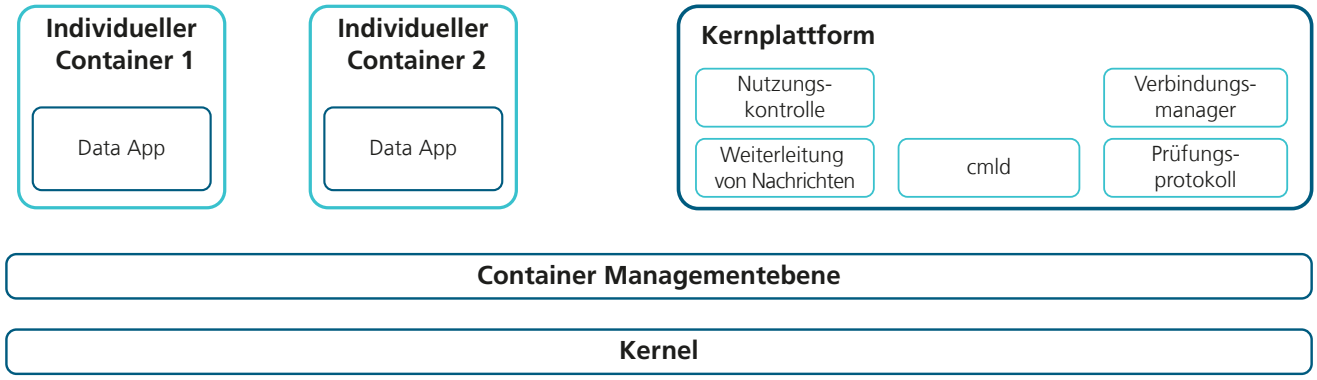


Abbildung 4.7: Container-Isolierung für Datenanwendungen (eigene Darstellung in Anlehnung an Otto et al. 2019) [12]

Datenzugangskontrolle

Die fünfte Dimension der Datensicherheit im IDS beschreibt die **Zugangskontrolle** zu Ressourcen. Hierbei gibt es verschiedene Modelle, welche verwendet werden können. Der **XACML** (eXtensible Access Control Markup Language) Standard44 wird hierbei am häufigsten verwendet. Die Hauptbausteine sind dabei Subjekt (z.B. ein Benutzer), Aktion (z. B. lesen, schreiben), Ressource (Datenbestand) und Umgebung (z.B., Zeit, Ort).[12]

Kontrolle der Datennutzung

Die **Kontrolle der Datennutzung** bildet die sechste Dimension der Datensicherheit im IDS dar. Diese kann durch einen maschinenlesbaren Vertrag, dessen Erfüllung von einer Partei erwartet wird, implementiert werden. Zudem existiert die Möglichkeit, die Verwendung von **Daten in verschiedenen Systemen zu verfolgen** und Beweise für die Verletzung von vereinbarter Nutzungsbeschränkungen zu sammeln. Vor diesem Hintergrund reichen die Lösungen von organisatorischen Regeln oder **rechtlichen Verträgen bis hin zu technischen Möglichkeiten zur Durchsetzung von Nutzungsbeschränkungen**. Der Schwerpunkt der IDS Referenzarchitektur liegt dabei auf der technischen Durchsetzung von Nutzungsregeln. Zu diesem Zweck müssen Datenverwendungsbeschränkungen durchgesetzt werden, welche Aktionen eines Systems überwachen und möglicherweise von Kontrollpunkten (d.h. Policy Enforcement Points, PEPs) abgefangen werden. Diese Aktionen müssen von einer Entscheidungsmaschine (d.h. einem Policy Decision Point, PDP) bewertet werden, um eine Genehmigung oder Verweigerung zu beantragen.[11]

Verfolgung der Datenherkunft

Die Verfolgung der Datenherkunft als siebte Dimension der Datensicherheit im IDS ermöglicht herauszufinden, wann, wie und von wem Daten verändert wurden und welche anderen Daten den Prozess der Erstellung neuer Daten beeinflusst haben. Der Schwerpunkt der **Datenherkunft** liegt hierbei auf **Transparenz und Verantwortlichkeit**. Dabei werden Datenherkunftsinformationen über ein Privacy Dashboard abgefragt, welches über eine Clearingstelle zugänglich ist. Hierbei gibt es zwei Optionen für die **Speicherung von Informationen zur Datenherkunft**. Zunächst einmal die **zentralisierte**, bei der ein Provenance Storage Point (ProSP) mit der Clearingstelle verbunden ist. Die zweite Option ist eine **verteilte Architektur**, wobei jeder Konnektor mit einem ProSP ausgestattet ist, sodass er direkt mit der Datenflussverfolgungskomponente verbunden ist.[12]

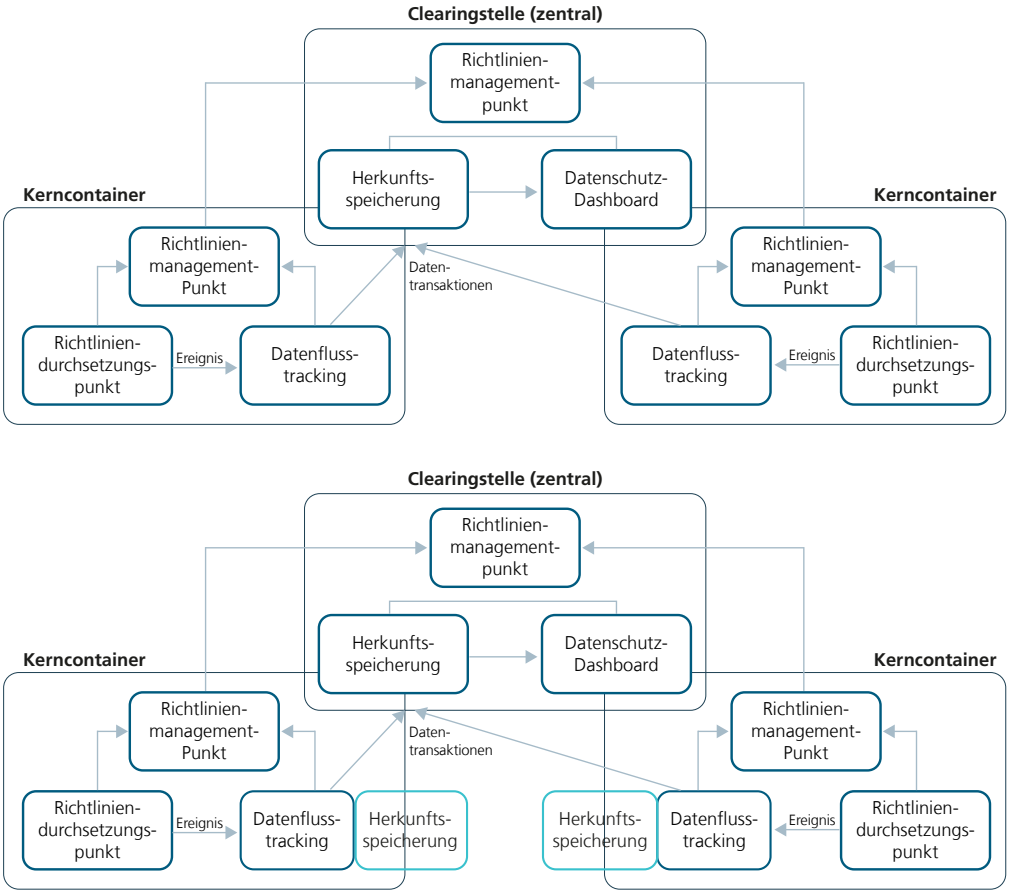


Abbildung 4.8: Kommunikationsinfrastruktur für Nutzungskontrolle und Herkunftskomponente [12]

Sicherheitsprofile im IDS

Im IDS gibt es vier verschiedene Sicherheitsprofile: freie Basis, Basis, Vertrauen und Vertrauen+. Das erste Sicherheitsprofil stellt die Basislösung dar, diese ermöglicht die Verwendung von IDS Konzepten und Technologien außerhalb des vertrauenswürdigen Ökosystems. Die zweite Stufe heißt Basis-Sicherheitsprofil und definiert die Mechanismen, die für ein Mindestmaß an Vertrauen, einschließlich des Zertifizierungsprozess benötigt werden, sodass im IDS Ökosystem unternehmensübergreifend interoperable, sicher und souverän Daten ausgetauscht werden können. Das Sicherheitsprofil Vertrauen definiert über das Sicherheitsprofil Basis hinausgehende Sicherheitseigenschaften. Das letzte Sicherheitsprofil Vertrauen+ stützt sich auf vertrauenswürdige Hardware auf der Basis von TPM und stellt damit die höchste Sicherheitsstufe im IDS dar.[12]

Tabelle 4.2: Überblick über die IDS Sicherheitsprofile und die damit verbundenen Dimensionen (eigene Darstellung in Anlehnung an Otto et al. 2019) [12]

	Freie Basis	**Basis**	**Vertrauen**	**Vertrauen+**
Entwicklung	Entwicklung als Open Source	Entwicklung in der IDSA Gemeinschaft	Entwicklung in der IDSA Gemeinschaft	Entwicklung in der IDSA Gemeinschaft und an strenge SLA bezüglich Sicherheitsupdates gebunden
Unterstützte IDS Rollen	Nicht zertifiziert, hierfür ist die öffentliche IDS Infrastruktur nicht verfügbar	Alle IDS Rollen werden unterstützt aber das Clearing House ist optional	Alle IDS Rollen werden unterstützt	Alle IDS Rollen werden unterstützt
Unterstützte Kommunikationsfähigkeiten	Keine Verbindung zu öffentlichen IDS Diensten oder Konnektoren herstellbar	Keine Verbindung zu anderen Konnektoren und Datenaustausch.	können mit anderen Konnektoren verbunden werden und Daten austauschen. Kann eine Verbindung mit einem Konnektor mit Basisprofil ablehnen.	können mit anderen Konnektoren verbunden werden und Daten austauschen. Kann eine Verbindung mit einem Konnektor mit Basisprofil ablehnen.
Höhere Sicherheitsmerkmale	Sicherheitslevel nicht definiert	Standard Sicherheitslevel	Erweitertes Sicherheitslevel	Hohes Sicherheitslevel

Gaia-X

Gaia-X als Vertrauensinfrastruktur nutzt die IDS Komponenten als Bestandteil für den sicheren und souveränen Datenaustausch. Über die vom IDS definierten Sicherheitsmechanismen hinweg, wird mit Labels in Gaia-X gearbeitet, welche Spezifikationen untern anderem über Sicherheitsmechanismen in drei verschiedenen Levels definiert. Hierbei stellt das „Label Level 1" die Grundbasis für die Datensicherheitsanforderungen dar und das „Label Level 3" stellt den höchsten Standard dar. [11,13]

Das **Label Level 1** definiert Vorgaben zum Datenschutz, Transparenz, Sicherheit, Übertragbarkeit und Flexibilität, zudem ist die Einhaltung von Regeln des „Gaia-X Policy Rules Document" die Grundlage zum Erhalt dieses Labels. Die Spezifikationen zu den „Gaia-X Policy Rules" sind Teil des Gaia-X Architektur Dokuments und die Vorgaben zur Datensicherheit auf dieser Ebene stammen von dem **Europäischen Cybersicherheitschema – Basis Level der ENISA**, welches zur Erfüllung implementiert werden muss. [11,13]

Das **Label Level 2** erweitert die grundlegenden Anforderungen des Label Level 1 und spiegelt ein höheres Sicherheitsniveau wider, Transparenz der anwendbaren rechtlichen Vorschriften und potenziellen Abhängigkeiten wir dabei zusätzlich adressiert. Zudem muss dem Kunden die Möglichkeit eines Dienstleistungsstandorts in Europa geboten werden. In Bezug auf die Cybersicherheit bestehen die Mindestanforderungen aus dem **ENISA Europäischen Cybersicherheitsschema -Substantielles Niveau.**[11,13]

Das **Label Level 3** zielt auf die höchsten Standards für Datenschutz, Sicherheit, Transparenz, Übertragbarkeit und Flexibilität sowie der europäischen Kontrolle. Es erweitert die Anforderungen der Stufen 1 und 2 mit Kriterien, die die Immunität gegen außereuropäischen Zugang und ein hohes Maß an Kontrolle über die Anbieterbindung voraussetzt. Ein Dienststandort ist hierbei in Europa obligatorisch. Für die Cybersicherheit ist die Mindestanforderung die Erfüllung des **Europäischen Cybersicherheitsschemas – Hohes Level von ENISA**.[11,13]

Darüberhinausgehend werden innerhalb der Gaia-X Initiative zum aktuellen Zeitpunkt an Föderationsdiensten gearbeitet, welche Grundlagenapplikationen zur Umsetzung der Gaia-X Infrastruktur darstellen und somit auch datensicherheitstechnische Implikationen generieren.[14]

Das erste Arbeitspaket stellt dabei **Identitäts- und Vertrauensdienste** dar, welche zur Authentifikation der Teilnehmer genutzt werden und die Kontrolle über die digitale Identität mittels Identitätsprüfungen und verschiedener Identitätsmanagement Ansätze gewährleisten soll. **Föderierte Katalogdienste** stellen das zweite Arbeitspaket der Föderationsdienstleistungen dar. Diese Dienste bestehen aus der Möglichkeit der Selbstbeschreibungen der einzelnen Teilnehmer einer Föderation. Hierbei werden explizit Daten zu Anbietern und ihren Angeboten aus den Selbstbeschreibungen hinterlegt. Das Arbeitspaket zum **souveränem Datenaustausch** basiert auf Mechanismen der Transparenz und der Kontrolle, wie und von wem die Daten in welchem Kontext verwendet werden. Dazu stellen digitale Vertragsverhandlungen, Validierungen und Überwachungen die Basis für diese Föderation und ermöglichen den Aufbau von Vertrauen. Das vierte Arbeitspaket befasst sich mit Verfahren zur **Bewertung von Regelkonformität**. Dabei handelt es sich um eine vorab Überprüfung bei der Aufnahme eines Angebots eines Unternehmens. Hierbei wird entsprechend mittels Evaluation des Angebots überprüft, ob die Regeln eingehalten werden und das Angebot entsprechend in der Föderation verfügbar gemacht werden kann. Das Gaia-X Konformitätswerk bestimmt dazu die Kriterien zur Regelkonformität. Zusätzlich zu den Arbeitspaketen dient das Portal als zentrales Beispiel für einen digitalen Zugang. **Das Portal** soll dazu den Startpunkt zu nutzerfreundlichen Diensten, Aufnahmeverfahren und Akkreditierung von Teilnehmern darstellen.[14]

Datensicherheit im SealedServices Ökosystem

4.1 Geschäftsstrategie

In der Geschäftsstrategie spielt die Datensicherheit für die beteiligten Unternehmen als auch die Infrastruktur im unternehmensübergreifenden Datenaustausch eine zentrale Rolle. Dies muss bereits auf der Subebene der Ziele adressiert werden, um „by-design" eine bestmögliche Architektur zur Datensicherheit zu schaffen. Somit muss bei der Geschäftsvision bereits eine fundierte Sicherheitsarchitektur inkludiert werden. In Hinblick auf wirtschaftliche und strategische Ziele spielt dies auch eine wichtige Rolle, in diesem Fall geht es jedoch primär um die Umsetzbarkeit und damit der Überwindung technischer Hürden um größtmögliche Datensicherheit sicherzustellen. Konkret bedeutet dies, dass Unternehmen eine entsprechende **Datensicherheitsstrategie** entwickeln müssen, um einen sicheren Datenaustausch zu gewährleisten. Hierbei kann auf Subebene des unternehmensübergreifenden Datenaustausches zum Beispiel mit **IDS Komponenten** gearbeitet werden, welche sicherstellen, dass ein interoperabler, sicherer und souveräner Datenaustausch, beispielsweise in einer Co-Produktion, etabliert wird. Die SealedServices Infrastruktur kann hierbei, angelehnt an **Gaia-X mit den verschiedenen Labels zu Transparenz und Sicherheit**, einen grundlegenden Standard zum Datenaustausch schaffen.

Auf Subebene der Co-Creation stellt die Datensicherheit auch eine wichtige Rolle dar, da durch den externen Zugriff auf Daten bzw. den Austausch von Daten über die SealedServices Infrastruktur ein **erhöhtes Sicherheitsrisiko durch Schnittstellen** geschaffen wird. Bei der Festlegung der Akteure innerhalb einer Co-Creation ist hierbei eine Definition der beteiligten Firmen, Abbildung der Datenflüsse und eine **Definition der Datensicherheitsmechanismen der Datenflüsse** essenziell. Hierbei kann auf die Standards von Gaia-X und IDS zurückgegriffen werden, um Datensicherheit, Transparenz und Souveränität im Datenaustausch entlang der Wertschöpfungskette zu gewährleisten. Auf den Subebenen der Maschinen der Unternehmen, der Cloud-Systeme der Unternehmen und der Infrastruktur der SealedServices kann auch auf die Tabelle 4.2 zurückgegriffen werden. In Bezug auf Datensicherheitslösungen werden darin Sicherheitsmaßnahmen innerhalb der einzelnen Subebenen (Maschine, Cloud, Infrastruktur) benannt.

In der Untersuchung des Marktumfeldes, welche die dritte Subebene darstellt, spielt im Gegensatz zu den anderen Subebenen der Geschäftsstrategie die Datensicherheit nur eine untergeordnete Rolle. Dies trifft insbesondere zu, wenn es sich um die Nutzung frei verfügbarer Daten handelt. Hingegen bei der Nutzung nicht frei verfügbarer Daten durch die Nutzung der SealedServices Infrastruktur zum Austausch von Daten mit benachbarten Sektoren, ist die Datensicherheit von besonderer Relevanz durch den möglichen Austausch sensibler Daten. Hierbei ist zwischen den jeweiligen beteiligten Unternehmen ein **einheitlicher Minimalstandard zur Datensicherheit** zu definieren, um Vertrauen zu generieren. Dabei ist, wie bei den anderen Subebenen, die Implementierung des IDS Standards zum sicheren und souveränen Datenaustausches denkbar, insbesondere da dieser Standard sektorenübergreifend angewendet wird und somit das nötige Vertrauen bereits in vielen Sektoren vorhanden ist. Dies würde zudem ermöglichen, dass die SealedServices Infrastruktur – angelehnt an Gaia-X – keine Spezifizierungen bei sektorübergreifendem Datenaustausch adaptieren müsste.

Ein produzierendes Unternehmen kann in der SealedServices Infrastruktur auf Basis von IDS und Gaia-X mit einem Dienstleistungsunternehmen entlang der Wertschöpfungskette Daten interoperabel, sicher und souverän austauschen. Die jeweilige Sicherheitsstufe, anhand von IDS und Gaia-X, kann hierbei von den beteiligten Unternehmen im Austausch frei definiert werden.

4.2 Geschäftsprozess

Im Geschäftsprozess ist die Datensicherheit allgegenwärtig, da diese auf allen Subebenen berücksichtigt bzw. sichergestellt werden muss. Auf der ersten Subebene im Kallenberg-Prozess wird dies bereits im ersten Schritt der Ermittlung des Leistungsbedarfes sichtbar, sodass Unternehmen die entsprechenden Marktdaten analysiert haben und somit Leistungsbedarf und Angebotslücken bestimmt haben.[4] Diese Daten vor externem bzw. unbefugtem Zugriff zu schützen und diesen Informationsvorteil in den folgenden Schritten des Prozesses zu nutzen, ist hierbei die Kernaufgabe. Um insbesondere unternehmensübergreifend Daten auszutauschen, ist **Vertrauen eines der wichtigsten Güter**. Daher ist bei der Datensicherheit primär auf bestehende Marktstandards zurückzugreifen, worauf die beteiligen Unternehmen bereits vertrauen. Hierbei kann beispielsweise für den Austausch von Marktdaten zum Leistungsbedarf mittels IDS Technologie sichergestellt werden, dass die ausgetauschten Daten nur für diesen Schritt im Prozess verwendet werden können. Gleiches gilt für das Vertrauen in die Infrastruktur, welche die Verbindung zwischen den beteiligten Unternehmen herstellt. Hierbei lässt sich auf die Architektur von Gaia-X zurückgreifen, um die Basis für Vertrauen auch in die Infrastruktur herzustellen.

Auch auf der zweiten Subebene der Geschäftsprozessebene, der Differenzierung zwischen datenbasierten und physischen SealedServices, geht es um die Wahrung der Sicherheit der erhobenen Daten. Dies betrifft insbesondere die Bausteine, die die SealedServices Infrastruktur zur Verfügung stellt und inwieweit diese Vorkehrungen zur Datensicherheit beinhalten. Hierbei ist eine Klarstellung über den genauen Ablauf der Nutzung der Daten und wie die daraus gewonnenen Informationen behandelt werden, notwendig. Auch hier wäre eine **Zertifizierung der Komponente**, zum Beispiel mit der Erfüllung der Zertifizierungskriterien des IDS, ein Weg, Vertrauen zu gewinnen. Alternativ bzw. darüber hinaus können weitere Maßnahmen, wie in der Tabelle 4.2 dargestellt, die Sicherheit und das Vertrauen der Unternehmen aufbauen.

Im Fall des Matching Verfahrens ist Datensicherheit essenziell, damit Unternehmen Daten für diesen Prozess bereitstellen. Da hierbei von allen beteiligten Akteuren sensible Daten der Infrastruktur für diesen Prozess bereitgestellt werden, muss hierbei für alle ein adäquater Datenschutz gewährleistet werden, um das Vertrauen zu gewinnen und zu erhalten. Der grundlegende Datenschutz kann hierbei mit den genannten Maßnahmen aus der Tabelle 4.2 dargestellt werden und insbesondere der Aspekt der **Souveränität der eigenen Daten** ist mittels IDS Technologie umsetzbar. Somit kann sichergestellt werden, dass die Daten nicht weiterversendet werden und beispielsweise bei der Konkurrenz oder beim Kunden direkt ohne das Einverständnis aufgerufen werden können.

4.3 Informationstechnologie

In der Informationstechnologie ist die Datensicherheit ein fester Bestandteil und bietet die Grundlage für die betrieblichen Aktivitäten, insbesondere im Falle unternehmensübergreifender Wertschöpfung.

Datensicherheit ist auf Subebene der Plattformsicherheit in verschiedenen Facetten relevant. Zunächst für den Marktplatz, hier ist relevant, dass auf Subebene der Plattform Daten zu Kontaktpersonen etc. geschützt werden. Zudem müssen Vorkehrungen getroffen werden, sodass ein Missbrauch von Anfragen, um beispielsweise Leerlaufzeiten bei Anbieter herauszufinden und damit den Preis zu senken, zu unterbinden. Darüber hinaus muss Datensicherheit auch in der Dimension des App Stores adressiert werden. In diesem Fall müssen **Applikationen entsprechend ihrer Datensicherheit klassifiziert** werden und Transparenz über die Analyseergebnisse der Applikationen im App Store geschaffen werden, um ein ganzheitliches Vertrauen in die SealedServices Infrastruktur zu schaffen.

Die zweite Subebene befasst sich mit der Plattformsicherheit. Hier kann wiederum auf IDS und Gaia-X zurückgegriffen werden, um **transparent die Methoden** zur Sicherstellung der Interoperabilität, Souveränität und Datensicherheit darzustellen. Darüber hinaus können Technologien aus der Tabelle 4.2 implementiert werden, um die Datensicherheit zu gewährleisten.

Die Subebene der Datenhaltung betrifft sowohl die SealedServices Infrastruktur als auch die teilnehmenden Unternehmen. Hierbei muss, wie bereits dargestellt, **mit Technologien der Datensicherheit Vertrauen zwischen allen Akteuren** geschaffen werden. Hierbei kann bei den einzelnen Unternehmen auf Basis des Multi-Cloud Ansatzes mit IDS Konnektoren eine interoperable, sichere und souveräne Datenhaltung geschaffen werden und gleichzeitig die Verfügbarkeit für unternehmensübergreifenden Datenaustausch beibehalten werden. Analog ist dies auf Subebene der Infrastruktur durch eine Anlehnung an das Gaia-X Konzept möglich.

Ein Unternehmen, welches physische Dienstleistungen an Anlagen anbietet, ist darauf angewiesen, die nötigen Daten für die Erbringung der Dienstleistungen vom Auftraggeber zu erhalten. Da es sich dabei um sensible Daten handeln kann, die somit technisch das Unternehmen verlassen, bietet dies aktuell eine Vielzahl an Angriffspunkten von außen. Die SealedServices Infrastruktur hingegen ermöglicht in diesem Fall nicht nur die vereinfachte Organisation des Datenaustausches, sondern hierbei kann auch auf Basis von IDS und Gaia-X ein sicherer und souveräner Datenaustausch gewährleistet werden.

5 Regulatorische Vorgaben

Die folgenden Abschnitte befassen sich mit den bereits umgesetzten oder in Ausarbeitung befindlichen Regularien der Europäischen Union und dem deutschen Lieferkettengesetz, welche die Grundregeln zum Umgang mit Daten definieren. Diese haben sowohl direkte als auch indirekte Auswirkungen für einen unternehmensübergreifenden Datenaustausch und die Co-Produktion von industriellen Dienstleistungen.

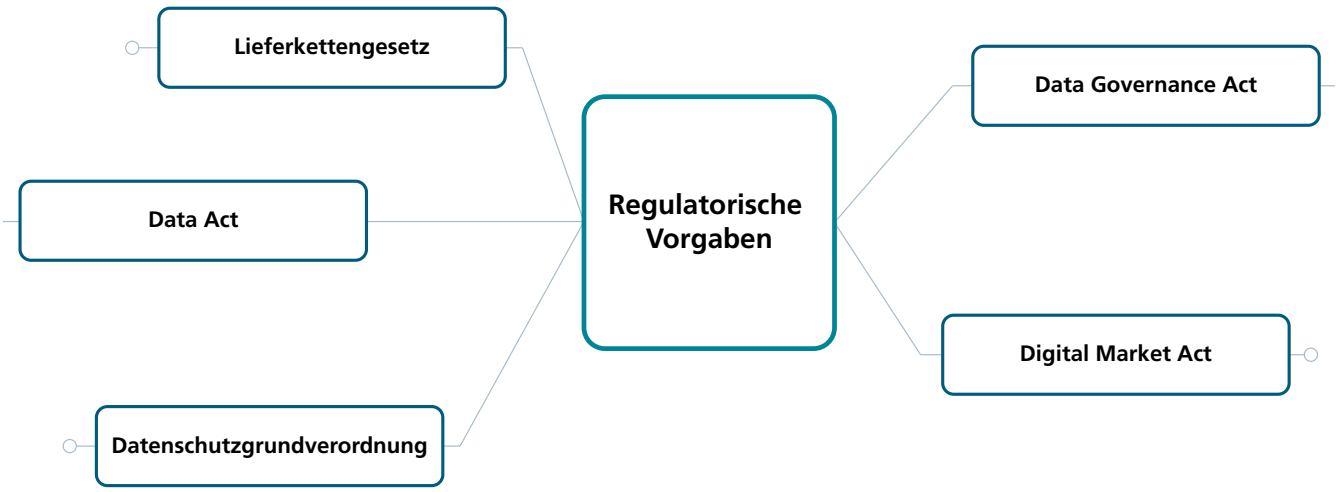


Abbildung 5.1: Auswahl der betrachteten regulatorischen Vorgaben

Data Governance Act

Der Data Governance Act befasst sich mit der **Weiterverwendung von Daten öffentlicher Stellen innerhalb der EU** für kommerzielle und nichtkommerzielle Zwecke. Darüber hinaus regelt dieses Gesetz die gemeinsame Nutzung von Daten zwischen verschiedenen Unternehmen durch Vermittlungsdienste und Datenkooperationen sowie die Förderung des Datenaltruismus durch registrierte datenaltruistische Organisationen. Diese neuen Vorschriften traten dabei zum 23.06.2022 in Kraft und sind ab dem 24.09.2023 anzuwenden. Für die genaue Umsetzung dieser Verordnung kann das von der Europäischen Kommission erarbeitete Vorschlagsdokument mit den spezifischen Rahmenbedingungen herangezogen werden.

Gesetz über digital Dienste (Digital Services Act)
Der Digital Services Act der EU beabsichtigt, die **Grundregeln für Anbieter digitaler Dienstleistungen** zu modernisieren und dabei eine Reihe neuer Sorgfaltspflichten für bestimmte Dienstleistungen einzuführen. Teil davon ist die Etablierung von Haftungs- und Sicherheitsvorschriften für digitale Plattformen, Dienste und Produkte. Dies betrifft jedoch nur große Anbieter direkt, welche mehr als 45 Millionen monatlich aktiven Nutzer in der Europäischen Union haben. Dies kann jedoch, durch von betroffenen Unternehmen in Anspruch genommene Dienstleistungen auch für kleinere Anbieter gegebenenfalls zu Änderungen führen. Bei dem Digital Services Act handelt es sich um eine Verordnung, welche zum 16.11.2022 in Kraft getreten ist und schrittweise bis zum 17.02.2024 umgesetzt werden muss. Für genauere Spezifikationen kann das von der Europäischen Kommission erarbeitete Vorschlagsdokument herangezogen werden.[16]

Gesetz über digitale Märkte (Digital Markets Act)
Der Digital Markets Act soll eine **Vorabregulierung für sogenannte »Gatekeeper«** der digitalen Wirtschaft darstellen (besonders mächtige Plattformunternehmen). Diese Regelung zielt ausschließlich auf die größten Plattformunternehmen ab, die in den letzten drei Geschäftsjahren einen Jahresumsatz von mindestens 7,5 Mrd. € in der Europäischen Union erzielt haben. Alternativ gilt diese Verordnung auch für Plattformunternehmen mit einer Marktkapitalisierung von mindestens 75 Mrd. € und monatlich mehr als 45 Mio. in der Europäischen Union ansässigen oder wohnhaften Endnutzern oder mehr als 10.000 in der Europäischen Union ansässigen gewerblichen Nutzern. Dies kann jedoch gegebenenfalls auch Effekte auf kleinere Infrastrukturen haben, wenn diese Dienstleistungen betroffener Unternehmen nutzen. Der Europäische Rat und das Europäische Parlament haben sich am 25.03.2022 auf eine finale Fassung des Digital Markets Acts vorläufig geeinigt. Diese Einigung wurde in der Folge am 01.11.2022 vom Europäischen Rat und vom Europäischen Parlament gebilligt. Die Verordnung tritt nun schrittweise bis 02.05.2023 in Kraft.[17,18]

Datenschutzgrundverordnung (DSGVO)
Die Datenschutzgrundverordnung ist eine Verordnung der Europäischen Union, welche die **Regeln für die Verarbeitung personenbezogener Daten** in der gesamten EU vereinheitlicht. Sie soll den Schutz personenbezogener Daten und den freien Datenverkehr innerhalb des europäischen Binnenmarktes gewährleisten. Sie ist auch in den Nicht-EU-Ländern des Europäischen Wirtschaftsraums (EWR) Island, Liechtenstein und Norwegen geltendes Recht und muss auch von Unternehmen außerhalb der EU beachtet werden, wenn sie ihre Dienstleistungen oder Produkte für EU-Bürger anbieten und deren Daten erheben oder verwenden. Die Datenschutzgrundverordnung ist seit dem 25. Mai 2018 in Kraft. Die genauen Regeln im Umgang mit Daten, in Hinblick auf die Datenschutzgrundverordnung, sind in der entsprechenden Verordnung des Europäischen Parlaments und Rates zu finden.[19,20]

Data Act
Der Data Act enthält **Regelungsvorschläge zur gemeinsamen Nutzung von Daten**, die möglicherweise neue Zugriffsrechte auf kommerziell sensible Daten schaffen. Zentrale Aspekte sind Austausch von Daten zwischen Unternehmen und Behörden im öffentlichen Interesse, Austausch von Daten zwischen Unternehmen und Werkzeuge für die gemeinsame Nutzung von Daten sowie intelligente Verträge.
Darüber hinaus befasst sich der Data Act mit der Klärung der **Rechte an nicht-personenbezogenen Internet-of-Things (IoT)-Daten**, die aus der beruflichen Nutzung stammen, Verbesserung der Portabilität für geschäftliche Nutzer, Ergänzung des Rechts auf Übertragbarkeit von Cloud-Diensten gemäß Artikel 20 DSGVO und **Rechte des geistigen Eigentums** zum Schutz von Datenbanken und Garantien für

nicht-personenbezogene Daten in internationalen Kontexten. Im Rahmen des letzten veröffentlichten Vorschlags wurde auch eine Bestimmung über das **Recht der Nutzer auf Zugang zu Daten**, die bei der Nutzung von Produkten oder Diensten erzeugt werden, hinzugefügt („Accessibility by Design«). Bei dem Data Act handelt es sich, wie bereits dargestellt, um einen Entwurf. Dieser wurde am 23.02.2022 vorgestellt und soll 2023 finalisiert werden. Aktuelle Spezifikationen dieses Vorschlages der Europäischen Kommission zum Data Acts können auf der Website der Europäischen Kommission gefunden werden.[21]

Lieferkettengesetz (Sorgfaltspflichtengesetz)

Aktuell planen sowohl die EU als auch Deutschland auf Landesebene ein Lieferkettengesetz. Bei dem Lieferkettengesetz der EU handelt es sich jedoch, im Gegensatz zu dem deutschen Vorhaben, bisher nur um einen Entwurf ohne finale Fassung und festen Einführungstermin. Daher liegt der Fokus im Folgenden auf dem deutschen Lieferkettengesetz.
Dieses sieht vor, dass Unternehmen ein **eigenes Risikomanagements** einrichten, um die **Risiken von Menschenrechtsverletzungen und Schädigungen der Umwelt zu identifizieren** und diese in der Folge vermeiden oder minimieren zu können. Hierbei gibt das Gesetz vor, welche Präventions- und Abhilfemaßahmen notwendig sind und verpflichtet Unternehmen zu regelmäßiger Berichterstattung. Zudem sind die entsprechenden Unternehmen verpflichtet ein Beschwerdeverfahren einzurichten.

Risikomanagement sowie Vorbeugungs- und Abhilfemaßnahmen sind zusätzliche Sorgfaltspflichten der Unternehmen. Diese Pflichten sind auf die eigene Geschäftstätigkeit, aber auch auf das Handeln eines Vertragspartners und das Handeln weiterer (indirekter) Lieferanten anzuwenden. Somit besteht die **Verantwortung der Unternehmen entlang der Lieferkette**. Hierbei ist jedoch hervorzuheben, dass diese Sorgfaltspflicht nur für den eigenen Geschäftsbereich und direkte Zulieferer gilt und die Sorgfaltspflicht bei allen dahinterliegenden Prozessen der Lieferkette abgestuft ist. Hierbei wird vorgegeben, dass im Falle vorgelagerter Zulieferer anlassbezogen bei „substanziierter Kenntnis über mögliche Rechtsverletzungen" gehandelt werden muss.

Das deutsche Lieferkettengesetz tritt schrittweise ab dem 1. Januar 2023 in Kraft und startet zunächst für Unternehmen mit mindestens 3.000 Mitarbeitern im Inland, ab 2024 auch für Unternehmen mit mindestens 1.000 Mitarbeitern im Inland. Die entsprechenden Unternehmen sind nach in Krafttreten des Gesetzes verpflichtet im ersten Schritt eine Risikoanalyse durchzuführen. Das bedeutet, dass Unternehmen sich zunächst um Transparenz bemühen müssen und die Teile ihrer Produktions- und Lieferkette identifizieren müssen, welche mit besonders hohen menschenrechtlichen und umweltbezogenen Risiken verbunden sind. Der genaue Wortlaut sowie die spezifischen Anforderungen an die Unternehmen durch das Lieferkettengesetz können auf der Website der deutschen Bundesregierung vorgefunden werden.[22]

Regulatorische Vorgaben im SealedServices Ökosystem

5.1 Geschäftsstrategie

Im Zusammenhang mit regulatorischen Vorgaben auf europäischer Subebene ergeben sich in der Ebene Geschäftsstrategie eine Vielzahl an Anknüpfungspunkten zur bereits frühzeitigen Einbeziehung dieser Vorgaben. Dies startet bereits auf der Subebene der Ziele. Hierbei muss von den Verantwortlichen bereits die Einhaltung der Regularien adressiert werden, um **frühzeitig eventuellen Konflikten entgegenzuwirken**. Im Fall der SealedServices Infrastruktur, welche sich insbesondere mit Daten im industriellen Business-to-Business (B2B) Umfeld befasst, ist die Datenschutzgrundverordnung (DSGVO) und der aktuelle Entwurf des Data Acts relevant. Die an der SealedServices Infrastruktur angeschlossenen Unternehmen sind dabei insbesondere in der Pflicht, da die Haftung für Verstöße beispielsweise bei einem unternehmensübergreifenden Datenaustausch von personenbezogenen Daten bei dem Datengeber liegt. Die Ziele der Unternehmen müssen daher dahingehend angepasst sein, dass diese sowohl bestehende Regularien, insbesondere die **DSGVO** aber auch kommende Regularien, wie den **Data Act**, berücksichtigen. Im Falle des Data Governance Act kann dies auch für Unternehmen von Interesse sein, die an der SealedServices Infrastruktur beteiligt sind. Allerdings nicht in Form einer Einschränkung, sondern in Form einer Möglichkeit von staatliche Institutionen, Daten zum Wohl der Allgemeinheit (für altruistische Zwecke) zu verwenden. Im Falle des Digital Services Acts, haben die Interoperabilitätsvorgaben für intermediärer Services, wie der SealedServices Infrastruktur aufgrund der aktuell begrenzten Größe keine Relevanz. Analog dazu ist auch der Digital Market Act nicht anwendbar, welcher Kernplattformanbieter die Besserstellung eigener Services gegenüber der von Serviceanbietern in der Plattform besserstellt. Hingegen sind auf der Subebene der Ziele und damit auf Subebene der Geschäftsführung neue rechtliche Vorgaben der Lieferkettenüberwachung zu berücksichtigen. Dazu müssen Risikoanalysen zur Einhaltung der Sozialstandards entlang der Lieferkette bis zur rechtlichen Durchsetzung, je nach Firmengröße, bis Anfang 2023 oder zu einem späteren Zeitpunkt geschaffen werden.

Auf der Subebene der Co-Creation sind, analog zu der Subebene Ziele, explizit die **DSGVO** und der **Data Act** zu berücksichtigen. Bei der Definition der Rollen innerhalb dieser gemeinsamen Wertschöpfung müssen hierbei datenschutzrechtliche Aspekte bezüglich **personenbezogener Daten,** beispielsweise zu Ansprechpartnern der beteiligten Unternehmen, berücksichtigt werden. Dem gegenüber stehen aber auch Informationspflichten, welche im Data Act vorgesehen sind. Dies führt dazu, dass beispielsweise Daten generiert bei der Nutzung von Maschinen oder eines Services dem Unternehmen, welche diese Maschine verwendet, zugänglich gemacht werden müssen. Darüber hinaus wird dazu der kommende Data Act **spezifische Vorgaben für die Ausgestaltung von Verträgen des Datenaustausches und des Datentransfers** festlegen, welche bei unternehmensübergreifendem Datenaustausch benötigt werden. Zudem werden durch den angekündigten Data Act **Restriktionen zur Weiterleitung von Daten in Drittländer** erhoben, welche jedoch zum aktuellen Zeitpunkt nicht weiter spezifiziert wurden. Im Falle des **Data Governance Acts** kann dies für die Co-Creation dahingehend von Interesse sein, dass eine Möglichkeit geschaffen wird, von **staatlichen Institutionen Daten** für altruistische Zwecke zu verwenden. Der Digital Services Act bezieht sich ausschließlich auf Infrastruktur- und Interoperabilitätsanforderungen. In Bezug auf die SealedServices Infrastruktur hat dies jedoch keine Implikationen, da diese rechtliche Vorgabe nur für sehr große Infrastrukturen Anwendung findet. Der Digital Markets Act, hingegen adressiert den Wettbewerb von Services, wie zum Beispiel den plattformeigenen Services des Matching Verfahrens, mit anderen Lösungen, erstellt durch Teilnehmer der SealedServices Infrastruktur. Da diese Regulation der Gleichstellung eigener und fremder Services in einer Infrastruktur erst bei größeren Plattformen greift, ist es für Unternehmen aktuell wenig sinnvoll, gemeinsam mit anderen in der SealedServices Infrastruktur beteiligten Unternehmen alternative Applikationen zum Matching Verfahren der Infrastruktur zu planen. Das Lieferkettengesetz spielt in Hinblick auf die Co-Creation eine wichtige strategische Rolle zur vereinfachten Überzeugung des Datenaustausches entlang der Wertschöpfungskette, über Daten zu sozialen Standards hinaus. Hierbei kann argumentiert werden, dass die Basis für den Datenaustausch durch Schnittstellen bereits besteht bzw. bis zur schrittweisen Umsetzung ab 2023 bestehen muss.

In Bezug auf die Subebene des Marktumfeldes handelt es sich um die Untersuchung der Handhabung von erwähnten Regularien für sektorübergreifende Teilnehmer, um entsprechend passende Lösungen zu entwickeln. Ein Beispiel zur aktuellen

praktischen Umsetzung kann in der IT-Branche gefunden werden. Dabei können Endkunden bereits die über sie erhobenen Daten erfragen. Hierbei handelt es sich jedoch nicht, wie vom Data Act adressiert, um eine interoperable Schnittstelle, sondern aktuell noch um einen komplizierten Weg. Entsprechende Systeme zur kundenspezifischen Zusammenstellung der generierten Daten können jedoch als Vorbild für eigene Systeme für die eigenen Maschinen und Services der Maschinen- und Anlagenbauer in SealedServices herangezogen werden, um damit unter Hinzunahme einer **interoperablen Schnittstelle** den **Data Act** zu erfüllen. Darüber hinaus ist im Austausch auch mit Unternehmen aus benachbarten Sektoren darauf zu achten, dass keine **personenbezogenen Daten** ausgetauscht werden, um die **DSGVO** zu erfüllen. Der Digital Services Act und der Digital Markets Act spielen bei der aktuellen Größe der Infrastruktur keine Rolle, wie bereits bei den anderen Subebenen. Im Fall des Lieferkettengesetzes kann es hierbei auch nur indirekte Effekte auf diese Subebene geben, da bereits Schnittstellen zur Einhaltung des Lieferkettengesetztes geschaffen werden müssen. Diese können je nach Ausführung mit wenig Aufwand auch zum Austausch von Daten mit anderen Unternehmen im Marktumfeld verwendet werden.

Ein Kunde eines Maschinenbauers kann über die SealedServices Infrastruktur durch die Interoperabilität Daten abfragen, die durch seine Maschine im Produktionsprozess entstanden bzw. entstehen, sowie dieser unter Hinzunahme von Gaia-X und IDS sicher und souverän für eigene Prozesse der Produktionsoptimierung nutzen.

5.2 Geschäftsprozess

Auf der Subebene des Kallenberg-Prozesses ist insbesondere die Datenbasis und die Möglichkeit der Verarbeitung von regulatorischer Relevanz[4]. Bereits im ersten Schritt der Ermittlung des Leistungsbedarfes sind bei der Datenerhebung und der Verarbeitung insbesondere auch von personenbezogenen Daten die **Einhaltung von DSGVO und zukünftig auch des Data Acts** zu beachten. Dazu zählt die Einhaltung von Regelungen zu personenbezogenen Daten (DSGVO), aber auch spezifische Vorgaben für die Ausgestaltung von Verträgen des Datenaustausches und des Datentransfers des geplanten Data Acts, welche bei unternehmensübergreifendem Datenaustausch nötig werden wird. Darüber hinaus werden durch den angekündigten Data Act Restriktionen zur Weiterleitung von Daten in Drittländer erhoben, welche jedoch zum aktuellen Zeitpunkt nicht weiter spezifiziert wurden. In Bezug auf den **Data Governance Act** bietet dies die Möglichkeiten entsprechend dem Leistungsbedarf, um **Daten staatlicher Institutionen** auszuweiten, solange dies altruistischen Zwecken dient. In Bezug auf den Digital Market Act und den Digital Services Act gibt es keine zutreffenden Vorgaben für beteiligte Unternehmen und die Infrastruktur in dieser Subebene. Das Lieferkettengesetz auf der deutschen Bundesebene hingegen hat Einfluss auf diesen Prozess und kann zudem als Unterstützer einer Co-Produktion genutzt werden, da damit die rechtliche Grundlage geschaffen wird, Daten entlang der Wertschöpfungskette bereitstellen zu müssen. Analog zu diesen Aussagen, bezogen auf den ersten Schritt des Kallenberg-Prozesses, treffen diese Regularien ebenfalls die anderen vier Prozessschritte[4]. Im Falle der Servicekomposition kann es dabei, neben den Vorgaben der DSGVO und des kommenden Data Acts zu Einschränkungen kommen, wenn der Maschinen- und Anlagenbauer oder die Infrastruktur »Gatekeeper«, nach der Definition der EU, als Dienstleister nutzt. In diesem Fall wären sie indirekt vom Digital Markets Act betroffen. Das **Lieferkettengesetz** hat im Fall des Kallenberg-Prozesses nur indirekte Auswirkungen, sodass zur Einhaltung geschaffener Schnittstellen gegebenenfalls die Datenverfügbarkeit erhöhen kann. Dies begründet sich aus Möglichkeiten der Nutzungen der Schnittstellen zum unternehmensübergreifenden Datenaustausch zur Refinanzierung dieser und beziehungsweise oder der **Schaffung neuer Einnahmequellen**.

Die Aufgabe der Konzeptionierung und Überprüfung der Einhaltung anhand der Regularien ist auch Teil der Subebene Differenzierung zwischen datenbasierten und physischen SealedServices. Dabei ist insbesondere bei der Erstellung der Bausteine eine Instanz zu definieren, die die Konformität mit regulatorischen Vorgaben sicherstellt, um die Umsetzung datengetriebener Geschäftsmodelle zu erleichtern. Bei diesem Schritt der Differenzierung ist jedoch auch auf Seiten des Anbieters die Adaption des bereitgestellten Datensets zur Darstellung der jeweiligen SealedServices Art und der Verwendung von Bausteinen wichtig, dass diese überprüft werden, ob diese Daten nach den Regularien in der angedachten Form verwendet beziehungsweise verarbeitet werden dürfen. Als Beispiel dafür kann die Verarbeitung von personenbezogenen Daten herangezogen werden, wobei hier die

DSGVO Anwendung findet. Auch hier ist der kommende **Data Act** anzuwenden, mit dem spezifische Vorgaben für die Ausgestaltung von Verträgen des Datenaustausches und des Datentransfers entstehen, welche bei unternehmensübergreifendem Datenaustausch zum Beispiel bei der Verwendung der Bausteine nötig werden können. Zudem sind auch hier die Restriktionen des Data Acts zur Weiterleitung von Daten in Drittländer relevant, welche jedoch zum aktuellen Zeitpunkt nicht weiter spezifiziert wurden. Darüber hinaus sind je nach Anwendung der Bausteine auch **indirekte Restriktionen** auf Gatekeeper durch den **Digital Market Act** möglich, jedoch sind hierbei die jeweiligen Gatekeeper verantwortlich und nicht die Maschinen- und Anlagenbauer oder die Infrastruktur. In Bezug auf den Data Governance Act und den Digital Services Act ergeben sich keine weiteren Implikationen für diese Subebene. Das **Lieferkettengesetz** kann hingegen im Falle der physischen SealedServices als **Treiber der Nutzung der Bausteine** genutzt werden, da auch wenn dies zunächst nur größere Unternehmen trifft, indirekt durch die Beteiligung an deren Lieferketten auch kleiner Unternehmen Daten gegebenenfalls bereitstellen müssen.

Auf der dritten Subebene des Matching Verfahrens ist die rechtliche Dimension besonders hervorzuheben. Hier handelt es sich insbesondere um die Übermittlung der Daten an eine Matching Instanz und die anschließende Weitergabe der Daten an ein anderes Unternehmen, welches rechtliche Auswirkungen beinhalten. Ein Beispiel hierfür ist die Weitergabe zur Schaffung einer Partnerschaft. Daher ist hierbei auf die Einhaltung von Anonymisierungsvorgaben der **DSGVO** zu achten und die zukünftige Konformität mit dem **Data Act**. Dies erfordert einen konformen Vertrag zum Datentransfer und die Einhaltung der noch nicht näher spezifizierten Restriktionen zum Transfer von Daten in Drittländer. Der Data Governance Act zur Bereitstellung von Daten aus staatlichen Institutionen ist für diese Ebene nicht relevant. Darüber hinaus sind auch der Digital Markets Act und der Digital Services Act nicht anwendbar, da keine ausreichende Größe zur Applikation der Regularien besteht. Das Lieferkettengesetz hingegen ist anwendbar und kann vorwiegend als Treiber genutzt werden, um mehr Unternehmen dazu zu bringen, am Matching Verfahren teilzunehmen.

5.3 Informationstechnologie

Die erste Subebene der Informationstechnologieebene plattformbasierter Anwendungen stellt eine Vielzahl an Herausforderungen in rechtlicher Hinsicht dar. Bezogen auf die Teilaspekte Marktplatz und App Store ergeben sich unterschiedlich gewichtete rechtliche Implikationen. Da der Marktplatz die Basis für das Matching Verfahren darstellt, sind hier besonders viele Daten notwendig und für die richtige Zuteilung auch erforderlich zu analysieren. Damit ist hierbei insbesondere die **DSGVO** und der angekündigte **Data Act** zu berücksichtigen, da die Analysen zu dem richtigen Kunden, Anbieter oder Partnerrecherche in der SealedServices Infrastruktur stattfindet. Da sich diese außerhalb der Unternehmen befinden, handelt es sich um einen unternehmensübergreifenden Datenaustausch, welcher spezifische Vorgaben insbesondere im Umgang mit personenbezogenen Daten hat. Darüber hinaus wird dazu der kommende Data Act spezifische Vorgaben für die Ausgestaltung von Verträgen des Datenaustausches und des Datentransfers festlegen, welche bei jeglichem unternehmensübergreifenden Datenaustausch nötig werden. Diese Problematik, als auch der Aspekt der personenbezogenen Daten besteht auch im Fall des App Store, jedoch werden hierbei weniger Daten und vorwiegend applikationsspezifische Daten verwendet, sodass das Problem personenbezogener Daten weniger gravierend ist, als bei dem Marktplatz. Darüber hinaus werden durch den angekündigten Data Act Restriktionen zur Weiterleitung von Daten in Drittländer erhoben, welche jedoch zum aktuellen Zeitpunkt nicht weiter spezifiziert wurden. Bezogen auf den **Data Governance Act** ergeben sich für plattformbasierte Anwendungen zum Allgemeinwohl neue Datenquellen durch die Möglichkeit der Nutzung von Daten staatlicher Institutionen. Im Falle des Digital Services Acts und Digital Markets Acts ergeben sich, wie auf den anderen Subebenen, keine direkten Vorgaben an die Infrastruktur. Aufgrund der im Vergleich zu den adressierten Plattformen der regulatorischen Vorgaben (Meta, Alphabet etc.), kleinen Größe der bereitgestellten Infrastruktur und Anzahl der Kunden findet diese Gesetzgebung hier keine Anwendung. Dies hat jedoch für die beteiligten Unternehmen die Folge, dass plattformbasierte Anwendungen in der SealedServices Infrastruktur keine Interoperabilität mit anderen Plattformen bieten müssen. Somit können spezifische

Anwendungen für den App Store entwickelt werden und der Marktplatz kann unabhängig von anderen Plattformen spezifisch für den Einsatz im Maschinen- und Anlagenbau aufgebaut werden. Das **Lieferkettengesetz** kann auch auf Subebene der plattformbasierten Anwendungen als **Treiber** genutzt werden, da Unternehmen gezwungen werden, Daten entlang der Wertschöpfungskette zu erheben, welches die Verbreitung entsprechender Applikationen durch den App Store erweitert. Besonders die dadurch bereits etablierten Schnittstellen und erhobenen Daten vereinfachen die Nutzung und Entwicklung plattformbasierter Anwendungen.

Bei der zweiten Subebene der Plattformsicherheit werden von rechtlicher Seite grundlegende Definitionen beispielsweise der **Haftung** durch den **Digital Markets Act** definiert, sodass die Plattform nur für **wissentlich rechtswidrige Inhalte** haftet. Somit liegt hierbei die Verantwortung und rechtliche Haftung beim Datengeber. Rechtswidrige Inhalte können dabei beispielsweise personenbezogene Daten (**DSGVO**) wie E-Mail-Adressen sein. Der Data Governance Act ist aufgrund seiner Fokussierung auf staatliche Institutionen für die Plattformsicherheit nicht relevant. Ebenso wenig ist der Digital Markets Act von Bedeutung, da dieser nur auf die Bevorzugung eigener Infrastrukturdienste abzielt, die keine direkte Sicherheitsrelevanz haben. Analog hat auch das Lieferkettengesetz keine Auswirkungen auf die Plattformsicherheit. In Bezug auf den Digital Services Act ist, aufgrund der Ausnahme kleinerer und mittlerer Infrastrukturen, keine Interoperabilität mit anderen Infrastrukturen vorgegeben. Dies hat zur Folge, dass die Anzahl der Schnittstellen so beeinflusst werden kann, dass die Plattformsicherheit durch weniger Schnittstellen als bei holistischer Interoperabilität erhöht werden kann.

In Bezug auf die dritte Subebene der Datenhaltung ergeben sich regulatorische Erleichterungen durch den kommenden Data Act. Dieser schafft grundlegende Standards für den Wechsel des Cloud-Anbieters, sodass ein Wechsel des Cloud-Anbieters zukünftig kostenneutral sein wird. Dies erhöht somit die Flexibilität der an der SealedServices Infrastruktur teilnehmenden Unternehmen. Durch den Multi-Cloud Ansatz, der SealedServices Infrastruktur wird damit die Flexibilität erhalten. Auf Subebene der Datenhaltung gibt es, bezogen auf personenbezogenen Daten, beispielsweise die Möglichkeit der automatischen Anonymisierung direkt an der Maschine (am Edge Device) oder auf Subebene der Cloud, sodass die Einhaltung der **DSGVO** damit automatisiert erreicht werden kann. Bezugnehmend auf den **Data Governance Act** ergeben sich Implikationen zur Schaffung möglicher Auswertung von bereitgestellten **Daten durch staatliche Institutionen**, jedoch keine Einschränkungen für die Infrastruktur oder die beteiligten Unternehmen. Für die Datenhaltung hat zudem auch der **Digital Services Act** und der **Digital Markets Act** keine direkten Implikationen. Einzig die **Schnittstellengestaltung** in der Datenhaltung wäre betroffen, da wie bereits erwähnt, dies jedoch erst für größere Infrastrukturen gilt. Im Gegensatz dazu ist das **Lieferkettengesetz** für die Datenhaltung sehr relevant, da **Daten zu Vorgaben bezüglich der Handhabung von Sozialstandards** durch die Unternehmen vorgehalten werden müssen.

6 Fazit und Ausblick

Data Governance spielt eine zentrale Rolle in der Ausgestaltung von unternehmensübergreifendem Datenaustausch in der kollaborativen Wertschöpfung. Hierbei bietet dieses Whitepaper einen Leitfaden bezüglich der zu adressierenden Teilbereiche. Dabei hebt dieses Whitepaper anhand des Bezuges auf die SealedServices Infrastruktur und ihrer verschiedenen Ebenen und Subebenen Handlungsfelder hervor. Insgesamt lassen sich hierbei für alle Unternehmensebenen Implikationen ableiten, um Datenmanagement innerhalb eines Unternehmens und übergreifend sowie Datenaustausch anhand eines Data Governance Rahmenwerkes zu gestalten.
Mit Blick auf zukünftige Entwicklungen in Bezug auf die SealedServices Infrastruktur sowie regulatorische und technologische Weiterentwicklungen, bieten sich neue Bereiche der intelligenten automatisierten Abläufe innerhalb der Data Governance. Daraus ergeben sich insbesondere neue Forschungsfelder hinsichtlich einer tiefgreifenderen Analyse und Übertragung regulatorischer Vorgaben auf praktische Abläufe in der SealedServices Infrastruktur. Darüber hinaus kann insbesondere ein Blick auf neue technologische Entwicklungen im Bereich des Datenqualitätsmanagements, durch beispielsweise intelligente Datenanalysen sowie neuer Methoden der Datensicherheit in einer weiteren wissenschaftlichen Kontribution betrachtet werden.
Zusammenfassend eröffnet dieses Whitepaper insbesondere für an SealedServices Infrastruktur beteiligten Unternehmen ein Rahmenwerk zur Adressierung des zunehmenden Bedarfs der Co-Produktion von Unternehmen. Dies kann den Unternehmen dabei helfen, holistisch diesen zunehmenden Herausforderungen zu begegnen. Darüber hinaus ermöglicht die Nutzung dieses Vorgehens die Schaffung neuer Geschäftsfelder des Datenaustausches und damit den Erhalt der Wettbewerbsfähigkeit und der vorübergehenden Schaffung eines Wettbewerbsvorteils.

7 Quellenverzeichnis

[1] Weber, K. (2012). Data Governance – Organisation des Stammdatenmanagements. IT-Governance. 6.3-8, Schweinfurt.

[2] Otto, B; Korte, T; Azkan, C; et al. (2019). Data Economy status quo der deutschen Wirtschaft & Handlungsfelder in der Data Economy, Dortmund.

[3] Henderson, D; Earley, S; Sebastian-Colema L.: DAMA DMBOK, Data management body of knowledge second edition

[4] Kallenberg (2002). Ein Referenzmodell für den Service in Unternehmen des Maschinenbaus, Hamm.

[5] Legner, C. & Otto, B. (2007). Stammdatenmanagement. Das Wirtschaftsstudium (WISU), 236 (4).562-568.ISSN 0340-3084.

[6] Pipino, L.; Lee, Y. & Wang, R.(2003). Data Quality Assessment. Communications of the ACM.45.10.1145/505248.506010.

[7] Manogaran, G., Thota, C., Lopez, D., Sundarasekar, R. (2017). Big Data Security Intelligence for Healthcare Industry 4.0. In: Thames, L., Schaefer, D. (eds) Cybersecurity for Industry 4.0. Springer Series in Advanced Manufacturing. Springer, Cham.

[8] Chang, V; Kuo, YH; Ramachandran, M. (2015) Cloud computing adoption framework: A security framework for business clouds. Future Generation Compu-ter Systems, 57. 24 – 41, Leeds.

[9] Gaia-X AISBL (2022). Homepage, https://www.gaia-x.eu/, Brüssel.

[10] International Data Spaces Association (2022). Our vision and mission, https://internationaldataspaces.org/why/; Berlin.

[11] Otto, B; Rubina, A; Eitel, A; Teuscher, A. et al. (2021) Gaia-X and IDS, Position Paper, https://internationaldataspaces.org/download/19016/, Berlin.

[12] Otto, B; Steinbuß, S; Teuscher, A; Lohmann, S. (2019) Reference Architecture Model Version 3.0; Berlin.

[13] Gaia-X AISBL (2022). Gaia-X Labelling Framework. Brüssel.

[14] Gaia-X AISBL (2022) Gaia-X Labelling Criteria. Brüssel.

[15] ecoVerband der Internetwirtschaft, (2022) Gaia-X Federation Services, Brüssel.

[16] Europäische Kommission (2020) Data Governance Act Proposal, Brüssel.

[17] Europäische Kommission (2020) Gesetz über digitale Dienste, Brüssel.

[18] Europäischer Rat (2020) Gesetz über digitale Märkte, Brüssel.

[19] European Commission (2020) Gesetz über digitale Märkte, Brüssel.

[20] European Commission (2016) Datenschutzgrundverordnung, Brüssel.

[21] European Data Protection Supervisor (2018) The History of the General Data Protection Regulation. Brüssel.

[22] European Commission (2022) Data Act Proposal, Brüssel.

[23] Deutsche Bundesregierung (2021) Entwurf eines Gesetzes über die unternehmerischen Sorgfaltspflichten in Lieferketten, Berlin.

8 Abbildungs- und Tabellenverzeichnis

Impressum

1. Auflage, Februar 2023

Herausgeber
Fraunhofer Institut für Software und Systemtechnik ISST
Emil-Figge-Straße 91
44227 Dortmund

Autor
Fraunhofer Institut für Software und Systemtechnik ISST
Dr.-Ing. Can Azkan
Sebastian Emons

Satz und Layout
Elisa Kadelka

Das Verbundprojekt wird im Rahmen des Programms „Innovationen für die Produktion, Dienstleistung und Arbeit von morgen“ vom Bundesministerium für Bildung und Forschung gefördert und durch den Projektträger Karlsruhe (PTKA) betreut.

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Kontakt

Dr.-Ing. Can Azkan
Tel. +49 231 976770
can.azkan@isst.fraunhofer.de

Fraunhofer-Institut für Software- und Systemtechnik ISST
Emil-Figge-Str. 91
44227 Dortmund
www.isst.fraunhofer.de