Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung

Studie zu zentralen Herausforderungen, Grundprinzipien und Voraussetzungen, konkreten Beispielen sowie Kernelementen eines Modells vertrauenswürdiger Datenräume im Auftrag des BAKOM

Patrizio Collovà, Michael Marti, Daniel Schwarz, Flurina Wäspi und Nicolai Wenger

Bern, 22.07.2021

Berner Fachhochschule
Wirtschaft
Institut Public Sector Transformation

Inhaltsverzeichnis

Management Summary

Die Studie beantwortet anhand einer Literaturübersicht und -analyse die folgenden Forschungsfragen:

1. Was sind die zentralen Herausforderungen, die sich in der Datenwertschöpfungskette in Bezug auf eine vermehrte Sekundärnutzung von Daten und eine erhöhte Teilnahme durch Individuen stellen?
2. Welche Grundprinzipien und Voraussetzungen sollen für vertrauenswürdige Datenräume gelten?
3. Was für Beispiele von vertrauenswürdigen Datenräumen bestehen bereits und welche Eigenschaften weisen diese auf?

Basierend auf den Erkenntnissen der Literaturstudie wird sodann ein Modell eines vertrauenswürdigen Datenraums vorgeschlagen.

Die Geschäftsmodelle der heutigen Big-Data-Ökonomie profitieren von starken Marktungleichgewichten und Marktversagen. Obwohl formal betrachtet abhängig von deren «informierter Zustimmung», teilen die Bürger*innen ihre persönlichen Daten nicht auf der Basis von Transparenz und Vertrauen, sondern weil ihnen kaum etwas anderes übrigbliebt, wenn sie digitale Anwendungen nutzen und am gesellschaftlichen Leben teilnehmen möchten. Vertrauen ist jedoch entscheidend, wenn die Potenziale des Datenteilens hinsichtlich Innovation, Effizienzgewinne und Benutzerfreundlichkeit für die Wirtschaft und Gesellschaft voll ausgeschöpft werden sollen. Die Studie konzentriert sich zwar primär auf die Beteiligten in der Datenökonomie, doch soll an dieser Stelle darauf verwiesen werden, dass auch staatliche Stellen (z.B. im Rahmen der Realisierung des Once-Only-Prinzips) im selben Ausmass auf das Vertrauen der Bürger*innen und Unternehmen in den Umgang mit Daten angewiesen sind.

Um dieses Vertrauen herzustellen, gilt es **eine Reihe von Herausforderungen** sowohl auf individueller als auch auf kollektiver organisatorischer Ebene anzugehen. Auf individueller Ebene wird in erster Linie die Ausgestaltung des Entscheidungskontexts thematisiert. Die Bürger*innen sollen in die Lage versetzt werden, die Folgen ihrer Entscheidung abschätzen zu können. Dazu ist eine einfach verständliche Form der Kommunikation nötig, die mit angemessener Information und visuellen Elementen (z.B. im Rahmen standardisierter Produktprüfungen) möglichst transparent informieren soll. Damit den Bürger*innen der Sinn der Information klar wird, sind Begleitmassnahmen in Form einfacher Botschaften nötig, um die Bevölkerung für die grundlegenden Probleme beim Datenteilen zu sensibilisieren. Darüber hinaus müssen sämtliche die eigene Privatsphäre betreffende Entscheide immer befristet sein und auch jederzeit rückgängig gemacht werden können. Als weitere Herausforderung für den erfolgreichen Aufbau eines vertrauenswürdigen Systems gelten die Anreize, die für die Teilnahme gesetzt werden. Die Teilnahme muss zu einer deutlichen Abnahme der Last des persönlichen Datenmanagements führen und die Kosten allfälliger Anbieterwechsel müssen so gering wie möglich ausfallen. Andererseits sollte die Teilnahme an einem Datenraum für die Bürger*innen kostenlos sein – sie bringen schliesslich bereits ihre persönlichen Daten ein. Monetäre Anreize hingegen werden skeptisch beurteilt, da sie sozial und gesellschaftlich schwächere Gruppen zu einer übermässigen Datenpreisgabe verleiten können sowie die Teilnahmeanreize für die datennutzenden Unternehmen senken. Auch bezüglich der Ausgestaltung interner Entscheidungsstrukturen von Datenräumen ist die Vermeidung einer faktischen Benachteiligung einzelner Bevölkerungsgruppen im Auge zu behalten. Vertrauenswürdige Räume sollen insgesamt so ausgestaltet sein, dass sie auch von denjenigen genutzt werden, die über keine vertieften Kenntnisse der Materie verfügen.

Auf der kollektiven Ebene steht die Schaffung robuster und vertrauenswürdiger Datenräume im Zentrum. Die diesbezüglichen Herausforderungen beziehen sich auf die Sicherstellung einer von allen Stakeholdern (datengebende und datennutzende Personen, Organisationen und Unternehmen) finanziell und personell unabhängigen, von jeglichen Interessenkonflikten befreiten Organisationsform, was auf eine Not-for-Profit-Struktur mit klaren Verantwortlichkeits- und Haftungsregeln für die Datenraumbetreiber hinausläuft. Abzuklären bleibt, inwieweit die heutigen rechtlichen Möglichkeiten dazu ausreichen. Des Weiteren ist die Rolle des Staates zu definieren. Die Literatur geht mehrheitlich von einem «liberalen Modell» aus, das den Staat (ähnlich wie im Telekommunikations- oder Elektrizitätsmarkt) in der Verantwortung als Regulator und Aufsicht sieht, nicht aber als permanenter Finanzierer oder Betreiber. Hinsichtlich der Herausforderung eines nachhaltigen Finanzierungsmodells für Datenraumbetreiber muss darauf geachtet werden, dass die Anreize

für die datennutzenden Unternehmen zur Teilnahme an einem vertrauenswürdigen Austauschsystem nicht über finanzielle Belastungen zunichte gemacht werden.

Die **Grundprinzipien und Voraussetzungen für vertrauenswürdige Datenräume** wurden anhand von drei Ebenen erläutert. Die erste, **individuelle Ebene** lässt sich so zusammenfassen, dass in vertrauenswürdigen Datenräumen einzelne Personen gewisse Rechte haben müssen, die sie selbstständig gegen bestimmte und identifizierbare andere Personen geltend machen können. Dazu gehört der Anspruch auf Transparenz, Kontrolle und Solidarität. Umgekehrt müssen die belangbaren Personen auch wissen, welche konkreten Pflichten sie haben.

Die zweite, **kollektive Ebene** beschreibt die Ideale, denen vertrauenswürdige Datenräume zu folgen haben. Dazu gehören: eine faire Aufteilung der Kosten und Nutzen der Datenspeicherung, -bearbeitung und -wiederverwendung; eine Durchlässigkeit der Räume und ein Angebot qualitativ einwandfreier Daten; Vereinbarung der genauen Aufteilung und der Datenpflege in einer Abmachung; Gewährleistung der Interoperabilität, die auf vielfältigen Ebenen vorkommt; Skalierbarkeit der Grundprinzipien, um auch dezentrale, kleinere Datenräume entstehen zu lassen und zu fördern; Nutzung von Datenräumen zur Unterstützung von Nachhaltigkeitszielen, der wirtschaftlichen Entwicklung und zur Verbesserung der politischen Steuerung.

Die dritte Ebene, die der **Durchsetzung der Grundprinzipien** gewidmet ist, erinnert daran, dass sowohl verbindliche als auch unverbindliche Instrumente eingesetzt werden sollten. Wichtig ist insbesondere, dass die Verantwortlichkeitsfrage geklärt und auch Alternativen zu langwierigen, kostspieligen Prozessen etabliert sind.

Eine **Bestandesaufnahme der praktischen Umsetzung von vertrauenswürdigen Datenräumen** gestaltet sich allein deswegen herausfordernd, weil der Suchbegriff schwierig einzugrenzen ist. Auf einer konzeptionellen Ebene gibt es in der internationalen Literatur eine Diversität, die sich auch in der Praxis wiederfindet. Ein näherer Blick auf die verschiedenen angedachten oder teilweise umgesetzten Institutionen zum Datenteilen erweckt eher den Eindruck eines komplexen Geflechts von sich wiederholenden Verhaltensweisen als konkreten Typologien.

Als nützlicher Typologisierungsansatz erweist sich in Anlehnung an Mulgan & Straub (2019) die Beurteilung unterschiedlicher Governance-Formen anhand zweier Dimensionen: Wert der Daten für die Öffentlichkeit und Ausmass an individueller Kontrolle über das Datenteilen. Das sich dadurch ergebende Feld reicht von Institutionen mit Daten, die hauptsächlich einen Wert für das Individuum besitzen und wo dieses auch die komplette Kontrolle über das Datenteilen besitzt (Personal Data Stores) bis zu Institutionen, die für die Allgemeinheit sehr wertvolle Daten verwalten, wobei die Daten ohne eine freiwillige (oder vermeidbare) Entscheidung der dahinterstehenden Individuen übermittelt werden (Public Data Trusts). Gerade dieser Ansatz der Data Trusts stellt eine vieldiskutierte Ausgestaltung eines vertrauenswürdigen Datenraumes dar. Die Vorteile eines Data Trusts werden darin gesehen, dass sich mit einer unabhängigen, treuhänderischen Verwaltung von Daten Verhandlungsspielraum für das Individuum ergibt, der in konventionellen Daten-Beziehungen nicht oder kaum existiert. Zu den Voraussetzungen für einen Data Trust gehört dabei die Einigung auf ein gemeinsames Ziel, eine Governance-Struktur, eine klare Vorstellung der Aufteilung des Nutzens / Gewinns aus dem Data Trust und die Sicherstellung einer nachhaltigen Finanzierung der Data-Trust-Strukturen. Je nach Art der Daten und Kontext kann ein Data Trust unterschiedliche Ausprägungen einnehmen.

Welche Form die neun verschiedenen vertrauenswürdigen Datenräume, die von der Europäischen Kommission geplant sind, einnehmen sollen, ist noch offen und wird höchstwahrscheinlich sektoriell ausgestaltet sein. Für die Umsetzung relevant sind an diesem Punkt das GAIA-X-Projekt und der IDS-Standard. Beide Initiativen haben sich dabei den Grundprinzipien der informationellen Selbstbestimmung, Partizipation, Offenheit und einem föderativen, dezentralen Vorgehen verpflichtet. Zur Umsetzung und Vermeidung von Lock-in-Effekten sollen zudem verschiedene technische Richtlinien beitragen.

Auf der Basis der Literaturstudie wurde **ein Modell eines vertrauenswürdigen Datenraums** zu definieren versucht. Die Schwierigkeit besteht darin, sich auf nicht allgemein anerkannten, zum grössten Teil nicht genau definierten Begriffen abstützen zu müssen. Wo präzise Definitionen fehlen, müssen sie durch

Annahmen ersetzt werden, weshalb das auf dieser Basis konstruierte Modell als ein vorläufiger Vorschlag zu verstehen ist. Ein wichtiger Punkt im Rahmen der Modellkonzeption ist die Zerlegung der Prinzipien vertrauenswürdiger Datenräume in einzelne prüfbare Eigenschaften. Die Definition solcher Attribute und die Aufstellung von Prüfskalen muss angegangen werden, weil zurzeit kein praxistauglicher Eigenschaftskatalog vorhanden ist. Nach einer solchen vertieften Analyse sind die Handlungen (aufseiten der Betreiber*innen) und die Prüfverfahren (aufseiten der Nutzer*innen) festzulegen und im Detail zu dokumentieren. Erst wenn diese Elemente und ihr Zusammenspiel als Rahmenwerk vorhanden sind, kann die Erstellung eines vertrauenswürdigen Datenraums systematisch angegangen werden. Erst eine breite Diskussion und Anwendung des vorgeschlagenen Modells in realen Fällen werden zeigen, ob dieses die Realität vertrauenswürdiger Datenräume passend abbildet.

1 Einleitung

Das Bundesamt für Kommunikation (BAKOM) erarbeitet zusammen mit dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) und der Bundeskanzlei bis Ende 2021 im Rahmen der Strategie «Digitale Schweiz»[1] einen Bericht zu den Voraussetzungen zur Schaffung von vertrauenswürdigen Datenräumen unter Berücksichtigung der digitalen Selbstbestimmung.

Im Zuge dieser Arbeiten hat das BAKOM das Institut Public Sector Transformation der Berner Fachhochschule Wirtschaft (BFH-W) beauftragt, eine Literaturübersicht und -analyse zu den folgenden Forschungsfragen zu erstellen:

1. Was sind die zentralen Herausforderungen, die sich in der Datenwertschöpfungskette in Bezug auf eine vermehrte Sekundärnutzung von Daten und eine erhöhte Teilnahme durch Individuen stellen? Die Herausforderungen werden mit Blick auf zwei gleichrangige Public-Policy-Ziele betrachtet: Die Förderung der digitalen Wirtschaft und Innovation durch Datennutzung sowie die digitale Selbstbestimmung im Sinne einer aktiven Mitbestimmung von Individuen im digitalen Raum.
2. Welche Grundprinzipien und Voraussetzungen sollen für vertrauenswürdige Datenräume gelten?
3. Was für Beispiele von vertrauenswürdigen Datenräumen bestehen bereits und welche Eigenschaften weisen diese auf?

Basierend auf den Erkenntnissen der Literaturstudie wird des Weiteren ein Modell eines vertrauenswürdigen Datenraums vorgeschlagen. Es handelt sich dabei um ein Wissensmodell, das die Kernelemente vertrauenswürdiger Datenräume und deren Beziehungen festlegt, mittels einer standardisierten Notation das Begriffsnetz aufzeigt sowie das thematische Wissen zu organisieren und vereinheitlichen versucht.

Die Gesamtstudie ist wie folgt aufgebaut: Die Kapitel 2 bis 4 behandeln die drei Forschungsfragen der Literaturanalyse, während sich das fünfte Kapitel dem Aufbau des Wissensmodells widmet. In Kapitel 6 finden sich die Schlussfolgerungen.

1 https://www.digitaldialog.swiss

2 Zentrale Herausforderungen im Datenzyklus

Dieses Kapitel eruiert anhand einer Literaturstudie die grössten Herausforderungen, die sich im aktuell wahrgenommenen Spannungsfeld zwischen den Anliegen von verstärkter Datennutzung und digitaler Innovation einerseits und der Verwirklichung der individuellen Selbstbestimmung im digitalen Raum andererseits ergeben. Für die Herleitung und Bestimmung der genannten Herausforderungen spielen Erkenntnisse bezüglich der besonderen Charakteristiken und der daraus folgenden Probleme der Datenökonomie eine essenzielle Rolle. Das Kapitel gliedert sich darum in einen ersten Teil, der sich den datenökonomischen Grundlagen widmet. Darauf basierend werden in einem zweiten Teil die in der Literatur identifizierten Herausforderungen sowohl mit Bezug auf die individuelle als auch auf die kollektive bzw. organisatorische Ebene dargestellt.

2.1 Grundlegende Merkmale und Problemstellungen in der Datenökonomie

Daten werden wahlweise als eine neue Art des Vermögens, als neue Währung, als neuen Rohstoff oder als neuen Produktionsfaktor bezeichnet (Heuberger et al., 2021; Jentzsch, 2017; Schneider, 2019; World Economic Forum, 2011). Im Unterschied zu anderen Wirtschaftszweigen, macht sich die *Datenökonomie* ein Gut zunutze, das einerseits immateriell (intangible), andererseits unendlich teil- und kopierbar ist, wodurch sich eine Nicht-Rivalität im Konsum ergibt. Zudem ist es schwierig, Dritte von der Datennutzung auszuschliessen, sobald die Daten den eigenen Kontrollbereich verlassen haben bzw. veröffentlicht worden sind (Nicht-Ausschliessbarkeit) (Jentzsch, 2017; Schneider, 2019). Darüber hinaus kann die Bekanntgabe, Bearbeitung und Nutzung von Daten die Position unbeteiligter Dritter beeinflussen (Externalitäten). Diese Grundeigenschaften von Daten verhindern die Entstehung eines Marktes im Sinne der klassischen ökonomischen Theorie, nach der die Festlegung des Preises über Angebot und Nachfrage bestimmt wird (Jentzsch, 2017).

Dennoch hat sich eine Datenökonomie herausgebildet, die eng mit dem Aufkommen von Anwendungen im Big-Data-Bereich verknüpft ist. Aus ökonomischer Sicht definiert sich *Big Data* primär über die Höhe des wirtschaftlich verwertbaren Informationsgehalts, also die Wertschöpfung, die mittels Daten bzw. deren Bearbeitung und Nutzung im Rahmen des *Datenzyklus* (data life-cycle) generiert werden kann (Picot et al., 2018; Wang, 2019).[2]

Die in der Öffentlichkeit geführte Big-Data-Debatte stellt häufig die Erhebung und Nutzung personenbezogener bzw. -beziehbarer Daten, im Folgenden auch vereinfacht als *persönliche Daten* bezeichnet, ins Zentrum. Zur Charakteristik von Big Data zählt allerdings auch die Vielfalt der Datenquellen, die miteinander verknüpft werden können (das dritte der fünf «V», siehe Fussnote 2), was die Grenzen zwischen persönlichen und nicht-persönlichen Daten verschwimmen lässt bzw. *De-Anonymisierungsprozesse* ermöglicht (Jarchow & Estermann, 2015; Picot et al., 2018; Purtova, 2017). Der Grad des Personenbezugs ist eine variable Grösse, die sich aufgrund der Bearbeitung resp. Verlinkung von Daten verändern kann (Heumann & Jentzsch, 2019). Hinzu kommt, dass die subjektive Wahrnehmung, welche Daten als schützenswert betrachtet werden und wie sensibel die aufgrund von Datenbearbeitung gewonnenen Informationen sind, individuell und kulturell stark variiert (Jarchow & Estermann, 2015).[3]

Im Zentrum der Debatte um persönliche Daten stehen wiederholt die grossen Betreiber sozialer Netzwerke und Plattformen, da sich an deren Marktverhalten die grundlegende Problematik der Datenökonomie besonders gut erkennen und darstellen lässt.[4] Im Folgenden werden die gemeinsamen Merkmale des in der sogenannten *Plattform-Ökonomie* vorherrschenden Geschäftsmodells auf der Basis von Blankertz (2020), Picot et al. (2018) und Schneider (2019) anhand von drei Punkten kurz umrissen:

2 Dies entspricht dem letzten der fünf «V», die häufig zwecks Chrakterisierung von Big Data herangezogen werden: Volume (Grösse), velocity (Tempo der Generierung und Analyse), variety (Diversität bzgl. Quellen und Formaten), veracity (Vertrauen in Qualität und Korrektheit) und value (Wertsteigerung) (vgl. für eine Übersicht Picot et al., 2018).

3 Im Gegensatz dazu fällt aus einer datenschutzrechtlichen Perspektive die Definition von personenbezogenen, bzw. -beziehbaren sowie von schützenswerten bzw. besonders schützenswerten Daten relativ präzise aus.

4 Genannt werden zwar immer wieder die vier grössten US-amerikanischen Unternehmen Google, Apple, Facebook und Amazon (Schneider, 2019), doch sollte im selben Atemzug auch die immer stärker werdende Plattformkonkurrenz aus China (z.B. Alibaba, Wechat, TikTok) eingeschlossen werden. Mit dem zunehmenden Einsatz von künstlicher Intelligenz (KI), dem Internet der Dinge (IoT) und der Verbreitung von «smart home devices» ist zudem eine Akzentuierung der bestehenden Oligopol-Struktur zu befürchten.

- **Tauschgeschäft:** Zwischen Plattformbetreibern (Unternehmen) und den Plattformnutzenden (Konsument*innen[5]) besteht ein Tauschgeschäft: Die Konsument*innen überlassen im Rahmen der geltenden Datenschutzgesetzgebung, die sowohl in der Schweiz als auch in der EU eine vorgängige *informierte Einwilligung* (informed consent) vorschreibt, den Plattformbetreibern kostenlos in einem bestimmten Umfang ihre persönlichen Daten. Im Gegenzug stellen die Unternehmen auf der Basis dieser Daten den Konsument*innen eine Reihe kostenlos verfügbarer Produkte bereit, die diese als besonders nützlich wahrnehmen (z.B. Online-Kartendienste, Messenger-Dienste, Plattformen für den sozialen Austausch).

- **Eigentliches Geschäftsmodell:** Das Geschäftsmodell der Unternehmungen besteht primär darin, dass sie die aufbereiteten persönlichen Daten der Konsument*innen entweder selbst nutzen oder ihren Businesspartnern zugänglich machen, um z.B. zielgerichtete Werbung schalten zu können oder zur Entwicklung und Vermarktung neuer (kostenpflichtiger) Produkte beizutragen.

- **Netzwerk- und Lock-in-Effekte:** Die Grösse der Nutzergruppe ist für die Plattformbetreiber von entscheidender Bedeutung. Je höher die Zahl der Nutzer*innen der kostenlos angebotenen Produkte, desto mehr persönliche Daten können gesammelt werden, was einerseits wiederum die Qualität und die Nutzenstiftung der zur Verfügung gestellten Produkte erhöht, andererseits auch den Erlös aus dem dahinter liegenden, eigentlichen Geschäftsmodell. So entstehen *Netzwerk-* und *Lock-in-Effekte*: Um die Konsument*innen so eng wie möglich an sich zu binden, bauen die Plattformbetreiber *geschlossene Ökosysteme* (walled gardens) auf, wodurch einerseits für die Konsument*innen sich die Kosten eines Wechsels zu einem anderen Anbieter erhöhen, andererseits für mögliche konkurrierende Unternehmen der Markteintritt stark erschwert oder ganz verunmöglicht wird.

Die Dominanz einiger weniger Konzerne, deren Geschäftsmodelle ganz oder teilweise auf den gesammelten persönlichen Daten der Konsument*innen beruhen, verhindert somit das Entstehen eines funktionierenden Marktes sowohl in der Beziehung zwischen Unternehmen und Konsument*innen als auch auf der Anbieterseite zwischen den Unternehmen. Das Marktversagen aufseiten der Konsument*innen entsteht aufgrund einer mangelnden Durchsetzungsfähigkeit ihrer Interessen in Bezug auf die Verwendung der persönlichen Daten. In Anlehnung an Blankertz (2020) sind dafür vier Gründe zu nennen, auf die nachfolgend näher eingegangen wird: fehlende Marktmacht, übermässige Informationskosten, kontextabhängige Entscheidungssituationen sowie kollektive Auswirkungen individueller Entscheidungen.

- **Fehlende Marktmacht:** Die Konsument*innen verfügen über keine Marktmacht, da sie nicht kollektiv organisiert sind und der individuelle datenliefernde Beitrag für die Plattformbetreiber zudem vernachlässigbar klein ist. Die Unternehmen haben darum keinen Anreiz, auf allfällige Bedenken und Forderungen Einzelner oder kleiner Gruppen einzugehen. Die bereits genannten Netzwerk- und Lock-in-Effekte drängen die Konsument*innen zusätzlich dazu, für sie ungünstige Bedingungen hinsichtlich des Schutzes ihrer Privatsphäre zu akzeptieren.

- **Übermässige Informationskosten:** Da mit dem Internet verbundene Geräte sowie Applikationen und Aktivitäten im Web in aller Regel und in unterschiedlichem Ausmass persönliche Daten erheben, werden die Konsument*innen sehr häufig nach ihrer «informierten Einwilligung» gefragt, sodass es am Ende unmöglich ist, den Überblick über die vielen verschiedenen Datennutzungsbedingungen zu behalten, ganz abgesehen von der Frage, ob der Inhalt überhaupt gelesen und verstanden wird und es sich somit wirklich um eine «informierte» Zustimmung handelt (Datenethikkommission der Bundesregierung, 2019; Delacroix & Lawrence, 2019; Nissenbaum, 2011; O'Hara, 2019).

- **Kontextabhängige Entscheidungen:** Die Antwort auf die Frage, wie viel der eigenen Privatsphäre man preisgeben möchte, hängt stark vom konkreten Entscheidungskontext ab und fällt daher inkonsistent aus. Es treten Affektentscheidungen und das Privatsphären-Paradoxon zutage (Jentzsch, 2017; Lamla & Ochs, 2019), auf die in Kapitel 2.2 näher eingegangen wird. Dies gilt insbesondere dann, wenn für die Konsument*innen gar kein vernünftiger Entscheidungsspielraum besteht, sofern eine bestimmte Dienstleistung in sinnvollem Umfang genutzt werden soll (Data Critiques, 2019).

5 Im Rahmen der Beschreibung der Datenökonomie wird für die Nachfrageseite der Begriff der Konsument*in verwendet.

- **Kollektive Auswirkungen von individuellen Entscheidungen:** Die Zustimmung zur Weitergabe von persönlichen Daten kann sich indirekt auch auf Personen auswirken, die bewusst einen restriktiveren Umgang gewählt haben (Data Critiques, 2019). Aufgrund von *Unraveling-Prozessen* können Datenschutzanstrengungen teilweise unterlaufen werden (z.B., wenn eine Krankenkasse ein Belohnungssystem für die «freiwillige» Bekanntgabe von persönlichen Gesundheitsdaten ihr gegenüber einführt (Jentzsch, 2017)).

Die Anzeichen für ein Marktversagen beschränken sich nicht auf die Nachfrageseite, sondern sind ebenso unter den Anbietern bzw. Unternehmen erkennbar (Blankertz, 2020). Die grossen Player haben frühzeitig eigene Daten-Ökosysteme geschaffen, deren Zugang anderen Anbietern entweder ganz verschlossen bleibt oder zumindest restriktiv geregelt ist. Diese Zugangsregeln schaffen Anreize für die Entwicklung von Produkten, die mit dem Ökosystem des Unternehmens, das den Datenzugang gewährt, kompatibel sind. Dadurch wiederum werden die Attraktivität und der Wert des bestehenden Ökosystems gesteigert. Die Datenhaltung verbleibt in jedem Fall bei den wenigen Datenkonzernen, wodurch verhindert wird, dass kleinere bzw. neu in den Markt eintretende Firmen unabhängig von den dominierenden Unternehmen und basierend auf einer eigenen Datenhaltung Produktinnovation betreiben können. Aufseiten der Unternehmen besteht das Problem der Big-Data-Ökonomie somit primär in fehlenden oder zu restriktiv definierten Datenzugängen für kleinere Unternehmen bzw. in den mangelnden Anreizen für die dominierenden Player, die von ihnen gehaltenen Datenbestände zu teilen.

2.2 Herausforderungen im wahrgenommenen Spannungsfeld von Datennutzung und individueller Selbstbestimmung

Die Datenökonomie gilt als Innovationstreiber und trägt zunehmend zur Wirtschaftsleistung bei (World Economic Forum, 2019). Gleichzeitig hängt die Verfügbarkeit des für diese Wertschöpfung essenziellen Rohstoffs, der (persönlichen) Daten der Bürger*innen[6] oder Konsument*innen, von deren Zustimmung ab.[7] Wie bereits beschrieben, beruht die Bereitschaft zur Datenbekanntgabe in der aktuellen Big-Data-Ökonomie nicht auf der Basis von Transparenz und Vertrauen, sondern ist letztlich eine Folge der schwachen Marktstellung der Konsument*innen gegenüber den Unternehmen. Die Nutzung der Web-Anwendungen bringt kaum spürbare Kosten mit sich, da sie nicht gegen Geld, sondern gegen die Preisgabe eines Teils der Privatsphäre erfolgt (Picot et al., 2018). Aus verhaltensökonomischer Perspektive begünstigen solche Marktbedingungen Affektentscheidungen zulasten rationaler Kosten-Nutzen-Abschätzungen (Jentzsch, 2017). Mit dem Begriff des Privatsphären-Paradoxons (privacy paradox) wird das häufig zu beobachtende Phänomen bezeichnet, dass das tatsächliche Verhalten im Internet in Bezug auf die Preisgabe persönlicher Daten nicht mit den intrinsischen Präferenzen übereinstimmt, die geäussert werden, wenn man sich nicht in einer unmittelbaren Nutzungssituation befindet (Lamla & Ochs, 2019). Es sind die intransparenten Bedingungen der Datenökonomie, die ganz im Sinne des vorherrschenden Big-Data-Geschäftsmodells solche Verhaltensanomalien ermöglichen und verstärken.

Die Verhaltensanreize, welche die Big-Data-Ökonomie sowohl den Konsument*innen als auch den anbietenden Unternehmen setzt, erweisen sich sowohl unter ökonomischen (suboptimale Entscheidungen der Marktteilnehmer*innen) als auch unter ethischen Gesichtspunkten (verhinderte Ausübung der individuellen Selbstbestimmung) als problematisch. Mulgan & Straub weisen diesbezüglich auf den Zusammenhang zwischen der Möglichkeit von Wertschöpfung und dem Grad der Kontrolle über die persönlichen Daten hin: Fehlende Kontrolle erhöht das Risiko des Missbrauchs persönlicher Daten, was im Anschluss das Vertrauen in die datennutzenden Unternehmen und Organisationen unterminiert. Fehlendes Vertrauen wiederum führt zu einem Rückgang der Bereitschaft, die persönlichen Daten zu teilen, was die Wertschöpfungsmöglichkeiten vermindert. Mulgan & Straub (2019) sprechen daher von einem Zwillingsproblem: Die optimale Antwort auf die fehlende Kontrolle läge in der Einschränkung des Datenaustauschs, die Realisierung von Wertschöpfungspotenzialen (in ihrem Beitrag auch im Sinne von *Public Value*) würde hingegen mehr Austausch und Verlinkung von Daten erfordern.

6 Personen, die ihre Daten bekanntgeben, werden im Folgenden als Bürger*innen bezeichnet. Im Datenschutzrecht entspricht dies dem Begriff der betroffenen Personen bzw. Datensubjekte.

7 Dieser Abschnitt konzentriert sich auf die Herausforderungen im Rahmen der Teilung persönlicher Daten. Daneben existieren Datenteilungsmodelle (so z.B. im Falle von Open Data bzw. Open Government Data), bei denen nicht Fragen der Privatsphäre, sondern Verbesserungen und Erleichterungen bezüglich des Datenzugangs im Zentrum stehen (Jarchow & Estermann, 2015).

Obwohl sich der Fokus dieser Studie primär auf den Austausch zwischen denjenigen Akteuren richtet, die sich im datenökonomischen Umfeld bewegen, sollte der Umgang staatlicher Stellen mit den ihnen anvertrauten oder von ihnen erhobenen Daten ebenfalls Erwähnung finden. Für die Umsetzung der in diesem Zusammenhang bedeutsamen europäischen-Deklaration zu E-Government[8] (Tallinn-Deklaration) von 2017, die u.a. die Beachtung der Prinzipien von «*once only*», Vertrauenswürdigkeit und Sicherheit, Offenheit und Transparenz sowie Interoperabilität fordert, bildet die Einrichtung vertrauenswürdiger Datenräume ebenfalls eine grundlegende Voraussetzung. Diese werden jedoch weniger aus der Perspektive der digitalen Selbstbestimmung diskutiert, sondern eher unter dem Gesichtspunkt verbesserter Effizienz und Benutzerfreundlichkeit staatlicher Dienstleistungen sowie der Schaffung von Public Value. Die nachfolgenden Ausführungen hinsichtlich der zentralen Herausforderungen können daher auch auf den Bereich staatlicher Daten übertragen werden, soweit sie nicht ausschliesslich Mechanismen der ökonomisch motivierten Datensammlung und -nutzung betreffen.

In der Literatur werden die Probleme und Herausforderungen, die sich im Rahmen der Suche nach einer optimalen Balance zwischen der Kontrolle über die persönlichen Daten und der wirtschaftlichen Nutzung von Innovationspotenzialen stellen, auf unterschiedlichen Ebenen angesiedelt und diskutiert. In den folgenden Abschnitten werden die Herausforderungen einerseits auf einer individuellen Ebene, andererseits auf einer kollektiven Ebene verortet.

2.2.1 Zentrale Herausforderungen auf individueller Ebene

Die Bekanntgabe persönlicher Daten, um im Gegenzug eine bestimmte Dienstleistung zu erhalten (oder anderen diese zu ermöglichen), erfolgt zum Preis einer Einschränkung der Privatsphäre (Picot et al., 2018). Dies gilt unabhängig von der konkreten Ausgestaltung der Transaktion bzw. der Frage, ob die Daten vom Individuum direkt zu einer Big-Data-Unternehmung gelangen (wie es heute die Regel ist) oder ob sie im Rahmen eines *Datenraum*-Modells[9] zugänglich gemacht werden. In der Literatur wird darum die geeignete Ausgestaltung des individuellen Entscheidungskontexts als eine erste wichtige Herausforderung definiert.

2.2.1.1 Verbesserung der Informationsgrundlagen

Verständlichkeit der Informationen

Die Bedingungen für die Aushändigung persönlicher Daten müssen auf die Fähigkeiten und die zeitliche Verfügbarkeit des oder der Durchschnittsnutzer*in ausgerichtet sein. Die für einen wirklich informierten Entscheid benötigten Informationen über die Verwendung sowie über die Kontroll- und Modifikationsmöglichkeiten der persönlichen Daten müssen transparent dargestellt und allenfalls mit visuellen Hilfsmitteln unterlegt sein (Data Critiques, 2019; O'Hara, 2019; Picot et al., 2018). Die Bürger*innen müssen in die Lage versetzt werden, die Folgen ihrer jeweiligen Entscheidung im Rahmen der Big-Data-Ökonomie abschätzen zu können. Nissenbaum (2011) weist in diesem Zusammenhang allerdings darauf hin, dass es ein Transparenz-Paradoxon (transparency paradox) zu überwinden gilt: Die umfassende Information über alle wichtigen Einzelheiten steht in Konflikt mit dem Anspruch auf einfache Verständlichkeit. Es soll also weniger die Ausführlichkeit, sondern die Angemessenheit im Vordergrund stehen.

Unabhängige Prüf- und Kontrollinstanzen für Privacy-Bedingungen

Eine Möglichkeit, der im vorangehenden Abschnitt formulierten Herausforderung zu begegnen, besteht im Sichtbarmachen anhand von systematischen Vergleichen und Visualisierungen. Bei physischen Produkten oder auch für einzelne Dienstleistungen bestehen unabhängige Organisationen (z.B. TÜV oder Stiftung Warentest in Deutschland) oder staatlich geförderte Bewertungssysteme (z.B. die europaweit eingesetzte Energieetikette bei elektrischen Geräten oder die «Nutri-Score»-Kennzeichnung bei Lebensmitteln), welche die Güte eines Produkts aufgrund transparenter Kriterien beurteilen (Picot et al., 2018). Ein Bewertungsraster, dessen Ergebnis für die Konsument*innen intuitiv und auf einen Blick verständlich dargestellt wird, trägt zur

8 https://www.newsd.admin.ch/newsd/message/attachments/49838.pdf
9 Die Datenethikkommission der Bundesregierung (2019, S. 133) subsumiert solche Modelle gesamthaft unter dem Begriff der „Personal Information Management Systems" (PIMS).

Transparenzbildung und zur verbesserten Information der Konsument*innen bei, ohne dass die negative Seite des Transparenz-Paradoxons zum Tragen kommt.

Kenntnisstand über die Datenökonomie und die Folgen des Datenteilens

Eine Information ist sinnlos, wenn der oder die Adressat*in nicht versteht, zu welchem Zweck sie erfolgt. Die Bürger*innen müssen daher ein tieferes Bewusstsein darüber gewinnen, wie die Mechanismen der Big-Data-Ökonomie und ihre Geschäftsmodelle funktionieren sowie welche Möglichkeiten bezüglich der Verwendung, Bearbeitung und Analyse von persönlichen Daten bestehen (Data Critiques, 2019). Dies bildet die Voraussetzung dafür, dass diese eine aktivere, selbstbestimmte Rolle einnehmen können (Jarchow/Estermann 2015). Dazu reicht es aus, wenn die Bürger*innen die grundlegenden Problemfelder kennen, die beispielsweise die von Data Critiques (2019, S. 10–11) genannten vier ethischen Dilemmata des Datenteilens umfassen:

1. Das Teilen persönlicher Daten bedeutet auch Teilen von Informationen über andere (wie z.B. Familie, Freunde).
2. Auch anonymisierte Daten können zur Erkennung kollektiver Muster genutzt werden.
3. Das Teilen von Daten tangiert auch diejenigen, die sich bewusst dagegen entschieden haben.
4. Daten, die auf dem Beitrag mehrerer Personen beruhen (shared provenance), ziehen kaum aufzulösende Fragen über Nutzungs- bzw. Teilungsrechte nach sich.[10]

2.2.1.2 Anreize für die individuelle Teilnahmebereitschaft

Ein geringes Bewusstsein über die Mechanismen der Datenökonomie und die Wege, wie Big-Data-Unternehmen an persönliche Daten gelangen können, dürfte zumindest zu Beginn auch zu einem eher geringen Interesse an der individuellen Registrierung bei vertrauenswürdigen Datenräumen führen (Delacroix & Lawrence, 2019). Es wird daher entscheidend sein, den Bürger*innen die richtigen Anreize zu setzen, um die Attraktivität der Beteiligung an Datenräumen zu steigern. Neben der Vertrauenswürdigkeit spielt die Abnahme der täglichen Last des persönlichen Datenmanagements eine wichtige Rolle (Blankertz, 2020; O'Hara, 2019). Der Aufwand der Teilnahme an einem Datenraum muss darum erkennbar gering sein, auch in Bezug auf einen späteren Anbieterwechsel (Sicherstellen einer einfach zu handhabenden Daten-Portabilität bzw. Interoperabilität der Datenräume; vgl. Datenethikkommission der Bundesregierung (2019)).

Eine besondere Herausforderung stellt diesbezüglich die Ausgestaltung der individuellen Partizipationsmöglichkeiten dar. Es ist davon auszugehen, dass sich nur sehr wenige Bürger*innen aktiv in die internen Entscheidungsprozesse des oder der Datenräume, an denen sie teilnehmen, einbringen wollen und können. Verschiedentlich hervorgehobene partizipative bzw. deliberative Prozesse (Hardinges et al., 2019) klingen gut, werden aber für sich genommen kein repräsentatives Meinungsbild der an einem Datenraum beteiligten Bürger*innen schaffen. Aus der politischen Partizipations- und Repräsentationsforschung ist bekannt, dass mehr formelle Mitwirkungsmöglichkeiten nicht zu einer höheren und vor allem gleichmässigeren Teilnahme der beteiligten Gruppen führen; die Bürger*innen müssen zur Beteiligung an den Entscheidungsprozessen befähigt sein, was u.a. zeitliche Ressourcen und das entsprechende Interesse resp. den notwendigen Kenntnisstand voraussetzt (Bühlmann et al., 2013; Linder & Mueller, 2017). Umso wichtiger ist es, mittels klarer Governance-Vorgaben, deren Einhaltung von einer Regulierungsbehörde auch wirksam überwacht wird, die grundlegenden Interessen der beteiligten Bürger*innen zu wahren und die Datenraumbetreiber an ihre Pflicht zu Rechenschaft und Verantwortlichkeit gegenüber denjenigen Beteiligten zu erinnern, deren Position es gegenüber der heutigen Situation zu verbessern gilt (vgl. dazu Abschnitt 2.2.2 sowie Abschnitt 4.2.1 über die Umsetzung der vertrauenswürdigen Datenräume in der Praxis).

Ein weiterer Anreiz besteht darin, dass die individuelle Teilnahme an Datenräumen kostenlos erfolgen kann.[11] Eine weitergehende, eigentliche Entschädigung für das Überlassen von persönlichen Daten wird hingegen in der Literatur aus mehreren Gründen mehrheitlich abgelehnt: Einerseits ist es schwierig, den Wert individueller

10 Dies zeigt sich spätestens dann, wenn sich eine Person für den Ausstieg aus einem Datenraum oder für einen Wechsel zu einem anderen Anbieter entscheidet, weshalb Delacroix & Lawrence (2019) in der Definition von Ausstiegsmodalitäten eine zentrale Herausforderung auf kollektiver Ebene erkennen.

11 Dies im Gegensatz zu heute bereits existierenden Angeboten einfacher Personal Data Stores, vgl. dazu Kapitel 4, Abschnitt 4.2.2.

persönlicher Datensätze zu bestimmen und der erzielbare Erlös, der sich aus dem Lizenzverkauf an datennutzende Unternehmen und Organisationen ergibt, dürfte für das Individuum gering ausfallen (vgl. Abschnitt 2.1). Ein solches System würde somit ein gewisses Enttäuschungspotenzial auf individueller Ebene in sich bergen bei gleichzeitiger Verteuerung und entsprechenden negativen Anreizen für die Datennutzer (vgl. Abschnitt 2.2.2). Andererseits können monetäre Anreize dazu führen, dass die Bürger*innen zu viele persönliche Daten teilen. Am stärksten betroffen wären ausgerechnet diejenigen Gruppen, welche sich aufgrund des geringen Kenntnisstandes bereits heute am stärksten an der übermässigen Preisgabe ihrer persönlichen Daten beteiligen und eigentlich durch vertrauenswürdige Datenräume geschützt werden sollten (Datenethikkommission der Bundesregierung, 2019).[12]

Dies führt zur Frage, wie verhindert werden kann, dass Datenräume am Ende nur von denjenigen Gruppen genutzt werden, die über relativ grosse Kenntnisse in der Materie verfügen. Delacroix & Lawrence (2019) empfehlen eine Reihe von Begleitmassnahmen, die von breit wirkenden Informationskampagnen bis hin zur Schaffung von «Fall-back»-Lösungen reichen für Personen, die keinen bewussten Entscheid für einen bestimmten Datenraum fällen können oder wollen.[13] Allerdings impliziert eine (staatlich oder privat organisierte) «Datenraum-Auffanggesellschaft» eine Abweichung vom Freiwilligkeitsprinzip, das einen wichtigen Pfeiler für das mehrfach propagierte «liberale Modell» (im Gegensatz zu einem «paternalistischen Ansatz») darstellt (Delacroix & Lawrence, 2019; Jarchow & Estermann, 2015).

2.2.1.3 Veränderbarkeit und periodische Erneuerung getroffener Entscheidungen

Reversibilität von individuellen Entscheidungen

Jede Einschränkung der Privatsphäre und somit jede Datenpreisgabe muss temporär und reversibel sein (Data Critiques, 2019; Picot et al., 2018). Die Bürger*innen müssen die Möglichkeit haben, jederzeit die weitere Nutzung ihrer persönlichen Einträge zu untersagen bzw. deren Löschung zu verlangen. Dasselbe gilt für den Entscheid, aus einem zuvor gewählten Datenraum gänzlich auszuscheiden bzw. einen anderen Datenraum-Anbieter zu wählen Delacroix & Lawrence (2019). Zu diesem Zweck müssen Verfahren definiert werden, die sicherstellen, dass die persönlichen Daten bei einem entsprechenden individuellen Entscheid tatsächlich zurückgezogen, übertragen und/oder gelöscht werden. Dazu sind auch die Möglichkeiten der Datenportabilität sowie der Interoperabilität (zwischen den Datenräumen) auszubauen und deren Benutzerfreundlichkeit deutlich zu vereinfachen (Delacroix & Lawrence, 2019).

Vermeiden der Bequemlichkeitsfalle

Während die quasi-treuhänderische Umsetzung von einmal festgelegten Bedingungen für die Zustimmung zur Nutzung persönlicher Daten sowie die damit verbundene Abnahme der Last des eigenen Datenmanagements ein grosser Vorteil von vertrauenswürdigen Datenräumen darstellt, würde es nicht einem selbstbestimmten Umgang mit den Daten entsprechen, wenn dies entweder unbewusst, aus Sorglosigkeit oder aus purer Bequemlichkeit zu einer neuerlichen Fremdbestimmung, diesmal durch die Datenraumbetreiber, führte. Das zuvor beschriebene Privatsphären-Paradoxon kann sich auch im Rahmen der Teilnahme an Datenräumen manifestieren. Die Datenraumbetreiber dürfen darum nicht mit Blankomandaten ausgestattet werden, sondern die Mandatierung muss zeitlichen und inhaltlichen Beschränkungen unterliegen, sodass die selbstbestimmte Entscheidungshoheit der Datengeber nicht auf Dauer ersetzt wird (Datenethikkommission der Bundesregierung, 2019).

2.2.2 Zentrale Herausforderungen auf kollektiver Ebene

Für die Ausgestaltung von Data-Governance-Modellen besteht eine Vielzahl an Vorschlägen (Hardinges et al., 2019; Mulgan & Straub, 2019; Schneider, 2019), was sich auch in der Praxis zeigt (vgl. Kapitel 4). Gemeinsam ist ihnen zumeist, dass eine von allen beteiligten Parteien (*Stakeholder*) unabhängige Stelle für den Betrieb

12 Darüber hinaus berührt die Frage der Entschädigung für die Datennutzung weitere Fragen bezüglich der rechtlichen Ausgestaltung des Eigentums der persönlichen Daten und/oder deren Nutzniessung. Diese Fragen sind jedoch nicht Gegenstand des vorliegenden Berichts.

13 Anders als von (Delacroix & Lawrence, 2019) vorgeschlagen, muss es sich dabei nicht notwendigerweise um eine staatlich finanzierte Lösung handeln, sondern könnte über eine von der Branche selbst organisierte Auffanggesellschaft (ähnlich wie bei der beruflichen Vorsorge in der Schweiz) geschehen.

des jeweiligen Datenraums zuständig und verantwortlich ist.[14] Die folgenden, aus der Literatur hergeleiteten Probleme und Herausforderungen konzentrieren sich auf Datenräume, welche (auch) für den Austausch persönlicher Daten besorgt sind. Als übergeordnete Zielsetzung kann die Schaffung von robusten und vertrauenswürdigen Rahmenbedingungen für das Teilen von Daten für Unternehmen, Organisationen und Private bezeichnet werden (Royal Academy of Engineering, o. J.). Dies zieht die Frage nach sich, durch was sich ein robuster und vertrauenswürdiger Rahmen auszeichnet bzw. welche Merkmale diesen herbeizuführen vermögen. Die in der Literatur wiederholt genannten Kriterien werden nachfolgend dargestellt.

2.2.2.1 Vermeidung von Interessenskonflikten

Unabhängigkeit des Datenraumbetreibers

Die rechtliche Struktur, die Finanzierung und die internen Entscheidungsmechanismen müssen sicherstellen, dass der Datenraumbetreiber sowohl von den Datennutzern als auch von einzelnen Datengebern (im Falle persönlicher Daten: den Bürger*innen) unabhängig ist. Die Betreiber eines Datenraums sollen keine anderen Interessen als die in den Statuten festgelegten verfolgen (Blankertz, 2020; Schneider, 2019). Konkret bedeutet dies, dass zum einen die Strukturen darauf ausgerichtet sein sollen, zu verhindern, dass sich die Oligopol-Situation der Big-Data-Ökonomie, wie sie in Kapitel 2.1 nachgezeichnet wurde, im Datenraum widerspiegelt. Stattdessen soll die Partizipation vieler ermöglicht und sichergestellt sein und ein möglichst einfaches und transparentes Verfahren zur Repräsentation der Interessen der Bürger*innen definiert sein (Blankertz, 2020; Royal Academy of Engineering, o. J.).[15] Zum anderen muss sichergestellt sein, dass keinerlei Interessenkonflikte (sowohl auf persönlicher als auch auf organisationeller Ebene) zwischen dem Datenraumbetreiber und den Stakeholdern (d.h. den datengebenden und datennutzenden Personen, Organisationen und Unternehmen) bestehen (Delacroix & Lawrence, 2019).

Not-for-Profit-Organisationsmodell

Aus dem Erfordernis der allseitigen Unabhängigkeit und der Verhinderung von Interessenkonflikten ergibt sich als weiteres vertrauensbildendes Merkmal von Datenräumen, dass die rechtliche Struktur einen Non-Profit-Charakter aufweisen muss (Data Critiques, 2019).[16] In der Literatur tritt in diesem Kontext sehr häufig der Begriff des *Data Trusts* auf. Oft wird damit allerdings nicht auf die konkrete, der angelsächsischen Tradition entstammende rechtliche Organisationsform Bezug genommen, sondern auf die Grundidee der von Eigennutzkalkülen befreiten treuhänderischen Verwaltung von anvertrauten persönlichen Daten im Sinne und zugunsten der am Datenraum teilnehmenden Bürger*innen (Hardinges et al., 2019; O'Hara, 2019; vgl. auch Kapitel 4.2.1). Wichtig in diesem Zusammenhang ist, dass jeder Datenraum gegenüber den teilnehmenden Bürger*innen rechenschaftspflichtig ist und bei Fehlverhalten auch haftbar gemacht werden kann (Delacroix & Lawrence, 2019). Daraus lässt sich für den vorliegenden schweizerischen Kontext die Frage ableiten, welche Möglichkeiten die geltende Rechtsordnung für die Schaffung vertrauenswürdiger Rahmenbedingungen bietet bzw. ob für die besonderen Anforderungen für vertrauenswürdige Datenräume neue rechtliche Organisationsformen geschaffen werden müssen.[17]

Finanzierungsmodelle für den nachhaltigen Betrieb

Die Frage der Finanzierung bildet einen wichtigen Aspekt im Rahmen der Beurteilung der Unabhängigkeit und des Vertrauens in einen Datenraum. Das Erfordernis der Unabhängigkeit und der Non-Profit-Struktur schliesst eine Finanzierung über renditeorientierte bzw. einseitige Stakeholder-Interessen vertretende

14 Der Betrieb eines Datenraumes kann, muss aber nicht die Verantwortung für die sichere Datenspeicherung umfassen. So verbleiben die Daten bei dezentral organisierten Datenraummodellen bei denjenigen Entitäten, die die Kontrolle über die Daten ausüben; vgl. O'Hara (2019) sowie Kapitel 4).

15 Unter Beachtung der in Kapitel 2.2.1.4 vorgebrachten Argumente bezüglich ungleicher Partizipation.

16 Dies bedeutet nicht, dass die Organisation keine Gewinne erwirtschaften darf, sondern dass keine renditeorientierte Eigen- oder Fremdkapitalgeber*innen an der Organisation beteiligt sein dürfen. Demgegenüber lässt die Datenethikkommission der Bundesregierung (2019, S. 134) eine privatwirtschaftliche Organisation zu, „wenn dabei der Betreiber an der Verwaltung, und nicht an der Nutzung der Daten verdient." Da auch für diese Organisationsform gemäss Datenethikkommission besondere Treuepflichten gelten und Interessenkonflikte auszuschliessen sind, dürfte der praktische Unterschied zur hier geforderten Not-for-Profit-Struktur allerdings gering ausfallen.

17 In diesem Zusammenhang ist auch zu klären, was mit den in einem Datenraum gehaltenen Daten im Insolvenzfall geschieht. Eine automatische Übertragung an die Gläubiger des insolventen Datenraums dürfte weder mit der digitalen Selbstbestimmung noch mit dem Erfordernis der jederzeitigen Reversibilität individueller Entscheidungen vereinbar sein.

Kapitalgeber*innen aus. Neben dem Modell einer rein staatlichen Finanzierung, das aus unterschiedlichen Gründen (vgl. unten) lediglich in bestimmten ausserordentlichen Fällen zum Zuge kommen sollte, könnte der Betrieb über die Vergabe kostenpflichtiger Lizenzen für den Zugang und die Nutzung der Daten sichergestellt werden (Blankertz, 2020). Hardinges et al. (2019) geben diesbezüglich jedoch zu bedenken, dass aufgrund solcher Lizenzen zusätzliche Hürden aufgebaut werden, was den Anreiz für die Nutzung vertrauenswürdiger Datenräume senkt. Stattdessen wird vorgeschlagen, dass sich die Datenraumbetreiber über Zusatzdienstleistungen im Bereich der Datenverwaltung finanzieren können, die sie für die datennutzenden Organisationen erbringen (z.B. zusätzliche Qualitätskontrollen, Training und Beratung im Bereich Data Science, Zugang zu Datenarchiven, auf die Bedürfnisse der einzelnen Kunden zugeschnittene Datenschnittstellen).

2.2.2.2 Rolle des Staates

Differenziert betrachtet wird die Frage nach der Rolle des Staates. Als sinnvoll wird zumeist das Auftreten des Staates als Regulator (oft werden dafür die Datenschutzbehörden genannt) erachtet, der die grundlegenden Data-Governance-Prinzipien festlegt und überwacht, nach denen die Datenräume organisiert sein müssen und operieren sollen. Der Staat als (exklusiver oder in Konkurrenz zu privaten Angeboten stehender) Betreiber von Datenräumen wird – mit Ausnahme von Daten, die staatliche Stellen selbst erstellen und verwalten – sowohl aus Datenschutz- als auch aus Wettbewerbsüberlegungen heraus skeptisch beurteilt.[18] Einerseits soll staatlicher Missbrauch von Daten verhindert werden, andererseits führt ein liberaler, wettbewerbskonformer Bottom-up-Ansatz eher zu einer Vielfalt an Angeboten, die den unterschiedlichen Bedürfnissen der Stakeholder entsprechen und auf gesellschaftliche Veränderungen auch rascher reagieren können als staatlich betriebene bzw. staatlich vorgeschriebene Monopole (Delacroix & Lawrence, 2019; Jarchow & Estermann, 2015).

Neben der Regulierung fällt dem Staat auch die Rolle der effektiven Durchsetzung der selbst aufgestellten Regeln zu. Dies betrifft potenziell erneut die mit der Datenraum-Regulierung betrauten Behörde, ferner (ggf. in den weiteren Instanzen) das Justizsystem insgesamt. Entscheidend ist, dass die konkrete Ausgestaltung der Durchsetzungsmechanismen den datengebenden Individuen effektive Mittel zur Verfügung stellt, um eine Verletzung ihrer berechtigten Ansprüche durch die Datenraumbetreiber bzw. die datennutzenden Organisationen nötigenfalls anzuzeigen und zu beseitigen. Dadurch werden die Voraussetzungen geschaffen, damit sich ein gewisser Ausgleich der zuvor festgestellten Ungleichgewichte unter den verschiedenen Akteuren in der Datenökonomie einstellen kann.

18 Anders zu beurteilen ist die Frage einer staatlichen Anschubfinanzierung, um eine Grundinfrastruktur aufzubauen (Blankertz 2020).

2.2.3 Übersicht und Verbindung zu den Grundprinzipien

Die zuvor als zentral bezeichneten Herausforderungen werden in der Tabelle nochmals im Überblick dargestellt. Gleichzeitig wird kenntlich gemacht, in welcher Beziehung die Herausforderungen zu den in Kap. 3 genannten Grundprinzipien von vertrauenswürdigen Datenräumen stehen.

Herausforderungen	**Grundprinzipien**
<u>Individuelle Ebene</u>	
1. Verbesserung der Informationsgrundlagen • Verständlichkeit der Informationen • Unabhängige Prüf- und Kontrollinstanzen für Privacy-Bedingungen • Kenntnisstand über die Datenökonomie und die Folgen des Datenteilens 2. Anreize für die individuelle Teilnahmebereitschaft 3. Veränderbarkeit und periodische Erneuerung getroffener Entscheidungen • Reversibilität von individuellen Entscheidungen • Vermeiden der Bequemlichkeitsfalle	• Transparenz, Vertrauen, Verständlichkeit und Vorhersehbarkeit (3.1.1) • Kontrolle (3.1.2) • Solidarität (3.1.3)
<u>Kollektive Ebene</u>	
1. Vermeidung von Interessenskonflikten • Unabhängigkeit des Datenraumbetreibers • Not-for-Profit-Organisation • Finanzierungsmodelle für den nachhaltigen Betrieb 2. Staat als Regulator	• Fairness (3.2.1) • Austausch und hohe Datenqualität (3.2.2) • Interoperabilität (3.2.3) • Skalierbarkeit (3.2.4 • Nachhaltigkeit (3.2.5) • Politikunterstützung (3.2.6) • Wirtschaftswachstum (3.2.7)
<u>Durchsetzungsebene</u>	
Staat als Garant für effektive Durchsetzung	• Einklagbare Durchsetzungs- und Kontrollmechanismen (3.3.1) • Nichtverbindliche Instrumente (3.3.2)

Tabelle 1 Herausforderungen und ihr Bezug zu den Grundprinzipien

2.3 Fazit

Die Geschäftsmodelle der heutigen Big-Data-Ökonomie basieren über weite Strecken auf starken Marktungleichgewichten und Marktversagen. Davon betroffen sind einerseits die Bürger*innen, die zwischen ganz wenigen, in sich geschlossenen Daten-Ökosystemen mit für sie ungünstigen Bedingungen hinsichtlich ihrer Privatsphäre und hohen Kosten im Falle eines Anbieterwechsels auswählen müssen. Andererseits können sich keine alternativen Anbieter in der Datenökonomie etablieren, da die grossen Player keine Daten mit potenziellen Konkurrenten teilen und neue Anbieter praktisch keine Chance haben, ein eigenes Netzwerk aufzubauen, das eine kritische Grösse überschreitet und dadurch für die Nutzer*innen attraktiv wird.

Obwohl formal betrachtet abhängig von deren «informierter Zustimmung», teilen die Bürger*innen ihre persönlichen Daten nicht auf der Basis von Transparenz und Vertrauen, sondern weil ihnen kaum etwas anderes übrigbliebt, wenn sie am gesellschaftlichen Leben teilnehmen möchten, da «digitale Teilhabe (..) zur notwendigen Bedingung sozialer Teilhabe» geworden ist (Lamla & Ochs, 2019, S. 26). Vertrauen ist jedoch entscheidend, wenn die Potenziale des Datenteilens hinsichtlich Innovation, Effizienzgewinne und Benutzerfreundlichkeit für die Wirtschaft und Gesellschaft voll ausgeschöpft werden sollen. Auch wenn sich die Studie primär auf die Beteiligten in der Datenökonomie konzentriert, darf an dieser Stelle nicht unerwähnt bleiben, dass auch der Staat (z.B. im Rahmen der Realisierung des Once-Only-Prinzips) auf das Vertrauen der Bürger*innen und Unternehmen in den Umgang mit Daten angewiesen ist und sich ihm ähnliche Herausforderungen stellen, soweit sie nicht ausschliesslich Mechanismen der ökonomisch motivierten Datensammlung und -nutzung betreffen.

Um dieses Vertrauen herzustellen und eine Balance zwischen persönlicher Kontrolle und den Nutzungspotenzialen zu erreichen, gilt es eine Reihe ungelöster Probleme und Herausforderungen sowohl auf individueller (Bürger*innen-)Ebene als auch auf kollektiver organisatorischer Ebene anzugehen.

Auf individueller Ebene wird in erster Linie die Ausgestaltung des Entscheidungskontexts thematisiert. Die Bürger*innen sollen in die Lage versetzt werden, die Folgen ihrer Entscheidung abschätzen zu können. Dazu ist eine einfach verständliche Form der Kommunikation nötig, die mit angemessener Information und visuellen Elementen (z.B. im Rahmen standardisierter Produktprüfverfahren) möglichst transparent informieren soll. Damit den Bürger*innen der Sinn der Information klar wird, sind Begleitmassnahmen in Form einfacher Botschaften nötig, um die Bevölkerung für die grundlegenden Probleme beim Datenteilen zu sensibilisieren. Darüber hinaus müssen sämtliche die eigene Privatsphäre betreffende Entscheide immer befristet sein und auch jederzeit rückgängig gemacht werden können.

Als weitere Herausforderung für den erfolgreichen Aufbau eines vertrauenswürdigen Systems für die Datenpreisgabe gelten die Anreize, die den Bürger*innen für die Teilnahme gesetzt werden. Einerseits muss sie zu einer deutlichen Abnahme der Last des persönlichen Datenmanagements führen und auch ein späterer Anbieterwechsel muss ohne Wechselkosten vonstattengehen können. Andererseits sollte die Teilnahme an einem Datenraum für die Bürger*innen kostenlos erfolgen können – sie bringen schliesslich bereits ihre persönlichen Daten ein. Über die Frage, ob die datennutzenden Unternehmen und Organisationen eine Entschädigung entrichten sollen, werden in der Literatur unterschiedliche Ansichten geäussert. Gegen eine monetäre Abgeltung spricht jedenfalls, dass dadurch die Anreize für die Unternehmen zur Nutzung vertrauenswürdiger Datenräume gemindert werden bei gleichzeitig voraussichtlich geringen Erlösen für die einzelnen Bürger*innen. Ein besonderes Augenmerk gilt den internen Entscheidungsstrukturen, die zwar partizipativ ausgestaltet sein können, bei denen aber aufgrund bekannter Defizite der Teilnahmefähigkeit und -bereitschaft darauf zu achten ist, dass die Benachteiligung sozial und gesellschaftlich schwächerer Gruppen abgefedert wird. Es gilt zu verhindern, dass die vertrauenswürdigen Räume nur von denjenigen genutzt werden, die über grosse Kenntnisse der Materie verfügen.

Auf der kollektiven Ebene steht die Schaffung robuster und vertrauenswürdiger Datenräume im Zentrum. Die diesbezüglichen Herausforderungen beziehen sich auf die Sicherstellung einer von allen Stakeholdern (datengebende und datennutzende Personen, Organisationen und Unternehmen) finanziell und personell unabhängigen, von jeglichen Interessenkonflikten befreiten Organisationsform. In der Praxis dürfte eine Not-for-Profit-Struktur mit klaren Verantwortlichkeits- und Haftungsregeln für die Datenraumbetreiber am ehesten vertrauensbildend wirken. Inwieweit die heutigen rechtlichen Möglichkeiten dazu ausreichen, wäre abzuklären. Des Weiteren ist die Rolle des Staates zu definieren, sowohl in Bezug auf Finanzierungs- und Regulierungsaspekte als auch auf seine Rolle als Datenlieferant und als Sekundärnutzer von Daten. Die Literatur geht mehrheitlich von einem «liberalen Modell» aus, das den Staat (ähnlich wie beim Telekommunikations- oder Elektrizitätsmarkt) in der Verantwortung als Regulator und Aufsicht sieht, nicht aber als permanenter Finanzierer oder Betreiber. Hinsichtlich der Herausforderung eines nachhaltigen Finanzierungsmodells für Datenraumbetreiber muss darauf geachtet werden, dass die Anreize für die datennutzenden Unternehmen zur Teilnahme an einem vertrauenswürdigen Austauschsystem nicht über finanzielle Belastungen zunichte gemacht werden.

3 Grundprinzipen und Voraussetzungen für vertrauenswürdige Datenräume

Das folgende Kapitel widmet sich basierend auf einer Literaturrecherche den Grundprinzipien und Voraussetzungen, denen Datenräume zu genügen haben, um als vertrauenswürdig zu gelten. Bei der Analyse hat sich gezeigt, dass diese Grundsätze drei verschiedenen Ebenen zugeordnet werden können, was die Übersicht und Verständlichkeit erhöht: Prinzipien, die Individuen direkt betreffen könnten; Prinzipien und Zielvorstellungen, die weniger von einzelnen Individuen, sondern von Datenräumen per se umzusetzen sind; und schliesslich zwei Voraussetzungen auf der Durchsetzungsebene, damit sich die Grundprinzipien entfalten können. Im Wesentlichen sind diese Ebenen voneinander abgrenzbar, trotzdem ergeben sich Schnittmengen, die im Rahmen dieser Studie nicht zentral sind. Auf jeden Fall ist für vertrauenswürdige Datenräume das Zusammenspiel aller Ebenen entscheidend.

3.1 Individuelle Ebene

Unter diesem Kapitel werden Grundprinzipien behandelt, die aller Voraussicht nach in Rechten und Pflichten münden könnten, die vor Gerichten direkt durchsetzbar wären oder dies heute sogar bereits sind (vgl. insbesondere das Schweizer Datenschutzgesetz auf Bundesebene, DSG). Diese Ebene lehnt sich stark an den Wissens- und Praxisstand der Ethik im Big-Data- und KI-Bereich an. Dort lautet die goldene Regel: Behandle die Daten anderer wie deine eigenen (Tranberg et al., 2018).

Grundprinzipien	Beschreibung	Empfehlungen
Transparenz, Vertrauen, Verständlichkeit und Vorhersehbarkeit	Informationen bereitstellen, verständlich darstellen und effektiv kommunizieren, sodass darauf aufbauend gesicherte Vorhersagen getroffen werden können.	Einfache Hilfsmittel, um komplexe Informationen zu vermitteln, bspw. die Aussagekraft von Daten über die Persönlichkeit.
		Frühzeitige, aktive Information, die die Anliegen der Informationsempfangenden ernst nimmt.
		Gewisse transparent zu machende Minimalinhalte sind (verbindlich) festzulegen.
		Ein öffentliches Register für die Aktivitäten öffentlicher Akteure in Datenräumen, sowie von Privaten, wenn deren Aktivität ein hohes Risiko birgt.
Kontrolle	Ihr Grundrechtsschutz gebietet, dass beteiligte Personen selbst steuern und bestimmen können, wer ihre Daten wofür und wie verwenden darf. Dazu gehört, dass sie bei Bedarf diese Entscheidungsmacht an einen vertrauenswürdigen Dritten delegieren können. Beinhaltet Cybersicherheit, Wahlfreiheit und das Recht auf Datenportabilität.	Verbindliche Handlungsanleitungen, falls die Kontrolle verloren gehen sollte (z. B. Information der betroffenen Personen).
Solidarität	In bestimmten Situationen ist das Teilen von Daten ethisch geboten.	Anreize zum Teilen, wo die Generierung von Public Value dies rechtfertigt.
		U. U. Zwang zum Teilen als ultima ratio.

Tabelle 2 Grundprinzipien individuelle Ebene

3.1.1 Transparenz und Vertrauen basieren auf Verständlichkeit und Vorhersehbarkeit

Transparenz und Vertrauen sind untrennbar mit Verständlichkeit (Intelligibility) und Vorhersehbarkeit (Predictability) verwoben (Tranberg et al., 2018). Das heisst, Informationen müssen nicht nur transparent gemacht werden, sondern die Involvierten müssen die zur Verfügung gestellten Informationen auch verstehen und auf deren Grundlagen Vorhersagen treffen können (Bostrom & Yudkowsky, 2011; Bossmann et al., 2018; AI HLEG, 2020b; Algorithm Watch, 2020). Dies schliesst ebenfalls die autonome Regulierung des Zugangs Dritter dazu ein. Sowie im Umkehrschluss den Schutz vor unbefugtem Zugriff, worunter auch *Cybersicherheit* zu subsumieren ist (vgl. ausserdem zur Cybersicherheit Kapitel 3.2.4, Skalierbarkeit zwecks dezentraler Datenräume)

Wo die Verständlichkeit fehlt, bzw. wo die zu vermittelnden Informationen von einer besonderen Komplexität gekennzeichnet sind, die die Informationskosten übermässig erhöht (vgl. Kapitel 2.1), empfehlen wir einfache Hilfsmittel. Beispielsweise, um den Wert der Daten und deren Aussagekraft einschätzen zu können (s. Kapitel 2.2.1.1, Verbesserung der Informationsgrundlagen):

- Unabhängige Prüf- und Kontrollinstanzen für Privacy-Bedingungen
- Einschätzung durch offizielle staatliche Stelle, u. U. kombiniert mit der Einordnung auf einer einheitlichen Skala analog den aktuellen Energie-Etiketten;
- Markierung von Daten, die eine hohe Sensitivität/ein besonderes Risiko aufweisen;
- Anzeige, wie viele Daten ein Anbieter bereits von der beteiligten Person besitzt unter Hinweis auf das Risiko von Verknüpfungen bzw. Persönlichkeitsprofilen.

Die Verständlichkeit ist auf eine wirksame Kommunikation angewiesen. Dazu gehören effektive Kanäle (z. B. E-Mail; Smartphone-App) sowie eine frühzeitige, aktive Kommunikation, die die Adressaten und ihre Anliegen ernst nimmt (Christen et al., 2020).

Die Informationen müssen den Involvierten erlauben, das Ergebnis vorherzusagen. Die KI-Expertengruppe der EU formuliert es so: «Es muss sichergestellt sein, dass das Planungsergebnis mit der Eingabe übereinstimmt und dass die Entscheidungen so getroffen werden, dass der zugrunde liegende Prozess validiert werden kann» (AI HLEG, 2020b, S. 27). Es handelt sich dabei um eine Zusicherung, die aus dem Geschäftsverkehr unter dem Schlagwort 'Rechtssicherheit' bekannt ist: Verträge können im Wissen darum entworfen und unterschrieben werden, wie sie ausgeführt werden, was die Transaktionskosten verringert (Coase, 1937; Williamson, 1985). Durch Rechtssicherheit bzw. Vorhersagbarkeit wird die persönliche Entfaltung erst möglich (Bostrom & Yudkowsky, 2011).

Zu den transparent zu machenden Minimalinhalten gehören gemäss der Literatur (AI HLEG, 2020a; Algorithm Watch, 2020; Christen et al., 2020; Schieferdecker et al., 2018) und eigenen Reflektionen:

- Erfassung, Nutzung und Verarbeitung von Daten per se;
- Zweck davon;
- Nachvollziehbarkeit der Nutzung und des Zugangs durch Dritte;
- Eindeutige Identifikation (auch zwecks Durchsetzung, s. dritte Ebene). Dafür existieren verschiedene Varianten von sogenannten Identitäts- und Vertrauensmanagement-Systemen: beispielsweise OpenID, OAuth, PKI, Blockchain, DNSSEC, qualifizierte elektronische Signaturen, Chipkarten;
- Die im Datenraum geltenden Regeln. Wo lange AGBs anfallen, sind diese zusammenzufassen und verständlich darzustellen;
- Involvierte Akteure im Raum, deren Beziehungen zueinander (Rollen und Hierarchien), sowie die Prozesse für (fundamentale) Entscheidungen;
- Business-Model, d. h. das rechtliche und finanzielle Konstrukt, insbesondere mit belastbaren Angaben darüber, was im Falle einer allfälligen Liquidation der Organisation mit den Daten geschieht;
- Die durch bestimmte Kategorien von Nutzenden (z. B. Forscher, Journalisten, NGOs) geltend machbaren Rechte;
- Gegebenenfalls angewendete Algorithmen und deren Zweck;
- Gegebenenfalls Umstand, dass Daten ins Ausland übermittelt werden und das dortige Datenschutzniveau.

Besonders hervorzuheben aus der obigen Liste ist die eindeutige Identifikation. Sie ist von entscheidender Bedeutung im häufig anonymen Internet. Sie stiftet Vertrauen und ist unumgänglich, um die richtige Ansprechperson zu identifizieren sowie berechtigte Ansprüchen geltend zu machen, falls nötig (vgl. Kapitel 3.3, Durchsetzung der Grundprinzipien)

Staatliche Akteure und gewisse Private könnten ihre Aktivitäten in Datenräumen in einem zentralen Register führen und veröffentlichen. Eine ähnliche Meldepflicht existiert auf Bundesebene bereits für die Datensammlungen öffentlicher Verwaltungen und Privater unter bestimmten Voraussetzungen, insbesondere bei regelmässiger Bearbeitung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen (Art. 11a DSG). Private sind auch zu einer aktiven Information der betroffenen Person bei der Beschaffung von Daten dieses Typs verpflichtet (Art. 14 DSG), Bundesorgane hingegen bei jeder Beschaffung (Art. 18a DSG).

3.1.2 Kontrolle - zwischen Grundrechtsschutz und Solidarität

Das zweite grosse Grundprinzip auf der individuellen Ebene ist die Kontrolle: Die beteiligten Personen sollen steuern und selbst bestimmen können, wer ihre Daten wofür und wie verwenden darf. Wenn es keiner eingegangen Abmachung entgegensteht, sollte die Entscheidung zur Datenfreigabe grundsätzlich reversibel sein (vgl. Kapitel 2.2.1.3, Veränderbarkeit und periodische Erneuerung getroffener Entscheidungen). Werden die Personendaten nicht mehr für den Zweck verwendet, für den sie das Einverständnis der betroffenen Person geniessen, gebietet der Grundsatz der Verhältnismässigkeit deren Löschung (Art. 4 Abs. 2 in fine DSG). Die Frage, ob eine Person, die ihr Einverständnis zurückzieht, auch die Löschung der bereits geteilten Daten verlangen kann, sollte sich gleich wie die Möglichkeit der Reversibilität entscheiden: indem das Interesse an der Vertragstreue (pacta sunt servanda) gegen das Interesse an der Löschung abgewogen wird. Dabei sind alle entscheidenden Umstände miteinzubeziehen, namentlich die Sensibilität der Daten. Auf alle Fälle wird das fundamentale Interesse an pacta sunt servanda nicht einfach zu überwiegen sein.

Die beschriebene Kontrolle ist nicht zuletzt ein Erfordernis, das aus den Grundrechten der Bundesverfassung fliesst. Die Idee von speziellen Digitalrechten geht wohl auf John Perry Barlows (1996) Declaration of Independence zurück, die als Reaktion auf die Verabschiedung des Telecommunications Act im US-Kongress zu werten ist. Barlows Grundgedanke war die Bewahrung der Freiheit im Internet. Im Fokus von Regierungen stand in den 00er Jahren vor allem die Etablierung von Rechten, die den Zugang zum Internet garantierten. Mit der Normalisierung des Online-Seins und der Einbettung von sozialen Medien im Alltag der Menschen wurde aber auch der Anwendungsbereich der Grundrechte im digitalen Raum herausgebildet (Dunleavy & Margetts, 2015). Speziell hervorzuheben sind die folgenden Grundrechte der Schweizer BV (Christen et al., 2020; Datenethikkommission der Bundesregierung, 2019; EDA, 2020):

- **Freie Entfaltung der Persönlichkeit** (Art. 10 Abs. 2 BV) und **informationelle Selbstbestimmung** (Art. 13 Abs. 2 BV): Diese Grundrechte ergänzen sich gegenseitig, wobei letztgenanntes häufig einschlägiger ist, beziehungsweise ersteres eher subsidiär zum Tragen kommt. Der Anspruch auf das erläuterte Konzept von Kontrolle leitet sich insbesondere hieraus ab. Der oder die Grundrechtsträger*in kann selbst darüber bestimmen, welches Bild von ihm oder ihr die Aussenwelt aufgrund der freigegebenen Daten haben darf. Auf die Pendants von Art. 13 Abs. 2 BV in der Charta der Grundrechte der EU (Art. 7 und 8) stützte sich auch der EuGH, als er in einem wegweisenden Urteil das Recht auf Vergessen postulierte (Hürlimann, 2014).

- **Gleichbehandlungsgebot** (Art. 8 Abs. 1 BV) und **Diskriminierungsverbot** (Art. 8 Abs. 2 BV): Vertrauenswürdige Datenräume dürfen keine Gruppe von Menschen aufgrund eines einenden Merkmals ohne Rechtfertigung diskriminieren. Jeder Mensch hat grundsätzlich Anspruch auf gleiche Behandlung, das heisst gleichen Zugang zu Datenräumen und gleiche Rechte und Pflichten in derselben Rolle.

- **Menschenwürde** (Art. 7 BV): Die Würde eines Menschen ist grundrechtlich absolut geschützt. Jede Verletzung ist verboten. Wo Daten oder ihre Bearbeitung die Menschenwürde tangieren, ist folglich die Bearbeitung davon oder möglicherweise gar der Datenraum selbst nicht tolerierbar.

Die Bearbeitung von Daten ist gemäss dem Verhältnismässigkeitsprinzip (Art. 5 Abs. 2 BV) stets in Alternativen zu prüfen: *anonymisiert*, durch *Differential Privacy*, *pseudonymisiert* oder ohne Verschleierung in Reincode. Zu den Alternativen und der Nutzungserlaubnis zugunsten Dritter sollte Wahlfreiheit herrschen. Das bedeutet, der vor der Wahl stehenden Person sollte keinerlei Nachteil oder Schlechterstellung erwachsen aus dem Umstand, dass sie sich für die eine statt der anderen Option entscheidet. Untersagt ist damit beispielsweise, den Abschluss eines Vertrags von der Preisgabe persönlicher Daten abhängig zu machen, wenn dies für die Abwicklung des Vertrags nicht nötig ist (Kopplungsverbot). Wo eine Schlechterstellung hingegen gerechtfertigt oder unausweichlich ist, sind zumindest die Konsequenzen anzugeben.

Zur Kontrolle über die eigenen Daten gehört nicht nur die Zugriffsberechtigung, sondern auch das Recht auf *Datenportabilität*. Form und Ausgestaltung haben sich nach dem neuen, frühestens 2022 in Kraft tretenden Schweizer Datenschutzgesetz zu richten (neuer Art. 28). Die Datenportabilität wird ergänzt durch *Interoperabilität* (Datenethikkommission der Bundesregierung, 2019).

Im Zuge des expandierenden wirtschaftlichen Potenzials von Big Data (s. Kapitel 2.1, grundlegende Merkmale und Problemstellungen in der Datenökonomie) ist mit einer Zunahme von Datenräumen zu rechnen. Damit verbunden ist die Zunahme an Aufwand für das Individuum, um die Verwendung der eigenen Personendaten in den verschiedenen Räumen zu kontrollieren. Die Inanspruchnahme von immer mehr zeitlichen Ressourcen kann zu einem faktischen Kontrollverlust für die Betroffenen führen. Es muss deshalb auch offenstehen, die Überwachung der Verwendung der eigenen Daten Dritten zu delegieren und ihnen diesbezüglich nötige Vollmachten zu erteilen. Etwa indem dass diese das Einverständnis in Vertretung der Betroffenen zur Verwendung der Daten geben können. Zur Frage, wie diese Dritten genau beschaffen sein könnten, s. Kapitel 4.2, Institutionen zur vertrauenswürdigen Datensteuerung.

Der beschriebene Kontrollanspruch steht in einem Spannungsfeld zu den Situationen, wo das Teilen von Daten ethisch geboten sein kann. Denn negative Effekte erwachsen der Gesellschaft nicht nur dort, wo zu viel, sondern auch da, wo zu wenig Daten geteilt werden. Ausserdem sind Daten nicht-rivale Güter, was sie ohne Mehrkosten beliebig vervielfältigbar macht (vgl. Kapitel 2.1). Daher kann es die Solidarität erfordern, dass Daten geteilt werden. Das Teilen kann, wo der gesellschaftliche Nutzen klar überwiegt, durch Zwang durchgesetzt werden. Ansonsten ist zugunsten des Public Value über Anreize oder zumindest Sensibilisierungen nachzudenken (Data Critiques, 2019; Datenethikkommission der Bundesregierung, 2019).

Wichtig scheint uns, dass auch verbindliche Handlungsanleitungen feststehen, wenn die Kontrolle verloren gehen sollte, etwa bei einem erfolgreichen Cyberangriff oder mangelhafter Umsetzung anderer direkt durchsetzbarer Prinzipien. Dies schafft einerseits Transparenz, andererseits kann so auch unter Umständen wichtige Zeit eingespart werden, falls die Betroffenen schnellstmöglich reagieren müssen, beispielsweise um ihre Konten zu sperren (O'Hara, 2019).

3.2 Kollektive Ebene

Auf dieser Ebene befinden sich diejenigen Grundprinzipien, die die anzustrebenden Rahmenbedingungen von vertrauenswürdigen Datenräumen definieren. Die daraus fliessenden Rechte und Pflichten können unmöglich für alle Datenräume a priori festgelegt werden, sondern müssen nach Betrachtung aller Umstände des Einzelfalls gedeutet werden (etwa die Fairness, vgl. 3.2.1; wohingegen die zu kommunizierenden Minimalinhalte der Transparenzpflicht allgemeingültig sind, vgl. 3.1.1). Ab 3.2.4 finden sich die Grundprinzipien, die eher als übergeordnete Ziele zu verstehen sind. Dem ganzen Kapitel ist gemein, dass, anders als auf der individuellen Ebene, diese Grundprinzipien nicht durch die Involvierten unmittelbar durchsetzbar sind. Allenfalls könnte eine staatliche Regulationsbehörde über deren Einhaltung wachen.

Grundprinzipien	Beschreibung	Empfehlungen
Fairness	Kosten und Nutzen des Sammelns, Speicherns und Verwendens von Daten fair verteilen	Vertragsvorlagen und Checklisten bereitstellen Vermeidung von Interessen-konflikten (vgl. Kapitel 2.2.2.1)
Austausch und hohe Datenqualität	Mehr Austausch führt zu mehr verfügbaren Daten. Ohne Qualitätsmanagement generiert sich daraus jedoch kein Mehrwert.	Unterhalt der Daten regeln, bspw. in einem Vertrag
Interoperabilität	Umfasst mindestens technische Infrastruktur, Quantität und Qualität von Daten, sowie Formate und Label.	Bestehende Standards mit Bedacht auswählen, klar festlegen und kommunizieren
Skalierbarkeit	Eigenschaft der Grundprinzipien, sich den wachsenden oder auch kleiner werdenden Gegebenheiten möglichst flexibel anpassen zu können.	Unterstützung und Begleitung bei der Installation, Befüllung und Nutzung von dezentralen Datenräumen, u. U. durch eine Behörde
		Schärfung des Bewusstseins für den potenziellen Wert dezentraler Datenräume
		Analyse der Datennutzung und Erschliessung neuer Quellen
Nachhaltigkeit	Erreichung insb. der globalen Nachhaltigkeitsziele und des Pariser Klimaabkommens	Daten nutzen zwecks Umweltmonitoring und Effizienzsteigerung
Politikunterstützung	Mehr und qualitativ gute Daten sollen einsetzbar sein, um bessere politische Entscheide, genauere Information, mehr Partizipation und eine effizientere Verwaltung zu fördern.	
Wirtschaftswachstum	Wachstum durch Kompatibilität mit dem insb. europäischen Ausland sowie durch Austausch und Zusammenarbeit verschiedener Akteure	Anreize für Datenräume, sich eurokompatibel zu gestalten, bekanntmachen
		Netzwerke schaffen und fördern, in denen sich Vertreter*innen verschiedener Branchen austauschen können

Tabelle 3 Grundprinzipien kollektive Ebene

3.2.1 Nur faire Datenräume verdienen Vertrauen

Datenräume müssen den darin Involvierten gerechte Entschädigungen bieten (Datenethikkommission der Bundesregierung, 2019; Open Data Institute, o. J.; Royal Academy of Engineering, o. J.; Schieferdecker et al., 2018). Damit sind die beteiligten Personen, die Datennutzenden und die Datenproduzenten alle gleichsam gemeint. Die Royal Academy of Engineering (o. J., S. 4) benutzt folgenden Wortlaut: “Ensuring that costs and benefits of collecting, storing and using data are fairly distributed.” Für die deutsche Datenethikkommission der Bundesregierung (2019) ist die Fairness Teil einer gerechten Wirtschaftsordnung, die allen einen angemessenen Zugang zu Datenräumen und deren Vorteile zuzustehen hat («Zugangs- und Verteilungsgerechtigkeit», ibid., S. 46). Die Entschädigung kann auch beziehungsweise sollte nicht primär monetärer Natur sein; um zu sehen, wie Interessenkonflikte vermieden werden könnten, vgl. Kapitel 2.2.2.1

(Unabhängigkeit des Datenraumbetreibers; Not-for-Profit-Organisation; und Finanzierungsmodelle für den nachhaltigen Betrieb).

Da dieses Prinzip gleich wie alle anderen auf der kollektiven Eben nur schwer allgemeinverbindlich in Form von gesetzlichen Normen vorgeschrieben werden kann – und dies auch nicht mit der Vertragsfreiheit vereinbar wäre – empfiehlt sich die Regelung dieser Punkte durch gegenseitiges Übereinkommen der involvierten Akteure. Um diesen die Ausarbeitung zu erleichtern, schlagen wir Vertragsvorlagen und Checklisten zu den wichtigsten Inhalten vor. Wo Datenräume besonders sensible Daten (etwa im Sinne von Art. 3 lit. c DSG; allenfalls auch weitere) enthalten, wäre zur Erhöhung des Vertrauens auch das obligatorische Einholen einer staatlichen Genehmigung des Übereinkommens eine diskutable Option. Schieferdecker et al. (2018) haben beispielsweise einen Fragebogen entwickelt, den Gemeindeverantwortliche selbst beantworten sollten beim Entwurf eines solchen Vertrags (weiteres Bsp. bei Royal Academy of Engineering, o. J.)

3.2.2 Austausch und Qualität

Datenräume sollen durchlässig sein (vgl. auch Kapitel 3.1.2, Datenportabilität, und Kapitel 3.2.1, Zugangsgerechtigkeit). Sie sollen sich untereinander austauschen können, verschiedene Datensätze miteinander kombinieren und so den datenbasierten Erkenntnis- und Effizienzgewinnen noch mehr Vorschub leisten (Christen et al., 2020). Die Attraktivität erweitert sich automatisch: stehen mehr Daten zur Verfügung, werden Datenräume auch für noch mehr Datenproduzenten und -nutzende interessant und umgekehrt (Schieferdecker et al., 2018, S. 178, sprechen von „Netzwerkeffekten“, vgl. auch Kapitel 2.1). Dies gilt auch für die vielversprechenden Technologien von Crowd-Sensing und -Sourcing, die heute noch weitgehend ungenutzt sind durch die öffentliche Verwaltung, aber eine wertvolle Datenquelle darstellen würden (Datenethikkommission der Bundesregierung, 2019; Schieferdecker et al., 2018).

Um dies zu erreichen sind zwei Aspekte von entscheidender Bedeutung: Erstens müssen die Daten miteinander kompatibel und zusammenführbar sein. Das bedingt Interoperabilität (s. 3.2.3), offene Schnittstellen und offene Standards (Schieferdecker et al., 2018) – ein Aspekt, der auch für die effektive Umsetzung der Datenportabilität (s. 3.2.1) unabdinglich ist. Zweitens müssen die Daten und Metadaten in einer ausreichenden Qualität vorliegen. Denn qualitativ minderwertige Daten sind ungeachtet ihres Umfangs nutzlos. Die Sicherstellung dieses Kriteriums macht auch die Regelung des Unterhalts nötig, beispielsweise im unter 3.2.1 beschriebenen Übereinkommen (Christen et al., 2020; Royal Academy of Engineering, o. J.).

3.2.3 Interoperabilität

Interoperabilität ist ein unumgänglicher Faktor, damit Datenräume effizient und effektiv sein können. Redundanzen und Diskrepanzen über Systeme hinweg können verringert werden. Daten können besser genutzt und die Entscheidungen auf deren Grundlagen informierter getroffen werden. Interoperabilität unterstützt also die Kernfunktionen von Datenräumen in massgeblicher Weise (Shiohira & Dale-Jones, 2019).

Interoperabilität ist kein klares Konzept. Sein Anwendungsfeld kann zwischen den Akteuren eines Datenraums, aber auch zwischen den Datenräumen verstanden werden. Der Inhalt wird oft auf die technischen Eigenschaften (Hard- und Software) beschränkt, kann aber auch viel weiter gefasst sein. Goldstein et al. (2018) schliessen bei ihrem holistischen Schichtenmodell der Interoperabilität sechs Stufen ein, die sich in zwei Kategorien unterteilen:

1. Enge Interoperabilität: technische Infrastruktur; Quantität und Qualität von Daten; Formate und Labels (Metadaten, Taxonomien).
2. Breite Interoperabilität: organisationale Praktiken (Kollaboration, Anreize); Institutionen, Gesetz und Politik (Zugang, Privatsphäre, Grundrechte); Menschen (Wissen, Inklusion, Bildung).

Auf jeden Fall wirkt die Reduzierung auf nur technische Eigenschaften als zu eng gefasst. Zumindest die Schichten der engen Interoperabilität im beschriebenen Modell sind miteinzubeziehen.

Ein wichtiger Aspekt der Interoperabilität sind Standards. Sie sind auch wichtig für die Umsetzung rechtlicher und ethischer Vorgaben. Standards werden entweder selbst projektbezogen entworfen, was sie flexibler und massgeschneiderter macht, oder sie werden übernommen, was ihre Interoperabilität steigert (Shiohira & Dale-Jones, 2019). Heute beschäftigen sich verschiedene Gremien mit der Festlegung von Standards: weltweit die ISO/IEC; IEEE; IETF; ITU; ETSI; W3C; europaweit die CEN; GAIA-X und IDS (vgl. Kapitel 4.3). Dabei stellen sich Fragen nach demokratischer Legitimation, repräsentativer Mitwirkung und der Folgenabschätzung bei Veränderung bestehender oder der Errichtung neuer Standards. Im Sinne der Nachhaltigkeit von Datenräumen ist es, bestehende Standards zu übernehmen, anstatt sie selber zu entwerfen. Angesichts ihrer Bedeutung und möglichen Defiziten, sind sie stets mit Bedacht zu wählen und in jedem Fall klar zu kommunizieren.

3.2.4 Skalierbarkeit zwecks dezentraler Datenräume

Schieferdecker et al. (2018, S. 180) haben eine Studie zu den «urbanen», d. h. *dezentralen* Datenräumen der Städte Bonn, Dortmund, Emden und Köln durchgeführt. Dabei stellten sie fest, dass ein Datenraum unterschiedlich gestaltet sein kann: « […] von einer zentralen Architektur im Sinne einer alleinigen Datenplattform bis zu einer völlig dezentralisierten Architektur mehrerer gleichberechtigter Datenplattformen, die sich untereinander austauschen und gemeinsam innovative Anwendungsszenarien umsetzen. Je nach den Anforderungen der jeweiligen Kommune ist es so möglich, eine geeignete Architektur für den urbanen Datenraum zu implementieren.»

Der Vorteil der dezentralen Architektur besteht namentlich darin, dass die bereits bestehenden Strukturen in den Gemeinden, Kantonen oder regionalen Organisationen verwendet werden können. Diese Strukturen sind in Bezug auf ihre Grösse sehr unterschiedlich. Um sie zu den Datenräumen zu entwickeln, die den hier beschriebenen Grundprinzipien entsprechen, ist es wichtig, dass diese Prinzipien skalierbar sind. Darunter ist die Eigenschaft der Grundprinzipien zu verstehen, sich den kleiner oder auch grösser werdenden Gegebenheiten möglichst flexibel anpassen zu können (in Anlehnung an Faust, 2021).[19] D. h., dass beispielsweise die Minimalinhalte der Transparenzpflicht (vgl. Kapitel 3.1.1) auch von kleineren Datenräumen ohne unverhältnismässigen Aufwand erfüllt werden können, Anforderungen aber auch wachsen, wenn der Datenraum grösser beziehungsweise risikoreicher wird (z. B. Einführung Registerpflicht), jedoch wiederum ohne dessen Wachstum zu behindern. Die europäische Datenstrategie erkennt in der Skalierbarkeit eines der Grundprinzipien, um den Privatsektor, insbesondere KMU, an Daten- und Cloud-Infrastrukturen und Diensten teilhaben zu lassen (Europäische Kommission, 2020a). Dezentrale Datenräume erhöhen ausserdem die Cybersicherheit, indem bei einem Leck nicht die Gesamtheit der Datenräume, sondern nur ein individueller betroffen ist (zur Cybersicherheit vgl. Kapitel 3.1.2, Kontrolle)

Mit Blick auf die Stadtentwicklung erkennen Schieferdecker et al. (2018) in der Skalierbarkeit ein Schlüsselmoment, um bestehende Datenräume und Infrastrukturen zugunsten optimierter Lösungen miteinander zu koppeln (Smart City Cockpit und integrierende systemische Stadtplanung), zum Beispiel den Zusammenhang zwischen Mobilität, Bebauung, Wetter und Luftqualität oder die Kombination des Wasser- und Stromsektors durch das Ausbauen von Abwasserleitungen zu Wärmequellen. Vernetzung, Smart City, Smart Village und Smart Region sind auch Ziele der Strategie Digitale Schweiz (Schweizerische Eidgenossenschaft, 2020).

Damit Gemeinden die heute noch weitgehend ungenutzten Potenziale von dezentralen Datenräumen zu nutzen beginnen, halten die Autoren verschiedene Empfehlungen bereit (Schieferdecker et al., 2018):

- Schaffung eines Angebots, das die Installation, Befüllung, Nutzung und den Betrieb eines urbanen Datenraums unterstützt und begleitet. Dazu könnte ein Beauftragter für den dezentralen Datenraum zählen;
- Schärfung des Bewusstseins, dass urbane Daten eine wertvolle Ressource sind und dezentrale Datenräume einen hohen Mehrwert bieten. Unter anderem, indem Aufklärungsmassnahmen für kommunale Mitarbeitende angeboten werden;
- Analyse von Möglichkeiten der Datennutzung in den dezentralen Verwaltungen und das Erschliessen von neuen Datenquellen.

19 In der Informatik bezieht sich Skalierbarkeit nur auf Hard- und Software. Im Kontext dieser Untersuchung wird der Begriff aber weiter verstanden.

3.2.5 Katalysator für die Nachhaltigkeit

Es gibt in der Wissenschaft keine einheitliche Definition des Begriffs 'Nachhaltigkeit', doch kommt er in fast allen Wissenschaften vor. Gemäss dem oft zitierten Brundtland-Bericht der Vereinten Nationen ist darunter eine Entwicklung zu verstehen, die die aktuellen Bedürfnisse befriedigt, ohne die künftigen Generationen darin zu beeinträchtigen, dasselbe zu tun (Chambers, 1988, S. 15). Daten sollen zur ökologischen, wirtschaftlichen und sozialen Nachhaltigkeit beitragen (Datenethikkommission der Bundesregierung, 2019; Europäische Kommission, 2020b).

Konkretisiert wurde die Nachhaltigkeit insbesondere in den 17 globalen Nachhaltigkeitszielen (Sustainable Development Goals, SDG) der UNO. Zu deren Erreichung hat sich auch die Schweiz im Pariser Klimaabkommen verpflichtet. Jedoch können sie bis zu ihrem Fälligkeitstermin 2030 ohne den Einsatz von neuen Technologien und grossen Datenmengen fast nicht mehr erreicht werden (z. B. Weltbank, 2018). Auch die Einhaltung des Pariser Klimaabkommens kann mit Effizienzgewinnen und Umweltmonitoring durch Datenauswertung unterstützt werden (vgl. Europäische Kommission, 2020b), sofern in Datenräumen quantitativ und qualitativ genügende Daten vorliegen (Goldstein et al., 2018).

Allerdings könnte sich die technologische Entwicklung auch negativ auswirken: führen Effizienzsteigerungen zu einem Preisrückgang, sind Fehlanreize und damit ein Rebound-Effekt zu befürchten (m. w. H. Schieferdecker et al., 2018). Um menschliche und ökologische Werte stärker ins Zentrum zu rücken, verteidigen Lange & Santarius (2018) die Beachtung des Prinzips der digitalen Suffizienz bei Datenräumen. Darunter verstehen sie Techniksuffizienz (wo wird wie viel Digitalisierung benötigt?), Datensuffizienz (welche Daten werden erfasst und ausgewertet werden?) und Nutzungssuffizienz (wieviel Zeit wollen wir jeweils in der virtuellen und in der realen Welt verbringen?). Die Suffizienz spiegelt sich Stand heute zumindest teilweise in den geltenden Grundsätzen zur Datenbearbeitung (Privacy by Design; Privacy by Default; Datensparsamkeit; Datenvermeidung).

3.2.6 Politikunterstützung

Gemäss der Strategie Digitale Schweiz sollen neue Technologien, das Aufbereiten und das Zurverfügungstellen von Daten durch den Staat (auf allen föderalen Ebenen) die Meinungsbildung, Civic-Tech-Anwendungen und die politische Partizipation fördern (Schweizerische Eidgenossenschaft, 2020). Für die Datenethikkommission der Bundesregierung (2019) sind digitale Technologien gar «systemrelevant» nicht nur für die Demokratie, sondern auch für die Entfaltung der Grundrechte in Anbetracht des schwindenden Einflusses des Journalismus und dessen Watchdog-Funktion. Die Nutzung von Datenräumen soll der Politik genauere Informationen liefern, Entscheide zu treffen helfen und die Bürger durch präziseres Monitoring besser ins Bild setzen sowie zur Beteiligung anregen. Ausserdem kann so die öffentliche Verwaltung transparenter, effizienter und benutzerfreundlicher ihren Auftrag erfüllen.

3.2.7 Wirtschaftswachstum

Das enorme Potenzial von Daten(-räumen) soll gemäss den gültigen Strategien auch der Schweizer Wirtschaft zu mehr Wachstum verhelfen. Dafür sollen Datenräume auch Zugang zu internationalen Märkten haben. Handelshemmnisse müssen abgebaut und die Kompatibilität nota bene mit der EU muss gesichert sein. Verschiedene Akteure sind einzubinden, insbesondere auch die Hochschulen. Für die Schweiz speziell hervorzuheben sind auch die Forcierung digitaler Finanztechnologien, -währungen und ihrer Finanzierungsmodelle (EDA, 2020; Schweizerische Eidgenossenschaft, 2020).

Die Anschlussfähigkeit insbesondere an europäische Datenräume ist bereits heute sinnvoll. Es ergeben sich daraus allgemeinbekannte Vorteile, wie die Vergrösserung des Markt- und damit Gewinnpotenzials. Daher wird ein eigentliches staatliches Anreizsystem zur Förderung der internationalen Kompatibilität vermutlich nicht nötig sein. Vorstellbar wäre hingegen, dass der Staat etwa durch Informationskampagnen sicherstellt, dass das Bewusstsein für internationale Zusammenhänge vorhanden ist, wenn neue Datenräume oder solche Pilotversuche entstehen. Er hat auch die Aufgabe, die internationalen Entwicklungen zu verfolgen und gegebenenfalls in die politischen Strategien einfliessen zu lassen. Beispielsweise schlägt die

Datenethikkommission der Bundesregierung (2019) vor, dass Datenräume ihren Sitz in der EU respektive dem EWR haben müssen. Ferner hat die öffentliche Hand auch ein Interesse daran, Netzwerke zu unterstützen, die den Austausch mit in- und ausländischen Verteter*innen unterschiedlicher Sektoren und Branchen (Wirtschaft, Hochschulen, öffentliche Veraltung) fördern.

3.3 Durchsetzung der Grundprinzipien

Damit sich die zuvor beschriebenen Grundprinzipien auf individueller und kollektiver Ebene entfalten können, müssen die folgenden Voraussetzungen erfüllt sein:

Grundprinzipien	Beschreibung	Empfehlungen
Einklagbare Durchsetzungs- und Kontrollmechanismen	Möglichkeit, bei einer Verletzung entweder selbst eine autoritäre Behörde anzurufen oder dass eine solche proaktiv tätig wird, um die Grundprinzipien nötigenfalls mit Zwang durchzusetzen.	Zuweisung der Rechenschaftspflicht
		Simple Beschwerdeverfahren zwecks Vermeidung langer, kostspieliger juristischer Prozesse
		Präventive Risikofolgenabschätzung
Nichtverbindliche Instrumente	Rechtlich unverbindliche Erwartungshaltungen gegenüber den involvierten Akteuren.	Best Practices, Standards, Label, Benchmarks, Selbstverpflichtungen fördern und definieren
		Klare Ausweisung Adressaten für Beschwerden und Rückmeldungen

Tabelle 4 Durchsetzung der Grundprinzipien

3.3.1 Einklagbare Durchsetzungs- und Kontrollmechanismen

In der Literatur unbestritten scheint, dass für jeden Datenraum so wie auch für jede daraus fliessende Anwendung feststehen muss, wer die Rechenschaftspflicht. Ohne dieses Element ist die (rechtswirksame) Durchsetzung der Grundprinzipien gar nicht möglich trägt (zur eindeutigen Identifikation vgl. Kapitel 3.1.1, Transparenz und Vertrauen). Fragen fangen sich insbesondere auch dort an zu stellen, wo mehrere Akteure hintereinander eingebunden werden, etwa wenn ein Datennutzer weitere Hilfspersonen hinzuzieht (z. B. Christen et al., 2020; Datenethikkommission der Bundesregierung, 2019; Delacroix & Lawrence, 2019; Royal Academy of Engineering, o. J.; Tranberg et al., 2018; vgl. Kapitel 2.2.2). Auch mit klaren Verantwortlichkeiten ist die Durchsetzung berechtigter Ansprüche bei einer neutralen staatlichen Stelle, etwa einem Gericht, meist ein langwieriger, kostspieliger Prozess. Wir empfehlen deshalb auch simplere Beschwerdeverfahren. Diese könnten im Datenraum selbst angelegt sein (interne Beschwerdestellen) oder über eine unabhängige Überwachungsstelle laufen, analog den Datenschutzbeauftragten von Bund und Kantonen (bzw. variable Lösungen zwecks Skalierbarkeit, vgl. Kapitel 3.2.4). Dort können Bürger*innen jederzeit eine Meldung machen. Gleichzeitig erteilt es Auskunft, leistet Hilfe und wirkt bei der Umsetzung der Prinzipien dadurch direkt mit. Umstritten ist, welche Kompetenzen einer solchen Institution idealerweise zu verleihen sind respektive wären.

Es wird auch verschiedentlich die Idee genannt, vor der Inbetriebnahme eines Datenraums eine präventive Risikofolgenabschätzung obligatorisch vorzuschreiben, wo ein hohes Risiko besteht (Europäische Kommission, 2020b). Dies reiht sich ein in die Vorschläge von Ethics in Design, Ethics by Design und Ethics by Default ein (Datenethikkommission der Bundesregierung, 2019). Ähnliche Mechanismen sehen auch die DSGVO der EU und das in Kürze in Kraft tretende revidierte DSG. Diese Vorschläge sind sehr zu begrüssen, stellen sie doch wesentliche Instrumente dar, um der Verletzung der Grundprinzipien effektiv vorzubeugen.

3.3.2 Nichtverbindliche Instrumente

Neben verbindlichen Vorschriften sollte auch ein Spektrum an nichtverbindlichen Instrumenten zur Verfügung stehen. In der Strategie Digitalaussenpolitik des EDA (2020) werden erwähnt: Best Practices, Standards, Label,

Benchmarks und Soft Law im weiteren Sinne. Solche Instrumente haben verschiedene Vorteile, darunter etwa der Beitrag an eine vorhersehbare und einheitliche Auslegung bindender gesetzlichen Vorgaben (ZHAW, 2018). Mehrere Institutionen haben auch bereits Fragebögen entworfen, damit Datenbearbeiter Selbstevaluationen zu ihrem Umgang mit Daten durchführen können (AI HLEG, 2020a; Royal Academy of Engineering, o. J.). Auch Selbstverpflichtungen auf freiwilliger Basis im digitalen Bereich, die über das gesetzliche Mindestmass hinausgehen, sind denkbar (sog. Corporate Digital Responsibility, Datenethikkommission der Bundesregierung, 2019).

Über das Gesagte hinaus schlagen wir vor, dass Datenräume klar ausweisen, an wen Betroffene Beschwerden und andere Rückmeldungen richten können. Ausserdem könnte es von Vorteil sein, wenn die Betreiber in regelmässigen Abständen die Einhaltung der Grundprinzipien und ihre Wirkung auf Gesellschaft, Wirtschaft und Umwelt kontrollieren würden. Staatliche Stellen könnten dies aufgrund ihrer Vorbildfunktion obligatorisch tun.

3.4 Fazit

Die Grundprinzipien und Voraussetzungen wurden anhand von drei Ebenen erläutert. Die erste, individuelle Ebene lässt sich so zusammenfassen, dass in vertrauenswürdigen Datenräumen einzelne Personen gewisse Rechte haben müssen, die sie selbstständig gegen bestimmte und identifizierbare andere Personen geltend machen können. Dazu gehört der Anspruch auf Transparenz, Kontrolle und Solidarität. Umgekehrt müssen die belangbaren Personen auch wissen, welche konkreten Pflichten sie haben.

Die zweite, kollektive Ebene beschreibt die Ideale, denen vertrauenswürdige Datenräume zu folgen haben. Dazu gehören: Eine faire Aufteilung der Kosten und Nutzen der Datenspeicherung, -bearbeitung und -wiederverwendung; die Räume sind durchlässig und bieten qualitativ einwandfreie Daten; die genaue Aufteilung und die Datenpflege sind vorzugsweise in einer Abmachung zu vereinbaren; die Interoperabilität, die auf vielfältigen Ebenen vorkommt, ist gewährleistet; um auch dezentrale, kleinere Datenräume entstehen zu lassen und zu fördern, sollten die Grundprinzipien skalierbar sein; Datenräume sollten dazu genutzt werden, Nachhaltigkeitsziele, die Politik und die Wirtschaft zu unterstützen.

Die dritte Ebene, die der Durchsetzung der Grundprinzipien gewidmet ist, erinnert daran, dass sowohl verbindliche als auch unverbindliche Instrumente eingesetzt werden sollten. Wichtig ist insbesondere, dass die Verantwortlichkeitsfrage geklärt und auch Alternativen zu langwierigen, kostspieligen Prozessen etabliert sind.

4 Vertrauenswürdige Datenräume in der Praxis

Im vorliegenden Kapitel geht es um vertrauenswürdige Datenräume in der Praxis. Um Verwirrungen zu vermeiden, dient als Einstieg ein Abschnitt über die begriffliche Abgrenzung, die in diesem Falle weder einfach noch ganz eindeutig ist (vgl. Abschnitt 4.1). In den darauffolgenden Kapiteln wird dann zuerst auf die Implementation der Data Trusts – einem eher angelsächsisch geprägten Konzept[20] – in der Praxis eingegangen (Abschnitt 4.2). Noch nicht spezifisch definiert ist der geplante vertrauenswürdige europäische Datenraum bzw. die verschiedenen sektoriellen Datenräume, die im dritten Kapitel diskutiert werden (vgl. Kapitel 4.3). In einem vierten und letzten Kapitel wird schliesslich ein Fazit gezogen (Abschnitt 4.4).

4.1 Begriffliche Abgrenzung

Wer sich ausgehend vom Begriff der (vertrauenswürdigen) Datenräume ein Bild von Use Cases und Umsetzungen zu machen versucht, erkennt schnell, dass es in der internationalen Literatur und (Fach-)Community diverse Begriffe und Konzepte gibt, die teilweise ineinander überfliessen und überlappend verwendet werden. In diesem Kontext wird von verschiedenen «Governance-Modellen» (Mulgan & Straub, 2019), oder auch «Patterns», gesprochen (Hardinges, 2020b). Die verschiedenen Institutionen entsprechen dabei eher einem komplexen Geflecht von sich wiederholenden Verhaltensweisen als konkreten Typologien (Hardinges, 2020b). Für das vorliegende Kapitel relevant ist einerseits der Begriff der vertrauenswürdigen Datenräume, welche gemäss der Datenstrategie der Deutschen Bundesregierung «Teilnehmerinnen und Teilnehmern gemeinsame, vertrauenswürdige Transaktionsräume [bieten], über die Daten bereitgestellt und gemeinsam ausgewertet bzw. bewirtschaftet werden können» (Bundeskanzleramt, 2021, S. 27). Im internationalen Kontext – insbesondere in Bezug auf die Umsetzung der europäischen Datenräume – wird auch von Data Spaces gesprochen. Im Bericht der Bundesregierung wird betont, dass die Daten in solchen Datenräumen dabei nicht zwingend an einem zentralen Ort zusammengeführt werden müssen, sondern dass es eine Vielzahl an Möglichkeiten gibt, wie Datenräume technisch und rechtlich ausgestaltet werden können (ebd.). Im angelsächsischen Raum wird eher von spezifischen Daten-Institutionen gesprochen, die im Verständnis des vorliegenden Berichtes eine Form von vertrauenswürdigen Datenräumen darstellen können. Dazu gehört insbesondere das Konzept der Data Trusts, auf die im folgenden Kapitel näher eingegangen wird.

4.2 Institutionen zur vertrauenswürdigen Datensteuerung

In der Praxis gibt es die unterschiedlichsten Formen von Daten-Institutionen, welche Menschen dabei unterstützen, Daten selbst zu verwalten oder sich stärker an der Verwaltung von Daten zu beteiligen. Einen Überblick gibt das Open Data Institute in seinem Bericht «Data Trusts: Lessons from three Pilots» (Hardinges et al., 2019). Die folgende Tabelle zeigt auf, dass die verschiedenen Ansätze im Gegensatz zu dem allgemeineren Begriff der vertrauenswürdigen Datenräume jeweils weitere qualifizierende Eigenschaften enthalten.

Approach	Distinguishing Feature
Data trusts	Takes what has been learned from the use of legal trusts. Trustees of a data trust will take on responsibility (with some liabilities) to steward data for an agreed purpose.
Data cooperatives	Takes what has been learned from cooperatives. A mutual organization owned and democratically controlled by members, who delegate control over data about them.
Data commons	Takes what has been learned from managing common pool resources – such as forests and fisheries – and applies the principles to data.

20 Vergleiche dazu auch Kapitel 2, insbesondere Abschnitt 2.2.2, in dem der Data Trust als eine mögliche Struktur beschrieben wird, welche eine Antwort auf die kollektive Herausforderung im Datenzyklus gibt, die Unabhängigkeit des Datenraumbetreibers zu gewährleisten.

Personal data stores	Stores data provided by a single individual on their behalf and provides access to that data to third parties when directed to by the individual.
Research partnerships	When data holders provide access to data to universities and other research organizations.

Tabelle 5 Institutionen zur vertrauenswürdigen Datensteuerung (Quelle: Hardinges et al., 2019, S. 9)

Ein für die Einordnung der unterschiedlichen Daten-Institutionsformen hilfreiches Raster liefern die Autoren des britischen Think-Tanks Nesta, die in ihrem Bericht «The New Ecosystem of Trust» (Mulgan & Straub, 2019) eine Typologie von Governance-Formen vorschlagen, in denen die Data Trusts ebenfalls eine grosse Rolle spielen (Mulgan & Straub, 2019, S. 6). Die unterschiedlichen Formen werden dabei von Mulgan & Straub über die Achsen «Wert der Daten für die Öffentlichkeit» (x-Achse) und «Kontrolle über das Datenteilen» (y-Achse) geplottet. Das sich dadurch ergebende Feld reicht von Institutionen mit Daten, die hauptsächlich einen Wert für das Individuum besitzen und wo dieses auch die komplette Kontrolle über das Datenteilen besitzt (Personal Data Stores), bis zu Institutionen, die für die Allgemeinheit sehr wertvolle Daten verwalten, wobei die Daten ohne eine freiwillige (oder vermeidbare) Entscheidung der dahinter stehenden Individuen übermittelt worden sind (Public Data Trusts).

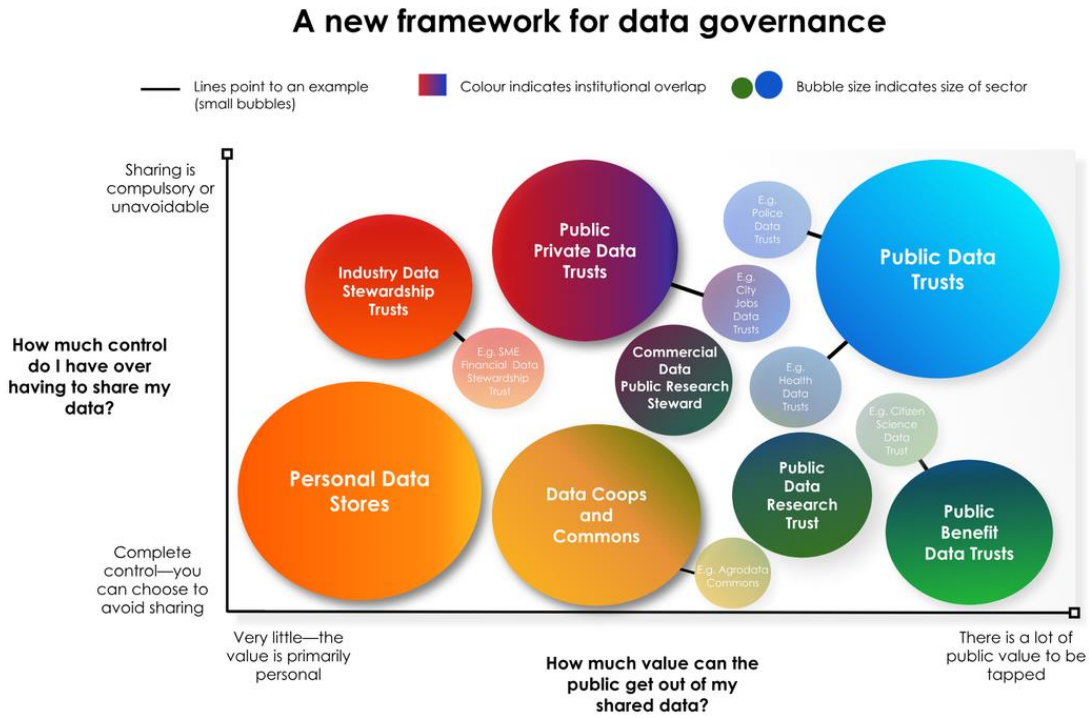

Abbildung 1 Typologie Governance-Formen (Mulgan & Straub, 2019, S. 6)

4.2.1 Data Trusts

Im folgenden Kapitel wird zuerst darauf eingegangen, was unter dem Begriff Data Trust verstanden wird, und welche Anforderungen und Vorteile einem Data Trust auf konzeptioneller Ebene zugeschrieben werden. In einem nächsten Schritt werden dann die verschiedenen Formen von Data Trusts und – wenn vorhanden – konkrete Praxisbeispiele diskutiert. Zur Strukturierung wird die von Mulgan & Straub vorgeschlagene Typologie von Governance-Formen im Bereich Daten-Institutionen verwendet (Mulgan & Straub, 2019, S. 6).

4.2.1.1 Das Konzept der Data Trusts

In ihrer Studie schlagen Mulgan & Straub (2019, S. 1) ein Framework für eine neue Art von Daten-Institution vor, die sie unter dem Oberbegriff Data Trust zusammenfassen. Nach der Definition des Open Data Instituts (ODI) können unter Data Trusts grob gesagt rechtliche Konstrukte verstanden werden, welche eine unabhängige, treuhänderische Steuerung von Daten anbieten (Hardinges, 2020a). Entgegen dem Ursprung des Begriffes soll sich ein Data Trust zwar von der Idee einer Treuhandgesellschaft inspirieren lassen, als rechtliche Form jedoch diejenigen Strukturen und Formen übernehmen, welche in einem gegeben Kontext Sinn machen (Hardinges et al., 2019). «Treuhänderisch» im Kontext der Data Trusts beschreibt dabei die Pflicht, bei der Steuerung von Daten die Grundsätze der «impartiality, prudence, transparency and undivided loyalty» zu berücksichtigen (Hardinges, 2020a, S. 2).

Die Nesta-Autoren präzisieren, dass sich die Data Trusts bei ihren Aktivitäten im gesetzlichen Rahmen bewegen müssen und so zu einer Wertschöpfung in «vertrauenswürdiger Art und Weise» beitragen sollen (Mulgan & Straub, 2019, S. 2). Die Data Trusts unterscheiden sich dabei sowohl durch ihre unterschiedlichen Zustimmungsbedingungen («conditions of consent») als auch einem unterschiedlichen Grad an privatem oder öffentlichem Wert der verfügbaren Daten voneinander (Mulgan & Straub, 2019, S. 1). Grundsätzlich klar ist, dass an Data Trusts sowohl staatliche als auch private Akteure beteiligt sein können. Gegenstand einer offenen Diskussion ist hingegen, ob sich ein Data Trust einem höheren ideologischen Ziel verpflichten muss – beispielsweise der Vision, mit einer Bottom-up-Strategie ein aktuelles Machtungleichgewicht zwischen datenhaltenden Organisationen und den Datenurhebern auszugleichen (Hardings 2021; Delacroix & Lawrence, 2019).

Der allgemeine Vorteil eines Data Trusts wird darin gesehen, dass sich damit Raum für Verhandlungen – collective bargaining – ergibt, der in heutigen konventionellen Daten-Beziehungen nicht existiert. Wylie & McDonald formulieren es so:

> «At present, most data relationships are written as exceptionally permissive, or outright open, licences. The act of creating a data trust, by contrast, is inherently specific, requiring the parties involved to agree on a **common purpose**, a **governance structure** and a **clear theory of shared benefit**. In other words, one opportunity that data trusts can provide is a way to create collective bargaining for data-sharing relationships» (Wylie & McDonald, 2018, S. 1, Hervorhebung hinzugefügt).

Zusätzlich zu den von Wylie & McDonald aufgeführten Voraussetzungen einer gemeinsamen Zielformulierung, Governance-Strukturen und einer Beschreibung der Verteilung des Nutzens oder Gewinns, betont das Open Data Institut noch die Notwendigkeit der **Sicherstellung einer nachhaltigen Finanzierung** (Hardinges, 2018).

4.2.1.2 Data Trusts in der Praxis

Für den Umgang mit Daten, die ohne die Einwilligung der Individuen mit bestimmten Verwaltungsstellen geteilt werden, und wo das Aggregat der Daten für die Allgemeinheit einen grossen Wert aufweist, schlagen Mulgan & Straub das institutionelle Arrangement des **Public Data Trusts** vor (Mulgan & Straub, 2019, S. 7). Solche Institutionen sollen gemäss Mulgan & Straub dabei sowohl für den Schutz der Daten als auch für die Maximierung des Public Value zuständig sein (und auch dafür verantwortlich gemacht werden können). Mulgan & Straub werfen die Frage auf, ob für solche Public Data Trusts auf bereits bestehende öffentliche Strukturen zurückgegriffen werden kann, oder ob es dafür neue Institutionen braucht. Nach Mulgan & Straub ist das zentrale Element hier die Glaubwürdigkeit und das Vertrauen der Bevölkerung in die Institution(en), die darüber entscheidet.

Ein Beispiel aus dem Schweizer Kontext könnte die vom Bundesrat im Sommer 2020 beauftragte «nationale Dateninfrastruktur Mobilität» (NaDIM) werden: Die zentrale Schnittstelle NaDIM soll die Datenbanken von verschiedenen Mobilitätsanbietern verknüpfen (Alliance Swisspass, 2021). Da das Projekt noch in den Kinderschuhen steckt und eine Umsetzung laut der Website von Alliance Swisspass für frühestens Ende 2023 geplant ist, lassen sich an dieser Stelle noch keine Aussagen über den tatsächlich generierten Public Value machen.

Eine Abwandlung des Public Data Trusts stellt der **Public Research Trust** dar, wobei im Unterschied zum Public Data Trust die Individuen über das Teilen oder Nicht-Teilen der Daten Kontrolle ausüben können, die Daten im Aggregat aber immer noch einen grossen Wert für die Allgemeinheit besitzen. Unter denselben Vorzeichen ist auch die Institution des **Public Benefit Data Trust** passend.

- Der **Public Research Data Trust** ist also eine Variante des Public Data Trusts, wobei eine Datenbank über verschiedene administrative und soziale Daten wacht, die sowohl von nationalen als auch von lokalen Regierungen kommen können (Mulgan & Straub, 2019, S. 7). Bewilligte Forschungsprojekte können dann über APIs Zugang zum Datenpool erlangen. Mulgan & Straub schlagen vor, dass Individuen zum Beispiel die Möglichkeiten für ein Opt-in oder Opt-out erhalten; also selbst entscheiden könnten, ob ihre Daten in dem Datenpool aufgeführt werden oder nicht, wobei die Frage der Default-Option von der Politik geklärt werden müsse (Mulgan & Straub, 2019, S. 7). Die Nesta-Autoren empfehlen dabei, dass der Public Research Data Trust in seiner Funktion als Wächter über die Daten idealerweise durch eine Institution vertreten wird, die bei der Bevölkerung und der wissenschaftlichen Community ein gutes Ansehen geniesst (für den Kontext UK wird beispielsweise das UK Office of National Statistics (ONS) als Kandidat genannt).

  Als Beispiele für Public Research Data Trust können drei Pilotprojekte des UK Open Data Instituts in Kooperation mit dem UK Office for AI (OAI) genannt werden. Beim ersten der drei Pilotprojekte handelt es sich um eine Kooperation des ODI mit dem Mayor of London und dem Royal Borough of Greenwich mit einem Fokus auf Echtzeitdaten aus Internet of Things-Sensoren (Open Data Institute, 2018; Sharing Cities, 2021). Ein zweiter Pilot, der im Januar 2019 gestartet wurde, zielt darauf ab, den illegalen Wildtierhandel zu reduzieren, indem Wildtierdaten aus der ganzen Welt besser zugänglich gemacht werden. Ein besonderes Augenmerk soll dabei auf Daten gerichtet werden, welche das Potenzial haben, den illegalen Wildtierhandel zu beenden. In Zusammenarbeit mit Naturschutzexperten und Technikern von Wildlabs (Wildlabs, 2021) will sich das Pilotprojekt zunächst auf zwei Bereiche konzentrieren, in denen die gemeinsame Nutzung von Daten innerhalb eines Data Trusts zur Unterstützung von maschinellem Lernen und KI genutzt werden könnte (Open Data Institute, 2019). Für ein drittes Pilotprojekt soll schliesslich in Zusammenarbeit mit der Non-Profit-Organisation WRAP (WRAP, 2021) die Frage angegangen werden, wie mit Lebensmitteldaten – insbesondere Daten über die Art der Lebensmittelabfälle und deren Verbleiben – Lebensmittelabfälle in den Lieferketten verfolgt und gemessen werden können (Open Data Institute, 2019).

- In die Kategorie des **Public Benefit Data Trust** fallen Institutionen, welche Daten vereinigen, die von Freiwilligen im Sinne eines öffentlichen Interesses bereitgestellt werden (Stichwort Citizen Science). In Bezug auf solche Initiativen ist es besonders wichtig, dass im Sinne der Citizen-Science-Ideologie auch die Institutionen, welche die Daten verfügbar machen, möglichst offen, einfach zu bedienen und zugänglich für Forschende und politische Entscheidungsträger sind (Mulgan & Straub, 2019, S. 9).

Als nächstes sehen wir uns die Institutionsformen auf der anderen Seite des von Mulgan & Straub aufgespannten Spektrums an: Treuhänderische Institutionen, welche sich mit Daten beschäftigen, die tendenziell eher geringeren Wert für die Allgemeinheit haben (im Vergleich zu den Public Data Trust und den Public Benefit Data Trust), dem Individuum aber weniger oder gar keine Entscheidungsbefugnis über das Datenteilen einräumen. In diese Kategorie fallen nach Mulgan & Straub die **Industry Data Stewardship** Trusts und die **Public Private Data Trusts**.

- In Bezug auf **Industry Data Stewardship Trusts** sprechen Mulgan & Straub von Einrichtungen, die sich um kommerzielle Daten kümmern, beispielsweise Finanzdaten von KMUs (Mulgan & Straub, 2019, S. 8). Diese Daten dürfen nur auf ausdrückliche Bewilligung mit Dritten geteilt werden. Im Governance-Geflecht sehen die Nesta-Autoren dabei sowohl Branchen-Regulierer als auch kleine und grössere Firmen und die Konsumenten. In Bezug auf die Industry Data Stewardship Trusts betonen Mulgan & Straub die Wichtigkeit interner Funktionen wie des/der data stewards, die eine entscheidende Rolle bei der Steuerung des Datenaustausches wahrnehmen.

- Eine weitere Kategorie ist gemäss Mulgan & Straub der **Public Private Data Trust**, wo für spezifische Daten oder Bereiche öffentliche und kommerzielle Daten von einem vertrauenswürdigen Dritten

(einem «trusted intermediary») verbunden werden (Mulgan & Straub, 2019, S. 8). Von besonderer Wichtigkeit ist dabei, dass diese Daten sorgfältig verwaltet werden und Missbrauch vermieden wird, wobei es eine strenge Rechenschaftspflicht und Standards geben muss (Mulgan & Straub, 2019, S. 8). Die Nesta-Autoren führen aus, dass ein solcher Public Private Data Trust im Gegensatz zu dem Industry Data Stewardship Trust eine formellere Verwaltung, sowie eine klare gesetzliche Grundlage benötigt, und möglichst viele unterschiedliche Interessengruppen miteinbeziehen sollte (Mulgan & Straub, 2019, S. 8). Ein Beispiel für einen solchen Public Private Data Trust könnte das Projekt Shared Streets sein, welches zum Ziel hat, ein globales, nicht-proprietäres System zur Beschreibung von Strassen aufzubauen. Das System soll dabei Strassendaten von privaten Unternehmen und Städten verbinden, wobei die referenzierten Daten nahtlos zwischen verschiedenen Karten übertragen werden sollen (SharedStreets, 2020).

4.2.2 Data Cooperations und Personal Data Stores

Noch nicht diskutiert wurden bisher die Institutionen, welche sich auf dem Spektrum von Mulgan & Straub tendenziell unten links anordnen (vgl. Abbildung 1). Hierbei geht es um Institutionen, welche auf Beziehungen anwendbar sind, in denen einerseits Kontrolle über das Teilen von persönlichen Daten ausgeübt werden kann, die Daten für die Allgemeinheit aber auch einen eher geringen Wert aufweisen. Institutionen dieser Art ist gemeinsam, dass sie die persönlichen Daten der Benutzerinnen und Benutzer des Datenraumes bewahren und ihnen gleichzeitig das Recht geben, ihre Daten kontrolliert an andere Organisationen freizugeben. Dies trifft zu auf sogenannte **Personal Data Stores (PDS)** – auch unter der Bezeichnung Personal Information Management Systems (PIMS) bekannt – und auch auf **Data Cooperations** (Daten-Kooperative).

Ein Beispiel für einen **Personal Data Store (PDS)** ist das Solid-Projekt (Solidproject, 2021), welches das Speichern von Daten in dezentralisierten Daten-«Pods» erlaubt. Der Zugriff darauf von Organisationen oder Applikationen kann von den Benutzerinnen und Benutzern selbst kontrolliert, und jederzeit widerrufen werden. Gespeichert werden kann dabei gemäss Solid jede Art von Daten, von Dokumenten, wie sie auch in Google Drive oder Dropbox abgelegt werden können, bis zu strukturierten Daten. Andere ähnliche – teilweise kostenpflichtige – Projekte sind MyDex, Digi.me, Hub of all Things, Open PDS oder Meeco. Als ein weiteres Schweizer Projekt ist BitsaboutMe zu nennen, welches 2017 von ehemaligen Ricardo.ch-Mitarbeitern gegründet wurde. Gemäss der Website soll BitsaboutMe ein Werkzeug sein, mithilfe dessen die User ihre persönlichen Daten einfacher managen und über die Plattform gezielt gegen Geld verkaufen können (BitsaboutMe, 2021).

Obwohl diese und ähnliche Projekte teilweise bereits mehrere Jahre laufen, hatten sie bisher keinen durschlagenden Erfolg. Mögliche Gründe dafür könnten sein, dass die PDS zwar zusätzlichen Datenschutz bieten, aber existierende Workflows erschweren (Hardinges, 2020). Zudem ist wahrscheinlich, dass die PDS bisher schlicht zu wenige User anziehen konnten, um für Organisationen wirklich attraktiv zu sein. Und wenn solche Lösungen nicht von grösseren Organisationen oder Firmen aufgenommen werden, werden auch keine Massen von individuellen Benutzern angezogen.

In diesem Zusammenhang kann auch auf das elektronische Patientendossier (EPD) verwiesen werden, welches im Verlauf des Jahres 2021 schrittweise in der ganzen Schweiz eingeführt werden soll (Patientendossier.ch, 2021). Über das EPD soll jede Benutzerin und jeder Benutzer festlegen können, welche Gesundheitsfachpersonen welche Gesundheitsdokumente konsultieren dürfen. Dabei soll man selbst Dokumente ins EPD ablegen, das Zugriffsprotokoll einsehen und Stellvertretungen bestimmen können (Patientendossier.ch, 2021). Über den Erfolg des EPDs kann zum jetzigen Zeitpunkt noch nicht viel ausgesagt werden, kritische Stimmen bemängeln aber, dass das Konzept des EPDs bereits veraltet sei, bevor es national den Durchbruch geschafft hat. Die flächendeckende Einführung des EPD verzögert sich unter anderem, weil sich der Zertifizierungsprozess für Spitäler und andere Einrichtungen des Gesundheitswesens als aufwändiger erwies als ursprünglich erwartet (Ruch, 2021; SRF, 2020).

- Beispiele für **Data Cooperations** (Daten-Kooperative) sind zwei Kooperativen im Gesundheitsbereich: Salus Coop - welche sich selber als ”citizen data cooperative that accelerates research and innovation

in the healthcare sector" beschreibt (SalusCoop, 2021) oder die Schweizer Initiative MIDATA (Midata, 2021), über welche Inhabende eines Datenkontos aktiv zur medizinischen Forschung und klinischen Studien beitragen können, indem sie bestimmten Organisationen oder Applikationen selektiven Zugriff auf ihre persönlichen Daten gewähren. Bekanntes Beispiel ist «Ally Science», welche eine Studie zur Pollenallergie in der Schweiz durchführen, oder MitrendS, wo Daten für die Erforschung der Nervenkrankheit Multiple Sklerose gesammelt werden. Im Sinne einer Kooperative können die Individuen dabei auch Genossenschaftsmitglieder werden und als solche die Genossenschaft (mit-)kontrollieren (ebd.).

4.3 Die Umsetzung der europäischen Datenräume

Im Februar 2020 stellte die Europäische Kommission ihre erste Datenstrategie vor (Europäische Kommission, 2020a). Erklärtes Ziel der Strategie ist es, dass die EU die Führungsrolle in einer datengestützten Gesellschaft übernehmen soll (ebd.). Durch die Schaffung eines Binnenmarkts für Daten sollen Daten innerhalb der EU und branchenübergreifend zum Nutzen von Unternehmen, Forschenden und öffentlichen Verwaltungen weitergegeben werden können.

> «Ziel ist die Schaffung eines einheitlichen europäischen Datenraums, eines echten Binnenmarkts für Daten, der für Daten aus aller Welt offensteht, in dem sowohl personenbezogene als auch nicht-personenbezogene Daten, darunter auch sensible Geschäftsdaten, sicher sind und in dem Unternehmen auch leicht Zugang zu einer nahezu unbegrenzten Menge hochwertiger industrieller Daten erhalten» (Europäische Kommission, 2020a, S. 5).

Die Kommission erklärt, dass Daten für alle Wirtschaftszweige und Gesellschaftsbereiche grosse Bedeutung haben. Gleichzeitig müsse berücksichtigt werden, dass jeder Sektor oder Bereich seine eigenen Besonderheiten habe und sich nicht alles im gleichen Tempo bewegen würde. Daher müssten Massnahmen zur Schaffung eines europäischen Datenraumes (wie im obigen Zitat skizziert) mit der Entwicklung von sektorspezifischen Datenräumen einhergehen (Europäische Kommission, 2020a, S. 6).

Konkret genannt werden neun verschiedene sektorspezifische Datenräume, darunter ein:

- gemeinsamer europäischer Industriedatenraum;
- gemeinsamer europäischer Datenraum für den europäischen Grünen Deal;
- gemeinsamer europäischer Mobilitätsdatenraum;
- gemeinsamer europäischer Gesundheitsdatenraum;
- gemeinsamer europäischer Finanzdatenraum;
- gemeinsamer europäischer Energiedatenraum;
- gemeinsamer europäischer Agrardatenraum;
- gemeinsame europäische Datenräume für die öffentliche Verwaltung und ein
- gemeinsamer europäischer Kompetenzdatenraum

Für die Umsetzung der im Bericht der Kommission skizzierten Datenräume sind insbesondere zwei Initiativen relevant: Die International Data Spaces Association (IDSA) und das GAIA-X-Projekt. Mit GAIA-X soll die Grundlage für eine föderierte und interoperable Dateninfrastruktur erarbeitet werden. Die in dieser Dateninfrastruktur angebotenen Dienste sollen dabei auf gemeinsamen Standards beruhen. An diesem Punkt kommt die International Data Spaces Association (IDSA) ins Spiel. Die IDSA hat sich zum Ziel gesetzt, einen Standard – den International Data Spaces-Standard (IDS) – zur Ermöglichung eines offenen, transparenten und selbstbestimmten Datenaustausches auszuarbeiten (International Data Spaces Association 2021).

Das Zusammenwirken von GAIA-X und IDS wird in einem Positionspapier der ISDA auch so beschrieben (Otto et al., 2021, S. 13):

> "GAIA-X focuses on sovereign cloud services and cloud infrastructure, while IDS focuses on data and data sovereignty. The interaction of GAIAX and IDS has three main tasks: self-sovereign data storage, trustworthy data usage and interoperable data exchange. This way, GAIA-X is developed in accordance with the European Data Strategy and supports smart data applications and innovations

> across industry sectors. For this purpose, GAIA-X and IDS complement each other to ensure cloud and data sovereignty for end-to-end data value chains in federated ecosystems."

4.3.1 International Data Spaces-Standard (IDS)

Bei der IDSA handelt es sich um einen gemeinnützigen Verein, in dem sich 130 Unternehmen aus 22 Ländern zusammengeschlossen haben. Der IDSA verfolgt das Ziel, einen (globalen) Standard, ein Governance-Modell und eine Implementationsstrategie für die Umsetzung der europäischen Datenstrategie zur Verfügung zu stellen (International Data Spaces Association, 2021). Mit dem sogenannten IDS-Standard soll für Unternehmen im Datenraum Datensicherheit, Datenschutz und Datensouveränität unter gleichen Wettbewerbsbedingungen gewährleistet werden. Der IDS wird als essentieller Bestandteil einer neuen Art der Datenökonomie beschrieben, da er vorschreibt, wie vertrauenswürdige Datenräume aufgesetzt und wie die Zugangspunkte zu solchen Datenräumen ausgestaltet werden sollten (International Data Spaces Association 2021).

> «The IDS standard is the blueprint for data exchange itself, based on European values, such as data protection and security, equal opportunities through a federated design and the guarantee of data sovereignty for the creator of the data and trust between participants" (International Data Spaces Association 2021).

Gegenseitiges Vertrauen soll ausserdem dadurch geschaffen werden, dass die Datennutzung auf der Basis von ethischen Grundsätzen und «gemeinsamen europäischen Werten» (International Data Spaces Association, 2020) passiert. Explizit genannt werden sind im Besonderen die *informationelle Selbstbestimmung* (*data sovereignty*), Partizipation, Offenheit und Föderalismus[21] (International Data Spaces Association, 2020).

4.3.2 GAIA-X

Unterstützen will die Bestrebungen der IDSA das im Herbst 2019 ins Leben gerufene Projekt GAIA-X, mit welchem ein europäisches Ökosystem für Dateninfrastrukturen geschaffen werden soll. Konkret geplant ist «eine Vernetzung dezentraler Infrastrukturdienste (insb. Cloud und Edge-Instanzen) zu einem nutzerfreundlichen System», wobei «die Vernetzung bestehender Infrastrukturen (…) über Open-Source-Anwendungen und interoperable Standards in Form einer gemeinsamen Referenzarchitektur passieren [soll], ohne zunächst eigene Rechnerkapazitäten aufzubauen» (Bundeskanzleramt, 2021, S. 12). Mit GAIA-X soll gemäss einem Bericht des Deutschen Bundesministerium für Wirtschaft und Energie die Interoperabilität und Portabilität von Infrastruktur, Daten und Diensten ermöglicht werden und ein hohes Mass an Vertrauen bei den Nutzern erzeugt werden (Bundesministerium für Wirtschaft und Energie, 2020, S. 2). Um die Umsetzung von zentralen Werten sicherzustellen wurden die folgenden technischen Richtlinien formuliert (Otto et al., 2021, S. 8):

- Security-by-design
- Privacy-by-design
- Enabling federation, distribution and decentralization
- User-friendliness and simplicity
- Machine-processability
- Semantic representation

Die über die Dateninfrastruktur angebotenen Daten- und Service-Angebote sollen dabei transparent sein und Abhängigkeiten (auch als Lock-in-Effekte bekannt, vgl. auch Kapitel 2.1) von einzelnen Anbietern reduziert werden (ebd.). In Anlehnung an die Mitteilung der Kommission zur europäischen Datenstrategie und den darin angedachten sektorspezifischen Datenräumen (Europäische Kommission, 2020, S. 26-27) wird postuliert, dass die Teilnehmerinnen und Teilnehmer von GAIA-X Daten und Services «souverän über sektorspezifische Datenräume hinweg nutzen» können (Bundesministerium für Wirtschaft und Energie, 2020,

21 Während Föderalismus in diesem Kontext nicht weiter ausgeführt wurde, ist davon auszugehen, dass der Begriff hier nicht aus einer Perspektive mit Schweizer Massstäben verstanden werden darf, sondern eher die Absicht kommuniziert, dezentral und unter Rücksichtnahme auf die regionalen (Wirtschafts-)Strukturen zu arbeiten.

S. 3). Diese sektorspezifischen Datenräume (hier Data Spaces genannt) sind auch in der folgenden Abbildung (vgl. Abbildung 2) skizziert. Die Abbildung zeigt, dass das GAIA-X Ökosystem aus einem Datenökosystem und einem Infrastrukturökosystem besteht, welche über die sogenannten «föderierten» Services von GAIA-X miteinander verbunden werden. Die ganze Architektur soll dabei auf gemeinsamen Regeln und Standards beruhen (vgl. auch das Kapitel 1.2.1 über den IDS) (Otto et al., 2021, S. 8). Durch die Kombination bestehender Lösungen nimmt GAIA-X die Rolle eines Dirigenten und Integrationspartners ein, wobei es keinen eigenen zentralen Datenspeicher unterhält (Otto et al., 2021, S. 9).

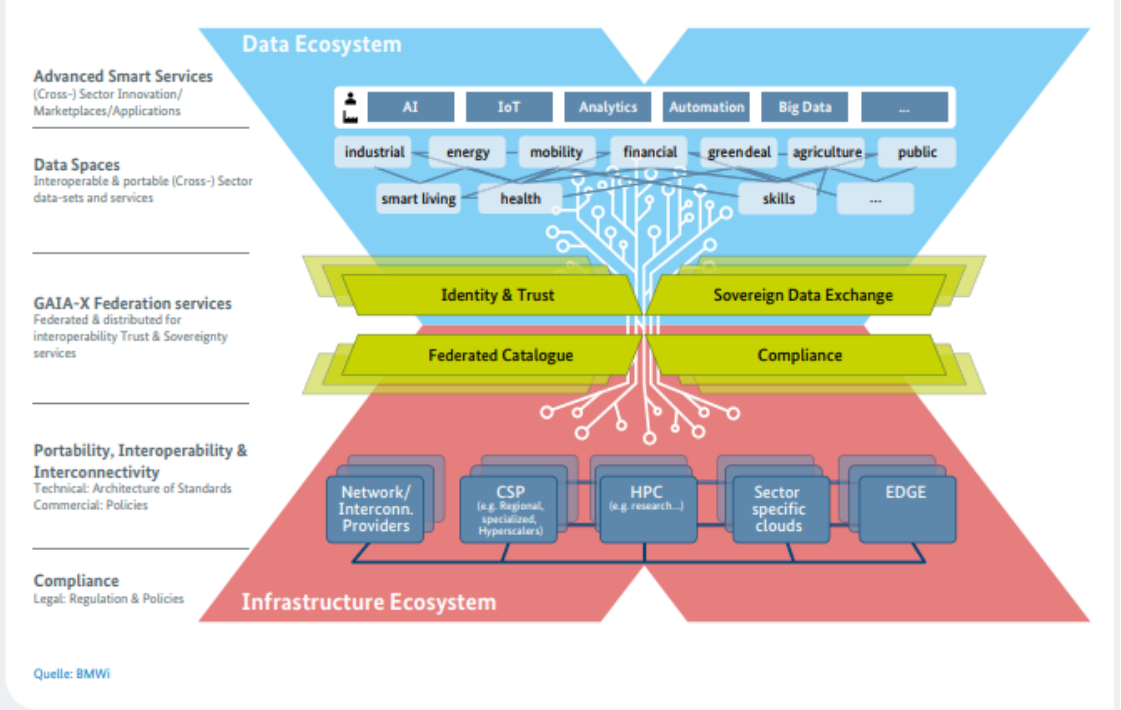

Abbildung 2 Architekturansatz mit den föderierten GAIA-X-Services (Quelle: Bundesministerium für Wirtschaft und Energie, 2020, S. 4)

4.4 Fazit

Eine Bestandesaufnahme der Umsetzung von vertrauenswürdigen Datenräumen in der Praxis gestaltet sich allein deswegen herausfordernd, weil der Suchbegriff schwierig einzugrenzen ist. Auf einer konzeptionellen Ebene gibt es in der internationalen Literatur eine Diversität, die sich auch in der Praxis wiederfindet. Ein näherer Blick auf die verschiedenen angedachten oder teilweise umgesetzten Institutionen zum Datenteilen erweckt eher den Eindruck eines komplexen Geflechts von sich wiederholenden Verhaltensweisen als konkreten Typologien. Ein nützlicher Ansatz einer Typologisierung stellt dennoch die Arbeit der Nesta-Autoren Mulgan & Straub dar, welche unterschiedliche Governance-Formen über den Wert der Daten für die Öffentlichkeit und des Ausmasses an Kontrolle der Individuen über das Datenteilen definieren (Mulgan & Straub, 2019).

Das sich dadurch ergebende Feld reicht von Institutionen mit Daten, die hauptsächlich einen Wert für das Individuum besitzen und wo dieses auch die komplette Kontrolle über das Datenteilen besitzt (Personal Data Stores), bis zu Institutionen, die für die Allgemeinheit sehr wertvolle Daten verwalten, wobei die Daten ohne eine freiwillige (oder vermeidbare) Entscheidung der dahinter stehenden Individuen übermittelt werden (Public Data Trusts). Gerade dieser Ansatz der Data Trusts stellt eine vieldiskutierte Ausgestaltung eines vertrauenswürdigen Datenraumes dar (vgl. die Arbeiten des Open Data Instituts). Die Vorteile eines Data Trusts werden darin gesehen, dass sich mit einer unabhängigen, treuhänderischen Verwaltung von Daten Verhandlungsspielraum für das Individuum ergibt, der in konventionellen Daten-Beziehungen nicht oder kaum existiert. Zu den Voraussetzungen für einen Data Trust gehört dabei die Einigung auf ein gemeinsames Ziel, eine Governance-Struktur, eine klare Vorstellung der Aufteilung des Nutzens / Gewinns aus dem Data Trust und die Sicherstellung einer nachhaltigen Finanzierung der Data-Trust-Strukturen (Wylie & McDonald

2018; Hardinges 2018). Je nach Art der Daten und Kontext kann ein Data Trust unterschiedliche Ausprägungen einnehmen – Daten mit einem hohen Wert für die Allgemeinheit können beispielsweise in einem Public Research Data Trust oder einem Public Benefit Data Trust behandelt werden, zu Daten mit einem geringeren kollektiven Wert und tiefer individueller Kontrolle passt ein Industry Stewardship Trust oder auch ein Public Private Data Trust (Mulgan & Straub, 2019).

Welche Form die neun verschiedenen vertrauenswürdigen Datenräume, die von der Europäischen Kommission geplant sind, einnehmen sollen, ist noch offen – und wird höchstwahrscheinlich sektorabhängig sein (Europäische Kommission, 2020a). Für die Umsetzung relevant sind an diesem Punkt das GAIA-X-Projekt und der IDS-Standard. Beide Initiativen haben sich dabei den Grundprinzipien der informationellen Selbstbestimmung, Partizipation, Offenheit und einem föderativen, dezentralen Vorgehen verpflichtet. Zur Umsetzung und Vermeidung von Lock-in-Effekten sollen zudem verschiedene technische Richtlinien von Security-by-design bis zu Machine-processability und Semantic representation beitragen (Otto et al., 2021, S. 8).

5 Kernelemente eines Modells vertrauenswürdiger Datenräume

5.1 Einführung

Die Definition vertrauenswürdiger Datenräume unter Berücksichtigung der digitalen Selbstbestimmung[22] baut auf einem Modell eines solchen Datenraums auf.

Ziel ist der Aufbau eines Wissensmodells, welches die Kernelemente vertrauenswürdiger Datenräume und deren Beziehungen festlegt. Eine solche Abbildung zeigt in expliziter Form und mithilfe einer standardisierten grafischen Notation das Begriffsnetz um das Thema "vertrauenswürdige Datenräume"[23]. Begriffe in diesem Zusammenhang sind als Entitäten im Sinne der Ontologie[24] zu verstehen. Das vorliegende Modell ist ein Versuch, das thematische Wissen zu organisieren und zu vereinheitlichen. Als Grundlage für Auswahl und Festlegung der Begriffe aus diesem Wissensbereich dienen die Erkenntnisse der Literaturstudie (Kapitel 2-4 dieses Berichts). Zwecks verbesserter Lesbarkeit sind nicht alle Begriffe mit Hinweisen auf die Definitionen belegt, sondern nur solche an kritischen Stellen. Für das gesamte Dokument gilt als erste Stelle für Definitionen das in Zusammenhang mit der oben erwähnten Studie erarbeitete Glossar.

Wie es für jedes Modell der Fall ist, gilt auch hier, dass derjenige Abstraktionsvorgang, welcher der Modellbildung zugrunde liegt, eine der verschiedenen möglichen Sichten auf die betrachtete Realität ist. Es handelt sich also um einen Vorschlag zur modellhaften Darstellung des Wissens in diesem Bereich. Ziel ist, eine dokumentierte Grundlage für die weiteren Analysen im Bereich vertrauenswürdiger Datenräume anzubieten. Das Modell wird dokumentiert, indem die Kernbegriffe eingeführt und erläutert werden. Anschliessend wird es in grafischer Notation auf der Basis eines internationalen Standards visualisiert und mit dem Modell der International Data Spaces Association (IDSA, vgl. IDS RAM 2019) in Bezug gebracht.

5.2 Modelldefinition und -aufbau

5.2.1 Massgebende Definitionen

5.2.1.1 Raum

Als "Raum" (engl. space) ist in diesem Zusammenhang im Sinn der mathematischen Definition (WolframAlpha 2021, Begriff "space") eine Menge (gemäss Definition aus der mathematischen Mengenlehre) von Objekten und eine Struktur (als Begriff aus der Algebra) dazu zu verstehen. Diese beruht entweder auf der den Objekten selbst zugrunde liegenden Struktur, oder ist eine an sich existierende.

Ein solcher Raum ist abstrakter Natur und nicht mit dem dreidimensionalen Anschauungsraum der euklidischen Geometrie gleichzusetzen. Seine Struktur ist durch einen Satz von Axiomen definiert. Erfüllt die Menge der betrachteten Objekte diese Axiome, gelten ihre Elemente als Elemente des Raums. Als grundlegende Eigenschaft gilt, dass nach der Durchführung sämtlicher Operationen, die auf diesem Raum zugelassen sind, nur Elemente entstehen, die wiederum Elemente des Raums sind. Ausserdem betrachtet man bei der Bildung des Raums nur diejenigen Eigenschaften, die durch die raumbildenden Axiome definiert sind. Von Bedeutung sind in erster Linie die Beziehungen zwischen Objekten, nicht die Objekte selbst. Elemente des Raums sind als Punkte zu verstehen, die durch *n* Komponenten parametrisiert sind. Der die Objekte umspannende Raum ist als n-dimensional zu betrachten. Zwischen diesen Punkten bestehen Verknüpfungen, die mittels (algebraischer) Operatoren eindeutig beschrieben sind. Verlassen Elemente einen Raum, so sind sie nicht mehr als dem Raum zugehörig einzustufen. Sie verlieren die Eigenschaften, die sie als Raumelement kennzeichnen.

22 Zur Definition von Selbstbestimmung und zu den Prinzipien der digitalen Selbstbestimmung siehe BAKOM (2020).
23 Es wird die folgende Notation aus der Linguistik verwendet: Bedeutungen in Anführungszeichen (semantische Ebene, Notation nach Frege), Benennungen in Schrägschrift falls sie Schlüsselwörter (lexikalische Ebene) und unterstrichen falls sie Einträge im Lexikon referenzieren (lexikalische Ebene).
24 Zur Definition von "Ontologie" im Sinn der Informatik und zu den Beziehungen mit der Philosophie (Metaphysik) siehe http://www-ksl.stanford.edu/kst/what-is-ontology und https://tomgruber.org/writing/ontology-definition-2007.htm.

5.2.1.2 Datenraum

Als Folge dieser Definition ist ein *Datenraum* als eine abstrakte Struktur zu betrachten, dessen Elemente *Daten* sind. Der Raum hat eine logische, keine physische Struktur und ist daher als *logisch* und *virtuell* zu bezeichnen. Seine physische Abbildung erzeugt eine physische Struktur, die nicht als Raum bezeichnet werden kann. Im Datenraum zugelassene Operationen (Speicherung, Zuweisung von Metadaten, Transformationen, Löschung, Import und Export; dazu siehe Kap. 5.2.1.7 "Operationen") erzeugen ausschliesslich wieder Daten, die als Elemente dieses Raums einzustufen sind. Die Raumelemente bestehen aufgrund einer rekursiven Beziehung aus anderen Daten oder sind nicht weiter zerlegbar. Eine solche zusammengesetzte Struktur wird als *Komposition* bezeichnet und beschreibt alle möglichen Strukturen von Daten.

5.2.1.3 Vertrauenswürdiger Datenraum

Eine besondere Form von Datenräumen ist der *vertrauenswürdige Datenraum.* Als solcher gilt ein Datenraum, der im Voraus festgelegten, genau definierten *Prinzipien* folgt. So wie Axiome die Struktur eines Raums im mathematischen Sinn festlegen, bestimmt die Erfüllung einer Menge fester Prinzipien, dass ein Datenraum als "vertrauenswürdig" definiert wird. Diese Definition ist gleichzeitig auch eine Klassifikation, weil ein vertrauenswürdiger Datenraum eine Unterklasse aller Datenräume ist. Als solcher weist dieser Raum alle Eigenschaften und Operationen der Oberklasse auf, verfügt aber noch über zusätzliche dazu.

Daten für Konsument*innen verfügbar zu machen, bedeutet zu definieren, für welche Gruppen sie zugänglich sind. Anzahl und Grösse (Zahl der Mitglieder*innen) dieser Gruppen, die auf diese Daten zugreifen können, bilden zusammen (im Sinn einer kumulativen, gewichteten[25] Beziehung) ein Mass für die Offenheit eines Datenraums. Dieses kann auf eine kategoriale Skala abgebildet werden. Daraus ergibt sich die Klassifikation in:

- Geschlossene Datenräume (engl. closed data spaces)
- Von verschiedenen Gruppen gemeinsam nutzbare Datenräume (engl. shared data spaces)
- Von jeder Gruppe nutzbare Datenräume (engl. open data spaces).

5.2.1.4 Daten

Ein *Datum* (Singularform von "Daten") ist gemäss ISO/IEC[26] definiert als Aussage über Tatsachen (engl. facts) in Form formalisierter und strukturierter Angaben in maschinenlesbarer Form. Ein einzelnes Datum weist folgende Eigenschaften auf:

- Es ist durch einen *Namen* benannt.
- Es ist durch einen *Typ* beschrieben. Man spricht genauer von einem *Datentyp.*
- Hat einen *Wert*, der dem Typ formell und inhaltlich entspricht.
- Es ist in einem gegebenen Zusammenhang mit einer Anzahl an Daten desselben Typs verbunden. Das Mass dieser Verbundenheit ist die *Kardinalität*.
- Es ist in einem gegebenen Zusammenhang entweder zwingend vorhanden oder nicht (engl. mandatory vs. optional). Das Mass dieser Verfügbarkeit als dichotomes Merkmal ist die *Optionalität.*
- Es kann als Folge von Problemen bei der Erhebung nicht verfügbar sein (engl. not available, mit dem Akronym NA abgekürzt).

Die Benennung eines Datums ist ein willkürlicher Vorgang, welcher von sozialen, kulturellen, politischen, technischen Vorgaben und Bedingungen abhängig ist. Falls die Benennung durch eine massgebende Quelle mit juristischer Verfügungs- und Entscheidungsgewalt eindeutig und verbindlich festgelegt ist, spricht man von einem *Term*. Die Autorität, welche die Benennung festlegt, ist ein terminologisches Büro. Eine Menge von Termen zu einem definierten Wissensbereich bildet eine *Terminologie*[27].

25 Die Gewichtung erlaubt die Berücksichtigung der Wichtigkeit und des Einflusses der entsprechenden Gruppe in Zusammenhang mit dem Datenraum.
26 Siehe ISO/IEC 2382:2015 Information Technology – Vocabulary (ISO - ISO/IEC 2382:2015 - Information technology — Vocabulary).
27 Dazu siehe bei der ISO-Standardisierungsorganisation den Bereich 01.020 "Terminology" (https://www.iso.org/ics/01.020/x/).

Da die Benennung willkürlich[28] (engl. arbitrary) ist, kann sie nicht allein für die Eindeutigkeit eines bestimmten Datums sorgen. Dafür ist eine *eindeutige Identifikation* (Kennung, engl. identification, als ID abgekürzt) notwendig. Diese legt fest, dass das von der Kennung referenzierte Datum, also das Objekt auf das diese Angabe hinweist und das Objekt selbst übereinstimmen. Sie sind im etymologischen Sinn "identisch", auf keinen Fall aber gleich[29]. Bei *Gleichheit* ist zwischen *struktureller* und *inhaltlicher* Gleichheit zu unterscheiden. Diese bewirkt, dass Objekte gleicher Struktur nicht auf dieselbe Referenz zeigen können, wenn sie nicht in den Werten aller ihren einzelnen Daten übereinstimmen. Um sie zu unterscheiden, sind *Metadaten* notwendig (z.B. Zeitstempel, Version, Geolokalisation). Erst in diesem Fall totaler struktureller und inhaltlicher Gleichheit handelt es sich um Kopien desselben Objekts[30].

Der mit den Daten verknüpfte Typ hat selbst eine Benennung. Seine Aufgabe besteht darin, den zugelassenen *Wertebereich* zu definieren. Damit verbunden sind die Regeln, welche die Zugehörigkeit eines Wertes zum Wertebereich beschreiben. Die Anwendung solcher Regeln, als *Validierung* bezeichnet (manchmal auch "Plausibilisierung", obwohl der Begriff auch eigene Konnotationen tragen kann), sichert die *Datenintegrität*. Damit vermeidet man, dass Werte mit unpassendem Datentyp dem Datum zugewiesen oder dass Sonderwerte als Nutzdaten erkannt werden. Hier ist zwischen *Ausreisser* und *Anomalien* zu unterscheiden. Während erstere als Folge einer methodisch falschen oder technisch fehlerhaften Erhebung entstehen, zeigen letztere Werte, die in einem (meist historischen) Zusammenhang aus statistischer Sicht mit Randwerten oder selten vorkommenden Werten zusammenhängen. Beide Arten von Datenwerten können nach geeigneter Interpretation wertvolle Informationen in Zusammenhang mit dem Datenzyklus[31] liefern. Neben Ausreissern und Anomalien bilden nicht verfügbare Datenwerte (Akronym NA für "not available") eine dritte Klasse von Problemfällen. Auch hier kann die Analyse der Ursachen wichtige Hinweise auf Probleme in der Lieferkette geben. Es ist möglich, fehlende Datenwerte durch Angaben des passenden Datentyps zu ersetzen. Dazu gibt es verschiedene Vorgehensweisen[32]. Kardinalität und Optionalität liefern quantitative Angaben über Wiederholbarkeit und Verfügbarkeit eines gegebenen Datums.

5.2.1.5 Qualität und Sicherheit

Zur Sicherung der Datenintegrität sind Massnahmen aus zwei Bereichen nötig: Qualitäts- und Sicherheitsmanagement. *Qualitätsmanagement* bietet Verfahren und Methoden zur Erstellung gültiger Daten und zur Vermeidung falscher, sowohl strukturell als auch inhaltlich. Dazu gehören auch Regeln und Vorschriften, die die Qualität von "gültig" und "falsch" auf operationeller Ebene technisch definieren und sichern. *Sicherheitsmanagement* bietet Verfahren und Methoden zum Schutz der Daten gegen Operationen an, die ihre Qualität beinträchtigen können, und solche zur Sicherstellung ihrer Verfügbarkeit gemäss den im Sicherheitsmodell definierten Rollen an. Ein solches Modell baut auf rollenbasierten Zugriffen gemäss RBAC-Modell[33]. Im Rahmen des Sicherheitsmanagements wird mithilfe von Verschlüsselungstechniken aus der Kryptografie das Datenschutzniveau der einzelnen Daten bestimmt. Man unterscheidet insbesondere zwischen unverschlüsselten (in Klartext vorliegenden), verschlüsselten, anonymisierten und pseudoanonymisierten Daten. In Zusammenhang mit vertrauenswürdigen Datenräumen spielt *Differential Privacy* eine wichtige Rolle. Die im Sicherheitsmanagement definierten Schritte zur Datensicherheit stützen sich auf die Resultate des Risikomanagements zum Risikoniveau und zur Sensitivität der analysierten Daten. Für die Überprüfung der Datensicherheit, insbesondere bei sensitiven Daten, sind Verfahren zu definieren (engl. PIAs, privacy impact assessments). Diese überprüfen die Einhaltung von Regeln (engl. governance rules) in der Praxis.

5.2.1.6 Physische Abbildung

Ein Datenraum ist mittels einer *Verteilungsstrategie* auf physische Speicherstrukturen abgebildet. Diese bilden den *logischen* Datenraum ab. Dieser dient der kurz-, mittel- und langfristigen Aufbewahrung der im logischen Raum enthaltenen Daten. Die Verteilungsstrategie legt fest, ob der logische Datenraum und seine physische Abbildung isomorph sind oder nicht. Im ersten Fall stimmen virtuelle und physische Struktur

28 Diese Willkürlichkeit ist Folge der Arbitrarietät des sprachlichen Zeichens als grundsätzliche Eigenschaft natürlicher Sprache.
29 Man vergleiche hier sameness und equality auf Englisch.
30 Man verweist hier auf die Begriffe deep copy und shallow copy auf Englisch
31 Der Begriff "Datenzyklus" an sich und in Zusammenhang mit vertrauenswürdigen Datenräumen ist in Kap. 3 besprochen.
32 Die Ableitung von Nutzdaten aus nicht vorhandenen Daten (NA) wird als Imputation bezeichnet.
33 RBAC ist Akronym für "role-based access model". Dazu siehe Role Based Access Control | CSRC (nist.gov).

überein, im zweiten handelt es sich um eine *verteilte physische* Struktur. Damit die physische Speicherstruktur das Ziel der effizienten[34], sicheren[35] und zuverlässigen[36] Speicherung erfüllen kann, müssen die Objekte aus dem logischen Datenraum in eine physische Form gebracht werden. Die zugrundeliegende Struktur ist als *Format* bezeichnet. Es definiert, in welcher Reihenfolge und mithilfe welcher Trennungselemente (engl. data delimiters) Daten physisch abgelegt werden. Dank der eindeutigen, dokumentierten Struktur (Format) können aus physisch gespeicherten Daten ohne Informationsverlust logische Datenstrukturen wiedergewonnen werden. Wegen der sequenziellen Struktur physischer Speichermedien spricht man von *Serialisierung* und *Deserialisierung* (engl. serialisation oder marshalling, bzw. deserialisation oder demarshalling).

Die physische Datenspeicherung muss zuverlässig sein. "Zuverlässigkeit" ist hier dadurch definiert, dass:

- Sämtliche Daten aus dem Datenraum während der vordefinierten Zeitspanne vollständig verfügbar sind.
- Die Daten in ihrer Struktur und in ihren Werten genauso vorliegen, wie sie zum ersten Mal in den Datenraum geliefert worden sind oder in der Form sind, in die sie aufgrund zugelassener Operationen umgewandelt worden sind.
- Die logischen Beziehungen zwischen den Daten physisch so abgebildet sind, dass nach der Deserialisierung das Beziehungsnetz wieder unverändert dargestellt werden kann.

Die physische Datenspeicherung als Umwandlung logischer in physische Datenstrukturen spielt eine zentrale Rolle auch beim Datenaustausch. Sie ist ein Thema bei der technischen Interoperabilität. Für die physische Abbildung und die Zuverlässigkeit der Datenspeicherung ist ausschliesslich die Betreiber*in des Datenraums verantwortlich. Andere Datenrollen sind nicht beteiligt, weil sie vertrauenswürdige Datenräume lediglich aus der logischen Sicht des virtuellen Raums betrachten und nutzen.

5.2.1.7 Operationen

Die in einem vertrauenswürdigen Datenraum zugelassenen Operationen trennen sich nach dem Entwurfsmuster "query and command" in lesende und schreibende Operationen.

Lesende Operationen erlauben den Zugriff auf Daten gemäss den angegebenen Suchparametern. Diese dienen als Filterkriterien, um aus dem Datenbestand eine Untermenge der Daten zu erhalten. Die Daten bleiben unverändert, d.h. ihre Werte vor und nach der lesenden Operation sind auf allen Stufen der betroffenen Datenstruktur gleich. Es handelt sich um idempotente Operationen ohne Nebenwirkungen. Neben den Suchfunktionen (engl. search) mit Eingabeparametern zur Eingrenzung des Suchraums gibt es identitätssuchende Funktionen (engl. find by id). Diese liefern zu einer eindeutigen Kennung (Schlüssel, engl. key) als Eingabeparameter die dazugehörige Datenstruktur. Wegen der geforderten Eindeutigkeit (engl. uniqueness) handelt es sich im mathematischen Sinn um eine eineindeutige Funktion (engl. univoque).

Zu den lesenden Operationen auf Datenebene gibt es auch solche für die übergeordnete Ebene der Metadaten. Einerseits geht es darum, die zu gegebenen Daten erhältliche Metadaten zu bekommen (engl. get metadata). Anderseits lassen sich Suchoperationen (search, find by id) auch auf Metadaten anwenden, da sie selbst Daten sind.

Schreibende Operationen sind wertverändernde Operationen, die die Werte der Daten oder auch ihre Struktur ändern. Bei der Durchführung solcher Funktionen muss stets geachtet werden, dass die Datenintegrität gewährleistet ist. Wichtigste Forderung in Zusammenhang mit vertrauenswürdigen Datenräumen ist, dass die von schreibenden Operationen erzeugten Daten (Rückgabetypen und -werte) zwingend Elemente des vertrauenswürdigen Datenraums sind. Die Nichteinhaltung dieser Forderung hat als Folge, dass die Prinzipien für vertrauenswürdigen Datenräume und letztlich die Axiome der Raumstruktur verletzt werden.

Die wichtigste Gruppe schreibender Operationen sind *Transformationen*, die Daten in andere Daten umwandeln. Dies kann auf Werteebene (inhaltlich) oder auf Datenstrukturebene (strukturell) stattfinden. Transformationen spielen eine entscheidende Rolle zur Sicherung der Datenqualität, eine wichtige Eigenschaft vertrauenswürdiger Datenräume. Finden Transformationen dann statt, wenn die Daten in den

34 In Bezug auf Speicherplatz, Kosten und Speichergeschwindigkeit.
35 Hinsichtlich unerlaubter Zugriffe, unsachgemässer Änderung oder gar Zerstörung der Daten.
36 Im Sinne der Abbildungstreue (DEF).

Datenraum eingeliefert werden und bevor jegliche Nutzung möglich ist, werden sie der Stufe der Vorverarbeitung (engl. preprocessing) zugeteilt. Hier findet Qualitätssicherung statt, was zur Annahme oder Ablehnung der gelieferten Daten führt.

Eine andere Gruppe schreibender Operationen sind *Formatierungen*. Diese lassen die bestehenden Daten an sich unverändert, bringen sie aber in eine andere Form (engl. format). Eine Formatierung wird angewendet, um proprietäre Formate in (quell-)offene Formate (engl. open data) umzuwandeln. Damit erfüllt man wichtige Forderungen vertrauenswürdiger Datenräume bezüglich Transparenz, Suchbarkeit, Introspektion und Reflexion. Wendet man nach der Formatierung zu offenen Daten eine besondere Art von Transformationen an, die *Anreicherung* (engl. data enrichment), können zu den offenen Daten noch Referenzen (engl. links) hinzugefügt werden. Die Verkettung von Formatierungen und Anreicherungen führt zur Umsetzung der LOD-Strategie (engl. linked and open data). Diese sichert den Informationsaustausch unter vertrauenswürdigen Datenräumen und erlaubt die Föderierung von Datenplattformen zu grossen, virtuellen Wissensressourcen.

Die Gruppe der schreibenden Operationen mit weitreichenden Folgen ist diejenige der *Löschungen*. Es handelt sich um Prozeduren und nicht Funktionen, weil sie keine Resultate liefern und durch Nebenwirkungen (engl. side effects) die Umgebung (also den Datenraum) verändern. Hier spielen die rechtlichen und ethischen Probleme eine entscheidende Rolle. Das Eigentumsrecht und das Recht auf Vergessen müssen durch entsprechende Schutzmechanismen und Beschwerdeverfahren sichergestellt werden.

Eine besondere Form von (schreibenden) Operationen sind *Speicheroperationen* (engl. save, restore). Diese bewirken zwar Änderungen im dem vertrauenswürdigen Datenraum zugrundeliegenden physischen Speicher(-raum), sind aber aus Sicht des vertrauenswürdigen Datenraums lesende Operationen. Die betroffenen Daten werden unverändert zur langlebigen Aufbewahrung abgelegt. Wenn sie aus dem Speicherraum geholt werden, gilt als Forderung, dass sie ebenso unverändert zur Verfügung stehen, wie sie abgelegt worden sind. Diese Forderung ist logisch nicht erfüllt, wenn die Daten nach der Speicherung den Datenraum verlassen. In diesem Fall können aber möglicherweise sämtliche Prinzipien eines vertrauenswürdigen Datenraums verletzt sein. Die Verkettung beider Speicherfunktionen (Abgabe in den Speicherraum und Entnahme daraus) ist aus Sicht der mit den Daten in Bezug stehenden Rollen eine Identitätsfunktion. Bei den Speicheroperationen spielt es aus dieser Sicht auch keine Rolle, ob es sich bei der Datenablage um einen Mechanismus zur Datensicherung zur Wiederverwendung handelt (kurz-, mittel- und langfristige Perspektive) oder um einen Archiv zur langlebigen Aufbewahrung handelt.

Zugelassene Operationen sind notwendige Voraussetzungen zur Erfüllung grundlegender Eigenschaften von vertrauenswürdigen Datenräumen: Integrität, Dauerhaftigkeit, Zuverlässigkeit, Suchbarkeit, Auskunfts-fähigkeit.

Die Ausführung von Operationen muss in einem vertrauenswürdigen Datenraum ständig und lückenlos geprüft werden. Mittels Authentisierung und Autorisierung auf der Basis eines Rollenmodells wird der vertrauenswürdige Datenraum gegen unerlaubte Anwendung von Operationen geschützt. Damit wird Schutzbarkeit als grundlegende Eigenschaft erfüllt.

5.2.2 Konstruktion von vertrauenswürdigen Datenräumen

Es sind Prinzipien, die vertrauenswürdige Datenräume von allen anderen Arten von Datenräumen unterscheiden. Diejenigen Prinzipien, welche zur Definition vertrauenswürdiger Datenräume führen, sind im Kapitel 3 dieses Berichts beschrieben. Im Vordergrund stehen dabei die Prinzipien auf individueller und auf kollektiver Ebene. Bei den individuellen Prinzipien handelt es sich gemäss Abschnitt 3.1 um:

- Transparenz
- Vertrauen
- Verständlichkeit
- Vorhersehbarkeit
- Kontrolle
- Solidarität.

Bei den Prinzipien auf kollektiver Ebene handelt es sich gemäss Abschnitt 3.2 um:

- Fairness
- Datenaustauschbarkeit
- Interoperabilität
- Skalierbarkeit
- Nachhaltigkeit
- Politikunterstützung
- Wirtschaftswachstum.

Vertrauenswürdige Datenräume weisen folgende *Eigenschaften* auf: Sie sind

- *Geschützt*, in dem Sinn, dass nur Personen in den dafür vorgesehenen Rollen Daten in einen solchen Raum liefern, sie bearbeiten oder beziehen können. Diese Eigenschaft bezeichnet man als *Schützbarkeit*. Mit dieser Eigenschaft wird *Sicherheit* gewährleistet.
- *Sicher*, weil durch geeignete Steuerungs- und Überwachungsmechanismen sichergestellt wird, dass Daten nicht versehentlich oder wegen unzulässiger Bearbeitung in ihrer Form oder ihrem Inhalt verändert werden, so dass sie nicht mehr erkennbar oder nutzbar sind. Diese Eigenschaft bezeichnet man als *Integrität* bezüglich Inhalt oder Form. Mit dieser Eigenschaft wird *Sicherheit* gewährleistet.
- *Langlebig*, weil die betreffenden Daten innerhalb vordefinierter Zeitspannen zur weiteren Nutzung vorhanden sind. Diese Eigenschaft bezeichnet man als *Dauerhaftigkeit* (engl. persistence).
- *Geprüft*, weil eine für Betrieb und Unterhalt des Datenraums zuständige Organisation die Datenlieferungen überwacht und nicht zugelassene Daten zurückweist. Diese Zulassung betrifft sowohl die Inhalte als auch Mechanismen krimineller Art ("Viren" in der breitesten Bedeutung), die die Datenbestände teils oder ganz zerstören können. Diese Eigenschaft bezeichnet man als *Zuverlässigkeit*.
- *Standardisiert und normiert*, weil nur Daten in bekannten, dokumentierten und offenen Formaten zwischen Datenräumen effizient und verlustfrei austauschbar sind. In diesem Zusammenhang sind insbesondere die Ansprüche von LOD (Linked and Open Data) zu erfüllen. Diese Eigenschaft bezeichnet man als *Interoperabilität.*
- *Durchsuchbar*, weil Mechanismen zur Verfügung stehen, um in den Datenbeständen Untermengen von Daten mithilfe von Suchbegriffen oder Abfragen[37] zu finden. Diese Eigenschaft nennt man *Suchbarkeit*.
- *Auskunftsfähig*, weil Informationen über die Datenbestände, ihre Veränderungen als Folge wertverändernder Operationen, die beteiligten Rollen und die den Daten zugrundeliegenden Strukturen geliefert werden können. Die gelieferten Informationen sind Daten über die Daten, also *Metadaten*. Die Eigenschaft, mithilfe von Metadaten Daten zu verstehen, bezeichnet man als *Introspektion* oder *Reflexion*. Sie ist eine notwendige Bedingung für ein Audit[38].

Die oben angegebenen *Eigenschaften* vertrauenswürdiger Datenräume *sichern* (direkt oder indirekt) *die Einhaltung der* individuellen und der kollektiven *Prinzipien*. Die untenstehenden Angaben erklären den Zusammenhang zwischen Eigenschaften und Prinzipien für jedes einzelne Prinzip. Dabei stützt man sich grösstenteils auf die in Kapitel 3 gemachten Angaben ab. Anzufügen ist jedoch, dass für die Modellkonzeption verschiedentlich abweichende, teilweise vereinfachende Annahmen getroffen werden mussten, um eine konkrete Modellausgestaltung vorschlagen zu können.

37 Abfragen werden durchgeführt, indem mittels geeigneter formalen Sprachen spezifiziert, welche Eigenschaften die Daten aufweisen müssen, die man sucht. Solche Sprachen sind deskriptiv, weil sie diese Eigenschaften beschreiben, aber nicht angeben, wie die entsprechenden Daten zu beschaffen sind.

38 Ein Audit untersucht, ob ausgewählte Artefakte entsprechende Vorgaben (z.B. Normen, Standards, Gesetze) erfüllen.

5.2.2.1 Verständnis der individuellen Prinzipien für die Modellkonzeption

Transparenz
Wie in Kap. 3.1.1 erwähnt, sind die Prinzipien *Transparenz, Vertrauen, Verständlichkeit, Vorhersagbarkeit* verwoben. In diesem Sinn tragen auch verschiedene Eigenschaften dazu bei, diese Prinzipien zu sichern. *Transparenz* ist zuerst durch *Integrität* gegeben, weil die dem vertrauenswürdigen Datenraum gelieferten Daten unverändert und unversehen den Nutzer*innen zur Verfügung stehen. Die Abgabemechanismen sind dokumentiert und nachvollziehbar, sodass Herkunft und Zweck der gelieferten Daten sichtbar sind. Auf der Basis entsprechender Sicherheitsmechanismen ist auch erkennbar, wer in welcher Rolle Daten liefert, auf diese Daten zugreift und Operationen darauf anwendet. In diesem Sinn trägt auch *Schützbarkeit* zur Erfüllung der Transparenz bei. Die zur Sicherung der Datenqualität eingesetzten Mechanismen sind ebenfalls dokumentiert und nachvollziehbar. Diese sorgen dafür, dass Transparenz in der Datenprüfung erfüllt ist. Die Gewinnung geprüfter Daten ist für Nutzer*innen einsehbar ("transparent") und verständlich. Sie führt dazu, dass zuverlässige Daten zur Nutzung verfügbar sind. Somit trägt auch *Zuverlässigkeit* zur *Transparenz* bei.

Vertrauen
Geschützte, *sichere*, *langlebige*, *geprüfte* Daten sorgen dafür, dass alle beteiligten Akteur*innen (insbesondere Bürger*innen) *Vertrauen* in die vertrauenswürdigen Datenräume aufbauen.
Vertrauen entsteht, weil:

- Geschützte Daten nicht willkürlich und unkontrolliert verändert werden können.
- Sichere Daten nicht versehentlich oder willentlich durch Unbefugte benutzt werden können.
- Langlebige Daten so lange unverändert verfügbar sind, wie von ihren Lieferanten vorgesehen worden ist. Innerhalb der vereinbarten Zeitspanne stehen sie für die erlaubten Nutzungsarten zur Verfügung.
- Geprüfte Daten wegen ihrer dank transparenter Bearbeitungsverfahren erreichten Qualität zuverlässig sind.

Verständlichkeit
Dieses Prinzip wird durch *Introspektion/Reflexion* und die Bereitstellung von *Metadaten* erfüllt. Die zur Verfügung stehenden Rohdaten werden durch Metadaten ergänzt, welche ihre Verständlichkeit durch Schaffung eines Kontexts zur Interpretation sicherstellen. Erst durch die Metadaten werden diese Daten auf syntaktischer Ebene zu Informationen auf semantischer Ebene. Solche Informationen können von den Nutzer*innen des vertrauenswürdigen Datenraums kontextabhängig interpretiert und somit verstanden werden. Erst die Anwesenheit von Metadaten sichert die Verständlichkeit der (Roh-)Daten. Mit ihrer Hilfe kann der Zusammenhang verstanden werden, in dem die Daten entstanden sind und benutzt werden. Damit kann der (semantische) Kontext gebildet werden, innerhalb dessen Daten (syntaktische Ebene) zu Informationen (semantische Ebene) werden, also Bedeutung erhalten. Metadaten sind auch unentbehrliche Grundlage für die Datenqualität. Verfahren und Techniken zu Metadaten sind Aufgabe des Metadatenmanagements.

Vorhersehbarkeit
Die zur Verfügung stehenden Daten und die dazugehörigen Metadaten sind mittels genau definierter und dokumentierter Mechanismen durchsuchbar. Die *Durchsuchbarkeit* verfügbarer Daten bildet die Grundlage der *Vorhersehbarkeit*. Die Anwendung mächtiger Suchmechanismen auf einer gesicherten und geprüften Datenbasis liefert die geeigneten Daten, um Vorhersagen (Prognosen) zu treffen. Da die Suchmechanismen bekannt und dokumentiert sind, lassen sich die Suchergebnisse validieren. Sind die zur Prognosebildung verwendeten Algorithmen ebenfalls spezifiziert und validiert, können die Berechnungsergebnisse auf der Basis vorhersehbarer, validierter Daten ebenfalls als überprüft und vertrauenswürdig betrachtet werden.

Kontrolle
Die an einem vertrauenswürdigen Datenraum abgegebenen Daten sind durch passende Verträge gesichert. Ihre Integrität ist durch die Datenraumbetreiber*in aufgrund juristisch bindender Abmachungen gesichert. Die im Datenraum vorhandenen Sicherheitsmechanismen regeln Zugriff und Nutzung der angebotenen Daten durch Authentisierungs- und rollenbasierte Autorisierungsverfahren.

Auf Daten angewendete Operationen unterliegen ebenfalls Sicherheitsmechanismen. Aus rechtlichen Gründen (siehe Kap. 3.1.2) sind insbesondere Freigabe und Löschung kritische Operationen. Beim Datenangebot muss die Datenraumbetreiber*in die Notwendigkeit einer Datenanonymisierung besonders berücksichtigen und entsprechende technische Lösungen anbieten.

Solidarität
Die im vertrauenswürdigen Datenraum vorhandenen Sicherheitsmechanismen müssen so ausgelegt werden, dass alle dazu berechtigten Nutzer*innen in der Lage sind, die zur Verfügung stehenden Daten einzusehen und zu beziehen. Die mittels Sicherheitsmechanismen definierten Bedingungen für die Datennutzung müssen sicherstellen, dass Daten unter Nutzer*innen geteilt werden (engl. data sharing). Jede beteiligte und berechtigte Partei muss in der Lage sein, die für sie zugelassenen Daten zu suchen, zu lesen und zu beziehen.

5.2.2.2 Verständnis der kollektiven Prinzipien für die Modellkonzeption

Fairness
Das Angebot an Daten durch die Betreiber*in verursacht Aufwände verschiedener Art:

- Betrieb der digitalen Plattform
- Sammlung der Daten
- Aufbereitung der Daten einschliesslich Verfahren zur Sicherung der Datenqualität
- Langlebige, sichere Datenspeicherung.

Durch entsprechende Verträge und Regelungen muss sichergestellt werden, dass die durch diese Aufwände entstehenden Kosten fair unter allen betroffenen Parteien geteilt werden. Dazu gehört auch ein Geschäftsmodell für Betrieb und Unterhalt der Datenplattform und für die angebotenen Dienstleistungen des vertrauenswürdigen Datenraums.

Fairness ist keine Eigenschaft der Daten an sich. Es handelt sich um ein Prinzip, welches von der Datenraumbetreiber*in sichergestellt, durch entsprechende Organisationen (Regulationsbehörde) definiert und in seiner Umsetzung überprüft werden muss.

Datenaustauschbarkeit
Der Datenaustausch zwischen Datenräumen setzt voraus, dass die Daten in einer Form vorliegen, die erkennbar und zur weiteren Verarbeitung geeignet ist. Die Sicherung der *Interoperabilität* ist die notwendige Grundlage für den Datenaustausch. Eng verknüpft damit ist die Verfügbarkeit von Metadaten, die von der Quelle an die Senke geliefert werden müssen, um die Rohdaten mittels *Introspektion/Reflexion* richtig zu interpretieren.

Ein Angebot an Schnittstellen zum Bezug und Austausch von Daten sichert die *Datenautauschbarkeit* zwischen Datenräumen untereinander und zwischen ihnen und externen Informationssystemen. *Interoperabilität* ist die notwendige Bedingung dazu.

Der Datenaustausch ist aber nur dann sinnvoll, wenn Daten in gesicherter Qualität vorliegen und von geprüften Lieferanten stammen. *Zuverlässigkeit* ist deshalb auch eine wichtige Eigenschaft zur Sicherung eines erfolgreichen Datenaustausches. Auch sie dient zur Erfüllung der *Datenaustauschbarkeit*.

Dieses Prinzip beruht aber nicht auf Eigenschaften der Daten an sich. Für seine Umsetzung muss die Betreiber*in entsprechende technische Massnahmen vorsehen und realisieren, um Datenaustauschbarkeit zu sichern.

Datenqualität
Daten zur Nutzung anzubieten ist nur sinnvoll, wenn ihre Qualität stimmt. Dafür muss die Betreiber*in ein Qualitätsmanagement aufsetzen und entsprechende Verfahren regelmässig anwenden. Die Sicherung der Datenqualität setzt proaktive, möglichst automatisierte Mechanismen voraus. Die Resultate der Qualitätsprüfungen einschliesslich der dafür verwendeten Operationen müssen protokolliert und den Nutzer*innen zur Einsicht zur Verfügung gestellt werden.

Skalierbarkeit
Der virtuelle, logische Datenraum – sowie er von den Nutzer*innen wahrgenommen wird – ist auf eine physische Struktur von Rechner- und Speicherknoten in einem Netzwerk abgebildet. Diese nur für die Betreiber*in sichtbare Struktur muss in der Lage sein, bei hoher Last die vertraglich abgemachten Leistungen anzubieten. Es handelt sich um die physische Sicht der *Skalierbarkeit*. Mittels SLAs (engl. service-level agreements) wird sichergestellt, dass die dem Datenraum zugrundeliegende Plattform diese

Qualitätsanforderungen erfüllt. Wichtige Überlegungen zur Skalierbarkeit betreffen Dezentralität, Verteilungsmechanismen und Redundanz hinsichtlich Rechnerleistung und Datenspeicherung. Dezentral ausgelegte Datenräume sichern eine föderierte, kooperative Struktur von Datenplattformen zu, welche im Vergleich zu zentralen Lösungen sowohl technische (Problem des "single point of failure") als auch organisatorische und politische (bezüglich Datenhoheit und -kontrolle) Vorteile anbieten.

Aus Sicht der Datengewinnung bedeutet *Skalierbarkeit* die Fähigkeit, neue Datenquellen an die Datenplattform anschliessen zu können. Somit kann die Betreiber*in den Nutzer*innen zusätzliche Daten anbieten. Diese müssen auch in der Lage sein, die Betreiber*in auf neue Datenquellen hinweisen zu können. Diese hat ihrerseits die Aufgabe, diese Quellen zu erschliessen, Daten zu beziehen und sie in möglichst guter Qualität und in interoperablen Formaten anzubieten.

Skalierbarkeit beruht auf keiner Eigenschaft der Daten an sich. Es handelt sich um ein Prinzip, welches von der Datenraumbetreiber*in sichergestellt werden muss.

Nachhaltigkeit
Dieses Prinzip betrifft einerseits die Daten und anderseits die Datenplattform.

In erster Linie geht es um die Verwendung der vorhandenen, angebotenen Daten zur Überwachung von Umweltzuständen und -ereignissen, sowie zur Verbesserung der Energieeffizienz. Es handelt sich nicht um eine Eigenschaft der Daten an sich, sondern um eine besondere, gezielte Form der *Datennutzung*. Diese kann soowhl im Rahmen von Forschungsprojekten um Umwelt- und Energiebereich als auch in Zusammenhang mit Monitoringverfahren mittels IoT (engl. Internet of Things) stattfinden.

Wichtige Komponenten der *Nachhaltigkeit* in zeitlicher Perspektive sind *Beständigkeit* und *Dauerhaftigtkeit* der Daten (engl. data persistence). Diese sind durch eine geeignete, sichere physische Speicherung gegeben.

In zweiter Linie geht es um die Art und Weise, wie die physische Datenplattform betrieben wird. Diese muss mittels umweltschönender, energiesparender Massnahmen so betrieben werden, dass die Aufwirkungen des IT-Betriebs auf die Umwelt (Energieverbrauch, Wärmeproduktion, CO_2-Ausstoss, Material für den IT-Betrieb und damit verbundene Recycling-Verfahren) minimiert werden können. Auch hier handelt es sich nicht um eine Eigenschaft der Daten an sich, sondern um die Strategien für Betrieb und Unterhalt er physischen IT-Infrastruktur im Sinn einer "Green IT".

Politikunterstützung und Wirtschaftswachstum
Ein Angebot an frei verfügbaren, allgemein zugänglichen, geprüften, hochwertigen und dokumentierten Daten unterstützt die politischen Handlungen in einer demokratischen Gesellschaft (*Politikunterstützung*), indem es Informationen bereitstellt, die im Rahmen politischer Massnahmen und Entscheidungen eingesetzt werden. Da diese Informationen aus vertrauenswürdigen Datenräumen stammen, sind sie selbst vertrauenswürdig. Dabei unterscheiden sie sich von ungeprüften Angaben, wie sie zum Beispiel in Form von fake news zu finden sind.

Ein Datenangebot aus vertrauenswürdigen Datenräumen führt zu *Wirtschaftswachstum*, weil gesicherte Informationen in guter Qualität die Grundlagen für Entscheidungsvorgänge der beteiligten Agenten im Markt bilden. Aus betriebswirtschaftlicher Sicht sind Daten in Organisationen und Unternehmen als Vermögen (engl. asset) zu betrachten. Die *Infonomics* (Wortbildung aus "information" und "economics"[39]) versucht, den Wert solcher Vermögen quantitativ festzuhalten.

5.2.3 Typen von Datenräumen

Datenräume können als virtuelle Märkte von Daten betrachtet werden. In dieser Funktion lassen sie sich nach verschiedenen Kriterien in Typen unterteilen.

[39] Dazu siehe als Übersicht https://www.gartner.com/en/publications/infonomics und https://www.gartner.com/en/information-technology/glossary/infonomics, sowie http://mitiq.mit.edu/IQIS/Documents/CDOIQS_201177/Papers/05_01_7A-1_Laney.pdf .

In ihrer Funktion als Drehscheiben zu Angebot und Konsum von Daten (Datenplattformen) können sich vertrauenswürdige Datenräume nach sozialen Modellen richten, die auf Austausch und gemeinsamer Nutzung aufbauen. In diesem Sinn kann gemäss Kap. 4.2 zwischen folgenden Typen unterschieden werden:

- Data Trusts
- Data Cooperatives
- Data Commons.

Ihre Eigenschaften sind im genannten Kapitel detailliert beschrieben. Die verschiedenen Typen lassen sich in der Praxis nicht eindeutig voneinander trennen.

Eine weitere Aufteilung unterscheidet zwischen folgenden Datenräumen:

- Themenbezogene
- Sektorspezifische.

Datenräume können Daten enthalten, die zwar themenbezogen *(themenbezogene Datenräume*), aber wegen der Vielfalt an Interessen der Bürger*innen nicht sektor- oder branchenspezifisch sind. Für Gesellschaft und Wirtschaft haben aber Daten eine zentrale Bedeutung, insbesondere in Zusammenhang mit Datenaustausch und -wiederverwendung. *Interoperabilität* als Fähigkeit zum reibungslosen Austausch standardisierter und normierter Daten bedeutet für Partner eines Wirtschaftszweiges, dass sie in der Lage sind, mit niedrigen Kosten in kurzer Zeit und mit wenigen, möglichst automatisierten Schritten Daten untereinander auszutauschen. Daher spielen *sektorspezifische Datenräume* eine wichtige Rolle im wirtschaftlichen Handel (vgl. entsprechende Hinweise in Kap. 4.3).

Zusätzlich können Datenräume hinsichtlich ihrer geographischen und politischen Bedeutung unterteilt sein in:

- Internationale
- Nationale
- Regionale (in der Schweiz: kantonale, überkantonale und innerkantonale)
- Kommunale (in der Schweiz: Gemeinde).

Die Einhaltung der oben erwähnten Prinzipien setzt eine ständige Überwachung des vertrauenswürdigen Datenraums voraus. Diese ist technisch durch Monitoring zu realisieren. Um die von den Prinzipien abgeleiteten Eigenschaften auszuweisen, muss ein vertrauenswürdiger Datenraum von einer bekannten und anerkannten Organisation betrieben werden. Diese hat eine juristische Form gemäss Zivilrecht (OR und ZGB), was dazu führt, dass sie vor Gesetz haftbar ist, falls Vertragsbedingungen in Zusammenhang mit dem von ihr betriebenen vertrauenswürdigen Datenraum verletzt werden. In den allgemeinen Geschäftsbedingungen (AGB), in den Rahmenverträgen und in den Einzelverträgen sind Pflichten und Rechte, die zwischen Vertragsparteien gelten, gemäss geltendem Recht festgelegt.

Die an einem vertrauenswürdigen Datenraum beteiligten Parteien müssen in der Lage sein, bei Problemfällen Rückmeldungen zu geben und Beschwerde einreichen zu können. Dafür müssen in Zusammenhang mit Datenräumen offizielle Verfahren festgelegt werden, die von einer neutralen Stelle bearbeitet werden. Dieses Prinzip führt dazu, dass die Mechanismen zur Einreichung und Behandlung von Beschwerden Bestandteile des Modells vertrauenswürdiger Datenräume sind.

Überwachung, Beschwerdemöglichkeiten sowie die dokumentierte Umsetzung der Prinzipien aufgrund prüfbarer Eigenschaften und deren Gegenprüfung durch beteiligte Bürger*innen stellen die notwendigen technischen Massnahmen zur Umsetzung der Prinzipien für vertrauenswürdige Datenräume. Diese Massnahmen sind die Implementierung von einklagbaren Durchsetzungs- und Kontrollmechanismen und von nicht verbindlichen Instrumenten, wie sie in Kap. 3.3 beschrieben sind.

5.2.4 Datenrollen in vertrauenswürdigen Datenräumen

Auf einer Seite tritt die *Betreiber*in*[40] als Anbieter*in von Dienstleistungen in Zusammenhang mit dem vertrauenswürdigen Datenraum auf. Auf der anderen Seite gibt es unterschiedliche Parteien, die je nach Ziel und Zweck in folgenden Rollen auftreten:

- Datenproduzent*innen
- Datenanbieter*innen
- Datenkonsument*innen.

Die Teilnahme der hinter den Rollen stehenden Individuen wird durch Anreize gefördert und verstärkt. Dazu siehe Kap. 2.2.1.2.

Statt von der marktorientierten Unterscheidung[41] zwischen Produzent*innen und Konsument*innen, geht man hier von einer zusätzlichen Einteilung der Produzent*innen aus. Man unterscheidet zwischen *Datenproduzent*innen* als erzeugende Instanzen der Daten und *Datenanbieter*innen* als solche, die diese Daten in den Datenräumen einliefern. Erstere sind für die physische Produktion (Datenerzeugung) zuständig. Bei ihnen entstehen die Daten, welche dann dank der Vermittlung der Anbieter*innen in den Datenraum gelangen. Beide Rollen können, müssen aber nicht übereinstimmen. Ein Beispiel dazu sind medizinische Daten, die im Rahmen von Untersuchungen, Behandlungen und Operationen in Spitälern, Kliniken, Arztpraxen, Laboratorien entstehen. Die Patientin, der diese Daten gehören, kann sie nach eigenem Ermessen in einer bestimmten Form (z.B. als Patientendossier) in einem vertrauenswürdigen Datenraum ablegen. Sie bietet Daten an, die von anderen erstellt worden sind. In einem anderen Zusammenhang kann ein Spital Daten bereitstellen (z.B. zu Forschungszwecken). In diesem Fall stimmen Produzent*innen und Anbieter*innen überein. Es ist auch möglich, dass Daten, welche zu einer eigenständigen[42] Datenstruktur gehören, von mehreren Anbieter*innen bereitgestellt werden. Ein Beispiel dafür ist das Patientendossier, dessen Inhalte von mehreren medizinischen Organisationen und Institutionen erstellt wird.

Die dem Datenraum anvertrauten Daten können in Bezug auf Personen eingestuft werden als:

- Personendaten im Allgemeinen
- Besonders schutzwürdige Personendaten
- Personenbezogene Daten (direkte Beziehung und Bezug zu Drittpersonen)
- Sachdaten als objektbezogene Daten (mit keinem direkten Bezug zu Personen).

Das Datenschutzniveau und die Bewertung des Personenbezugs der Daten (engl. data privacy) sind zwischen Rechtsräumen unterschiedlich, was sich in der unterschiedlichen Auslegung auf Gesetzesebene widerspiegelt. Datenschutz hat Kontrolle als Folge. Zu diesem Thema in Zusammenhang mit Grundrechtsschutz und Solidarität siehe Kap. 3.1.2.

Die Anbieter*in übernimmt bei der Abgabe der Daten in den vertrauenswürdigen Datenraum die Rolle der *Datenbesitzer*in* (engl. data owner)[43]. Gemäss der Beschreibung dieser Rolle in der Fachliteratur über Data Management hat sie gegenüber anderen Parteien entsprechende Rechte und Pflichten. Besonders hervorzuheben ist die Haftung für den Umgang mit den eigenen Daten. In einem vertrauenswürdigen Datenraum muss für jeden Datenstrom, der hineinkommt oder ihn verlässt, eine verantwortliche Person in der Rolle des Data Owners definiert werden.

Die *Datenbesitzer*in* definiert Verfügbarkeit und Wiederverwendung ihrer Daten mittels einer besonderen Art von Verträgen, der *Lizenzen*. Diese müssen von den Konsument*innen der lizenzierten Daten wahrgenommen werden, weil sie die Art und Weise regeln, wie diese Daten weiterverwendet werden. Eine besondere Form solcher Lizenzen sind solche aus dem Open-Source-Bereich, die in verschiedenen Ausprägungen vorhanden sind (z.B. die Creative Commons License CC[44]).

40 In Kap. 2.2.2 sind die Kerneigenschaften einer Datenraumbetreiberin auf kollektiver Ebene besprochen.
41 Aus Sicht der klassischen Ökonomie.
42 Im Sinn von "in sich geschlossen", "selbständig", "nicht von anderen abhängig".
43 In Kap. 2.2 wurde bereits festgestellt, dass eine uneinheitliche Terminologie besteht: Bürger*Innen, betroffene Personen und Datensubjekten.
44 Dazu siehe Mehr über die Lizenzen - Creative Commons

Als Spiegelbild zur Aufteilung in Datenproduzent*innen und -anbieter*innen, hat man auf der Konsumseite die *Datenkonsument*innen* (engl. data consumer) und *-nutzer*innen* (engl. data user). Wie es auch auf der Produktionsseite der Fall ist, können auch hier beide Rollen übereinstimmen, indem sie sich auf die gleiche Person beziehen. Der Unterschied besteht darin, dass Datennutzer*innen die von den Anbieter*innen bereitgestellten Daten verwenden, während Datenkonsument*innen diese Daten vom Datenraum beziehen, um sie den Nutzer*innen zur Verfügung zu stellen. Ein Beispiel dafür sind Patient*innen, die ihre Daten für medizinisches Fachpersonal (Ernährungsberater*innen, Physiotherapeut*innen usw.) zugänglich machen, damit sie beraten werden können. Der Zugang zu diesen Daten findet über eine App statt, die aus technischer Sicht als Konsument*in auftritt.

Sowohl Produzent*innen als auch Anbieter*innen und Konsument*innen gehören zu sozialen Gruppen. Die persönlichen, aus dem eigenen Wertesystem abgeleiteten Werte in Bezug auf die eigenen Daten (insbesondere den psychologischen Wert als Mass der emotionalen Bindung zu den Rohdaten), können die je nach Grad der Zugehörigkeit zu einer oder mehreren sozialen Gruppen auch in einem bestimmten Ausmass mit Werten dieser Gruppen übereinstimmen. Dazu ist noch die *Public Value* zu berücksichtigen, sowohl in Bezug auf einzelnen Gruppen als auch gruppenübergreifend.

Aus Sicht der Datenbesitzer*in müssen die von ihr abgegebenen Daten durch die für den Datenraum verantwortliche Instanz geschützt werden. Diese als *Betreiber*in* bezeichnete Organisation kann eine privat- oder öffentlich-rechtliche Struktur sein. Ein besonderer Fall liegt vor, wenn der Staat als Betreiber des vertrauenswürdigen Datenraums auftritt[45]. Bei privatrechtlichen Organisationen ist noch zu unterscheiden, ob es sich um gewinnorientierte (kommerzielle) oder nicht-gewinnorientierte (engl. no-profit) Organisationen handelt. Für Betrieb, Unterhalt und Sicherung des Datenraums sind bei der Betreiber*in *Datenmitarbeiter*innen* (engl. data officer) in verschiedenen organisatorischen Funktionen angestellt. Ihre Tätigkeiten sind in einer Stellenbeschreibung definiert, was auch entsprechende Rechte und Pflichten in Zusammenhang mit dem Datenraum und den darin enthaltenen Daten einschliesst. Durch Prozesse der *Compliance* wird sichergestellt, dass Verhalten und Arbeitsweise der Datenmitarbeiter*innen den Organisationsrichtlinien[46] (engl. policies) entsprechen.

5.2.5 Datenaustausch zwischen Datenräumen

Alle Arten von Datenräumen – und somit auch vertrauenswürdige – müssen zum Bezug und Lieferung von Daten durch externe Akteure, zum Datenaustausch mit anderen Datenräumen oder mit Informationssystemen Schnittstellen definieren und dokumentieren. Neben der verbindlichen Beschreibung der angegebenen Funktionen gehört zwingend die Spezifikation der ausgetauschten Daten, deren Strukturen und Typen (mit Wertebereichen) dazu. Die bei der Ausführung der zugelassenen Funktionen entstehenden Probleme müssen in Form von Ausnahmen (engl. exceptions) ebenfalls dokumentiert sein. Dazu gehören noch die Rahmenbedingungen, die die Skalierbarkeit solcher Schnittstellenimplementierungen sichern.

Ein reibungsloser Datenaustausch ist notwendige Bedingung für die *Datenportabilität*. Diese ermöglicht den Abzug der Daten aus einem Raum und die darauffolgende Abgabe in einen anderen. Dies ist nicht nur eine technische Angelegenheit, sondern zuerst ein Recht der Datenbesitzer*in (dazu siehe Kap. 3.1.2).

Beim *Datenexport* werden Daten eines vertrauenswürdigen Datenraums so aufbereitet, dass sie diesen Raum verlassen können, um anderweitig verwendet zu werden. Genau bis zum Punkt der vollständigen Aufbereitung zwecks Export sind diese Daten immer noch vertrauenswürdig. Sobald sie aber in für den Export geeignete Form die Grenzen des Raums verlassen, verlieren sie die Eigenschaften, die sie als vertrauenswürdige Daten kennzeichnen. Das Überschreiten der Grenzen führt dazu, dass die Prinzipien, die zur Bildung und Aufrechterhaltung eines vertrauenswürdigen Datenraums notwendigerweise eingehalten werden müssen, nicht mehr sichergestellt werden können. Die Betreiber*in ist nicht mehr in der Lage, diese Prinzipien durchzusetzen, weil sich die Daten ausserhalb ihrer Einflussreichweite befinden. Diese Tatsache ist aus der axiomatisch begründeten Definition eines Raums abzuleiten. Sie gilt in der Folge zuerst für

45 Zu diesem Punkt siehe Kap. 2.2.2.2.
46 Organisations- oder Unternehmensrichtlinien umfassen alle Vorgaben, um die strategischen Unternehmensziele zu erfüllen.

Datenräume als Oberklasse und dann für vertrauenswürdige als Unterklasse. Aufgrund der Transitivität gilt der Verlust an Raumeigenschaften also sowohl für Räume an sich als auch für vertrauenswürdige Datenräume.

Der Datenaustausch findet statt:

- Bidirektional zwischen vertrauenswürdigen Datenräumen
- Monodirektional von einem vertrauenswürdigen Datenraum zu einem nichtvertrauenswürdigen Datenraum
- Monodirektional von einem nichtvertrauenswürdigen Datenraum zu einem vertrauenswürdigen Datenraum.

In allen Fällen werden die Daten in einem zwischen Datenräumen verbindlichen Format bereitgestellt, in eine für den physischen Datentransport über den Übermittlungskanal geeignete Form umgewandelt und dann verschickt. Die von der Senke (Sender) gelieferten Daten werden bei der Quelle (Empfänger) passend umgewandelt und dann in den Datenraum eingeliefert.

Im dritten Fall werden Daten aus einem nichtvertrauenswürdigen Datenraum bei der Einlieferung geprüft. Nur wenn die Qualitätssicherung erfolgreich ist, dürfen die Daten in den vertrauenswürdigen Datenraum integriert werden.

Zum Datenaustausch muss ein Datenraum *Export- und Import-Operationen* anbieten, sowohl für punktuelle Lieferungen als auch für Massenladungen und -entladungen (engl. bulk load, dump). Bei den Export-Operationen verlassen die Daten den vertrauenswürdigen Datenraum. Unabhängig davon, ob die Senke vertrauenswürdig ist oder nicht, sind die sich auf dem Übermittlungsweg befindenden Daten an sich nicht mehr vertrauenswürdig. Die Betreiber*in kann nicht mit hundertprozentiger Sicherheit gewährleisten, dass die Daten nach Grenzübergang und bei der Übermittlung die Prinzipien vertrauenswürdiger Datenräume erfüllen. Sie muss also beim Datenaustausch von ihren Sorgfaltspflichten entbunden werden, da sie nicht mehr mit Sicherheit garantieren kann, dass die Vertrauenswürdigkeit der Daten nicht verletzt wird. Durch geeignete technische Massnahmen kann zwar die Sicherheit und somit der Erfüllungsgrad der Prinzipien erhöht werden, totales Vertrauen ist aber nicht möglich. In diesem Sinn sind auch Daten, die zwischen vertrauenswürdigen Datenräumen ausgetauscht werden, nicht vertrauenswürdig an sich. Es gilt eine probabilistische Erfolgsquote als Mass zur Einhaltung der Datenraumprinzipien.

5.3 Modellstruktur

5.3.1 Kernmodell

Die Definitionen im vorangehenden Kapitel dienen dem logischen Aufbau eines Modells für vertrauenswürdige Datenräume.

Dieses Kernmodell, sowie die Erweiterung über die Umsetzungsmechanismen für Prinzipien fassen zusammen und zeigen in standardisierter grafischer Notation (UML) die Entitäten beider Modelle und ihre Zusammenhänge.

Das untenstehende Diagramm[47] zeigt die Struktur dieses Modells als Gesamtheit seiner Elemente und deren Beziehungen.

Bedeutung der Farbcodierungen:

- Gelb: Kernbegriffe des Datenraums
- Hellgrün: Architekturelemente

47 Die zwei in grafischer Notation abgebildeten Modelle (Abb. 3 und 4) sind in der Standardnotation UML (Unified Modeling Notation, Version 2.5, Diagrammart "class diagram") erfasst. Die Rechtecke sind Symbole für Konzepte, also Entitäten im Sinne einer Ontologie. Die Beziehungen (Assoziationen) zwischen ihnen sind durch durchgehende Linien dargestellt. Eine Struktur der Art <Entität A> <Beziehung> <Entität B> ist eine logische Aussage über den Zusammenhang zwischen zwei Konzepten. Diese kann auch als funktionale Verknüpfung der Art <Beziehung>(<Entität A>, <Entität B>) betrachtet werden. Die nummerischen Angaben nahe den Entitäten bei den Assoziationslinien geben die Anzahl der betroffenen Entitäten an (Kardinalität, Multiplizität): genau 1 (kann weggelassen werden), 1..* eine oder mehrere, 0..* keine oder mehrere (Kurzform: *), 0..1 keine oder genau eine (Optionalität).

- Grau: Gesellschaftliche Elemente
- Hellblau: Juristische Elemente
- Violett: Klassifikatorische Elemente
- Rosa: Organisatorische Elemente.

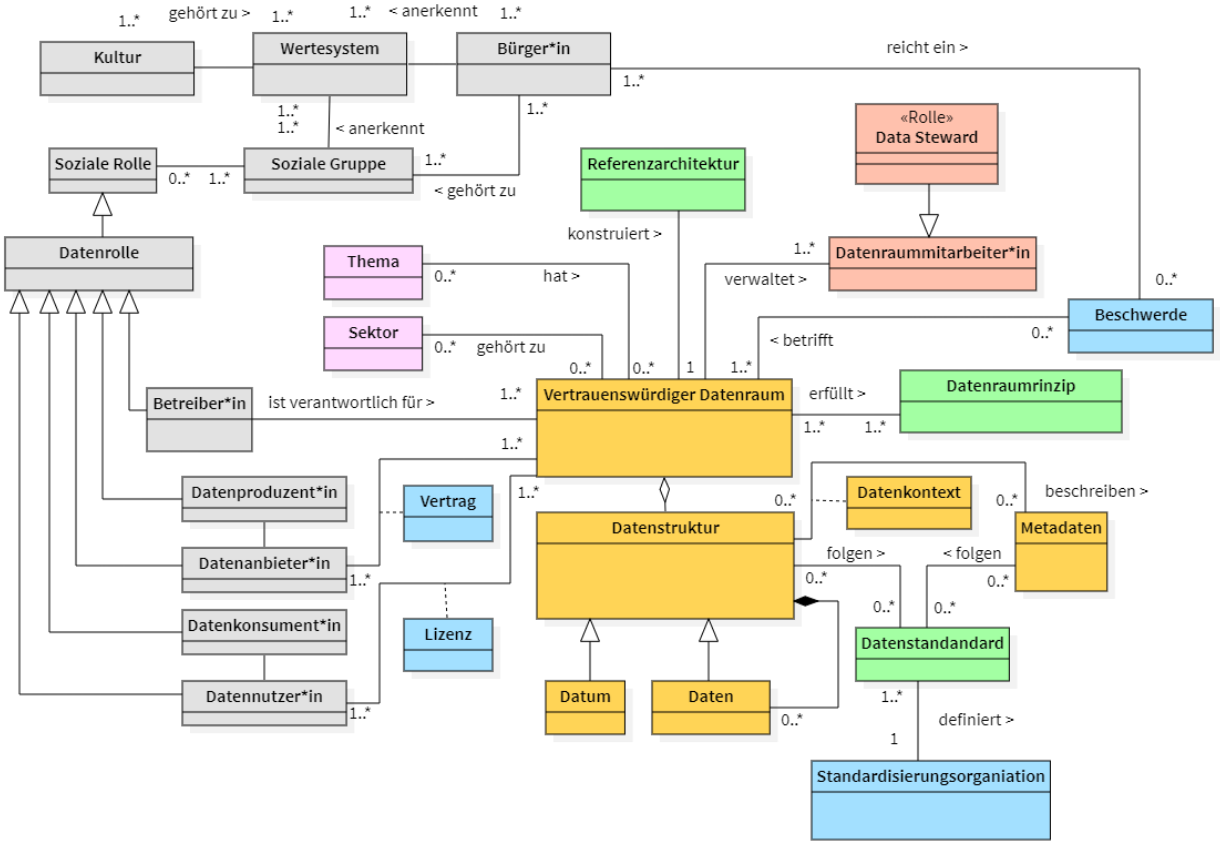

Abbildung 3 Struktur des Kernmodells (Diagramm)

5.3.2 Architektur vertrauenswürdiger Datenräume

Die IDSA (International Data Spaces Association, International Data Spaces | The future of the data economy is here) hat mehrere Studien zum Thema "Datenräume" veröffentlicht.

Das Dokument "Perspectives of the Reference Architecture Model"[48] zeigt Grundlagen und Aufbau des RAM-Architekturmodells. Im Gegensatz zur vorliegenden Arbeit, welche ein Wissensmodell des vertrauenswürdigen Datenraums zeigt, handelt es sich im RAM um eine vollständige Architektur, in deren Rahmen sich auch ein Domänenmodell befindet.

RAM baut auf einer *Architektur* in fünf *Schichten* (engl. layers) auf, die die Struktur von Datenräumen abbilden:

- Business
- Functional
- Process
- Information
- System.

48 Dazu siehe https://internationaldataspaces.org/publications/ids-ram/.

Orthogonal dazu legt dieses Modell drei *Sichten* (engl. view) fest:

- Security
- Certification
- Governance.

In Zusammenhang mit dieser Studie ist die Informationsschicht von zentraler Bedeutung. Die besprochenen Begriffe sowie das gesamte Wissensmodell dieser Studie widerspiegeln ein konzeptionelles Modell gemäss der Definition von IDS RAM (2019:11).

Zentrale Begriffe in diesem Modell sind:

- Data Owner (hier: Datenbesitzer*in)
- Data Provider (hier: Datenanbieter*in)
- Data Consumer (hier: Datenkonsument*in)
- Data User (hier: Datennutzer*in)
- Service Provider (hier: Datenraumbetreiber*in)
- Vocabulary Provider.

Wie aus dieser Liste ersichtlich, stimmen die von IDS RAM angegebenen Rollen mit denen in der vorliegenden Arbeit überein. Dadurch, dass die IDS-Architektur den Einsatz von Ontologien zur Beschreibung von in Datenräumen bereitgestellten Daten befürwortet, wird die Rolle der *Metadatenautorität* (engl. vocabulary provider) besonders hervorgehoben. Eine solche Stelle hat die Aufgabe, für Datenangebot und -austausch massgebende Definitionen und Metadaten als Vokabulare im Sinn einer Ontologie festzulegen und zu verwalten (IDS RAM, 2019:24 und 31). Es handelt sich um eine Standardisierungs- und Normenorganisation (wie z.B. ISO und DIN), deren Aufgabe darin besteht, Standards für Metadaten zu definieren und zu dokumentieren. Die Datenrollen sind angehalten, sich an diese Standards zu halten, um Qualität und Transparenz der Daten sicherzustellen.

Der Unterschied des Modells dieser Studie zu demjenigen von IDS RAM besteht darin, dass Letzteres die Architektur unterstützt und ein konzeptionelles Modell zum Datenaustausch als Bestandteil der Informationsschicht definiert. Das hier vorgeschlagene Modell stellt dagegen eine datenorientierte Sicht ins Zentrum. Beide Modelle sind aber untereinander kompatibel und ergänzen sich gegenseitig.

IDS RAM verwendet zur konzeptionellen Darstellung (engl. conceptual representation) den zentralen Begriff der *Ressource* (engl. digital resource). In Zusammenhang mit Datenräumen handelt es sich um das, was in der vorliegenden Studie als (digitale) Daten mit eindeutiger Kennung, festgelegtem Typ und dazugehörigem Wert definiert ist. IDS interpretiert sie als "commodity", d.h. als wirtschaftliches Gut, welches unter Teilnehmer*innen gehandelt und ausgetauscht wird. Instanzen solcher Güter befinden sich gemäss der Beschreibung dieser Studie als Daten in vertrauenswürdigen Datenräumen.

Die in IDS RAM betonten Vorteile von Ontologien zur Beschreibung und Festlegung von Daten und Metadaten sind auch im Sinn dieser Studie zu bestätigen. Neben der Nutzung von IDS RAM als Referenzarchitektur für vertrauenswürdige Datenräume, wird deshalb empfohlen, Standards im Bereich semantischer Technologien[49] gemäss Definitionen des W3-Konsortiums[50] zu verwenden. Damit ist es möglich, auf der Basis anerkannter Standards Daten und Metadaten der vertrauenswürdigen Datenräume zu modellieren.

5.3.3 Umsetzung der Prinzipien vertrauenswürdiger Datenräume

Vertrauenswürdige Datenräume entstehen aus allgemeinen Datenräumen, weil Prinzipien umgesetzt werden, die die Vertrauenswürdigkeit sichern. Dazu sind Handlungen notwendig, welche eine bestimmte Organisation als verantwortliche Instanz durchführt, um einen vertrauenswürdigen Datenraum zu erzeugen.

49 Insbesondere RDF, RFD/S, OWL, SHACL, SPARQL mit Turtle, RDF/XML und RDFa.
50 Dazu siehe https://www.w3.org/standards/semanticweb/.

Wegen des Abstraktionsgrads der Prinzipien, können Handlungen nicht direkt darauf angewendet werden. Es ist zuerst nötig, eine *Operationalisierung* durchzuführen. Damit können Prinzipien in benannte, prüfbare Eigenschaften (Attribute als Qualitäten) heruntergebrochen werden. Es entsteht eine hierarchische Struktur, die als Qualitätsbaum die innere Struktur der Prinzipien abbildet. Prüfbare Eigenschaften sind durch politische, juristische, technische oder soziale Massnahmen wie Verträge, Lizenzen, Gesetze, Standards, Normen, Konventionen, Gruppenmeinungen gesichert.

Die Handlungen, deren Umfang und Mächtigkeit im Voraus festgelegt ist, werden auf die Eigenschaften der Prinzipien angewendet. Für jede Eigenschaft wird eine Skala festgelegt, die den aktuellen Wert der betroffenen Eigenschaft prüft, nachdem die entsprechende Handlung angewendet wird. Die Prüfung ist ein Vergleich zwischen einem erwarteten Wert und dem nach der Durchführung erhaltenen Wert. Stimmen beide Werte überein (je nach Skala entweder vollständig oder innerhalb einer Toleranzgrenze), ist die Handlung erfolgreich durchgeführt worden.

Die Resultate, welche im Zusammenspiel aller Ergebnisse der durchgeführten Handlungen entstehen, führen zu einem vertrauenswürdigen Datenraum.

Bürger*innen üben während einer oder mehrerer Zeitspannen Datenrollen aus. Sie haben in diesen Rollen eine Erwartungshaltung in Bezug auf die vom Datenraum zu erfüllenden Prinzipien. Sie prüfen in einer oder mehreren Datenrollen anhand festgelegter Prüfverfahren, ob die Eigenschaften einen Wert ausweisen, der mit ihren Erwartungshaltungen übereinstimmt. Ist der Vergleich positiv, d.h. der Grad an Übereinstimmung ist positiv und signifikant, gilt die Eigenschaft als bestätigt. Die Summe aller Bestätigungen für alle Eigenschaften aller Prinzipien ist ein Mass für die Vertrauenswürdigkeit des untersuchten Datenraums aus Sicht der beteiligten Bürger*innen.

Damit wird empirisch bewiesen, dass der Datenraum als vertrauenswürdig betrachtet werden kann. Diese Kennzahl kann im Sinn eines Ranges verwendet werden, um Datenräume nach absteigender Vertrauenswürdigkeit zu klassifizieren (engl. ranking).

Der Vergleich zwischen den Werten aus den Handlungsresultaten und den Werten aus der Bestätigung ergibt einen Wert, den man als Mass der Übereinstimmung zwischen der organisatorischen Seite, welche für die Handlungsdurchführung zuständig ist, und der Bevölkerung als Nutzerin der vertrauenswürdigen Datenräume verstehen kann.

Das untenstehende Diagramm[51] zeigt die Mechanismen zur Erzeugung von vertrauenswürdigen Datenräumen.

Bedeutung der Farbcodierungen:

- Gelb: Kernbegriffe des Datenraums
- Hellgrün: Architekturelemente
- Hellblau: Juristische Elemente
- Weiss: Mechanismen zur Umsetzung der Prinzipien.

51 Verwendete Notation: UML Version 2.5, Diagrammart "class diagram". Für weitere Hinweise zur Notation vgl. Fussnote zu Abb. 3 in Kap. 5.3.1.

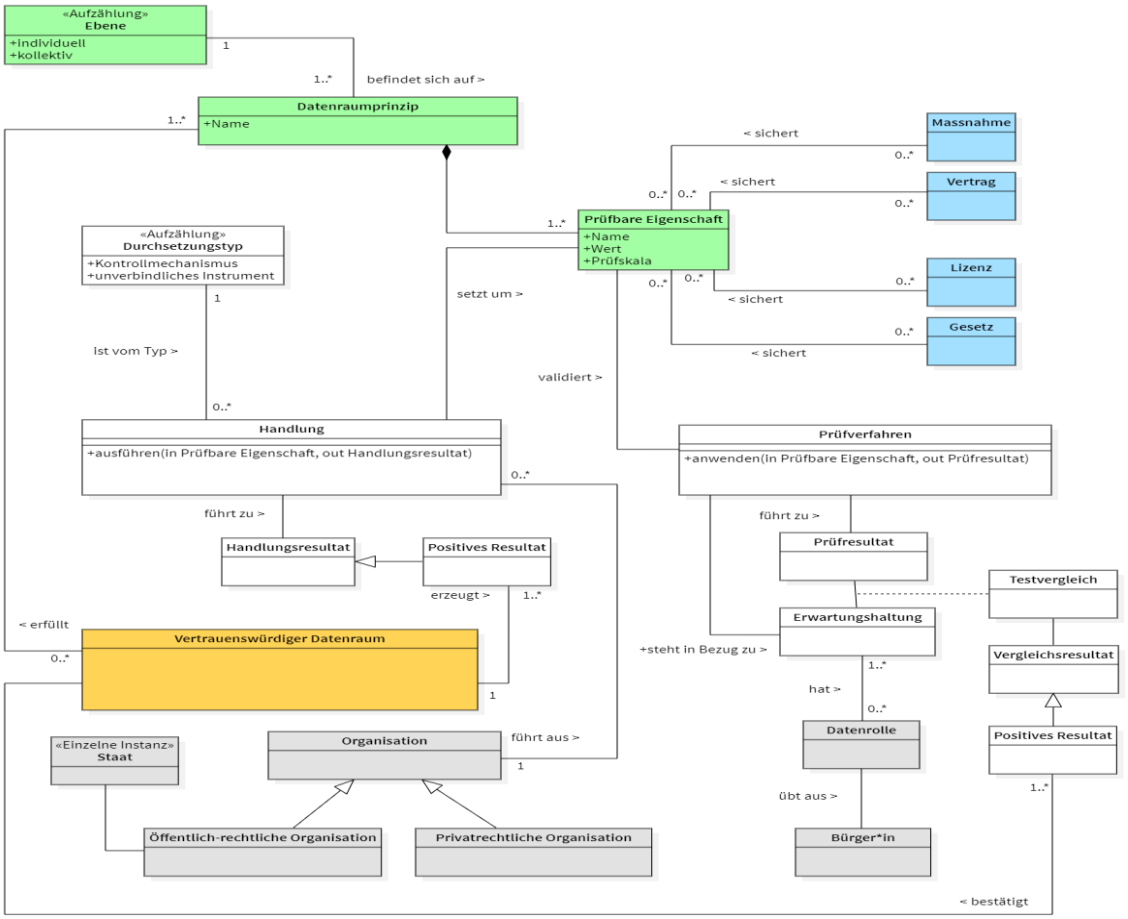

Abbildung 4 Mechanismen zur Erzeugung von vertrauenswürdigen Datenräumen (Diagramm)

5.4 Datenzyklus bei vertrauenswürdigen Datenräumen

Als "Datenzyklus" bezeichnet man den Werdegang der Daten von ihrer Entstehung über die Abgabe in den Datenraum bis zum Konsum nach Veröffentlichung und der möglichen Entfernung (Archivierung oder Löschung) (vgl. auch Kap. 2.1). In diesem Sinn handelt es sich um einen Lebenslauf auf der Zeitachse. Das Wort "Zyklus" deutet auf eine zeitliche Wiederholung hin, die es eigentlich nicht gibt[52]. Es handelt sich vielmehr um eine zeitliche Abfolge von Zuständen in den Daten, wobei ein Zustand mit einer oder mehreren (wertverändernden oder nicht) Operationen verbunden ist. Nach deren Ausführung treten die Daten durch Zustandsübergänge in einen anderen Zustand über. Es wäre also zwecks Vermeidung von Mehrdeutigkeiten empfehlenswert, von einem *zustandsbehafteten Lebenslauf der Daten* (engl. stateful life sequence) zu sprechen.

Das untenstehende Diagramm[53] zeigt alle möglichen Zustände und die zulässigen Zustandsübergänge:

52 Dazu siehe www.duden.de/rechtschreibung/Zyklus
53 Notation: UML Version 1.5, Diagrammtyp "state diagram" (https://www.uml.org/).

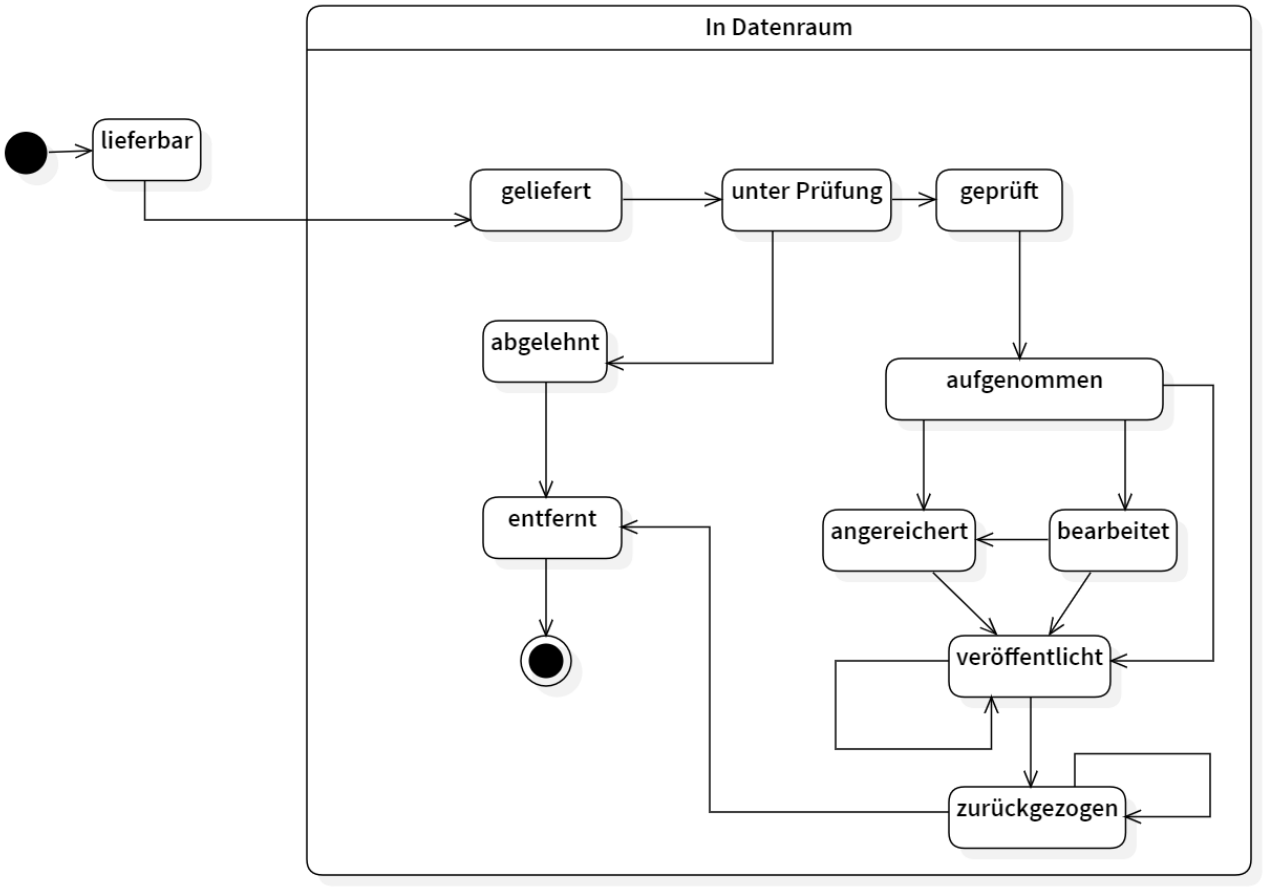

Abbildung 5 Mögliche Datenzustände und zulässige Zustandsübergänge (Diagramm)

Wenn die Anbieter*in bereit ist, ihre Daten zu liefern, muss sie zuerst einen geeigneten Datenraum finden. Anschliessend nimmt sie die von der Betreiber*in gestellten Bedingungen an[54] und liefert die Daten ab. Als Folge dieser physischen Abgabe befinden sich die Daten im Datenraum. Um die Prinzipien eines vertrauenswürdigen Datenraums erfüllen zu können, prüft die Betreiber*in die Daten auf Form und Inhalt. Um Transparenz und Reproduzierbarkeit zu gewährleisten, finden die Prüfungen vollautomatisch und regelbasiert statt. Die Automatisierung verfolgt das Ziel, möglichst objektive, beliebig wiederholbare und in allen Schritten nachvollziehbare Prüfungen durchzuführen. Zwar ist die Definition der Prüfregeln eine subjektive Handlung, auch wenn diese Subjektivität durch die Anwendung von Standards und Normen zum Teil entschärft werden kann. Aufgrund der Entscheidungen einer anerkannten Expertengruppe kann aber die Subjektivität der einzelnen Entscheidungen in eine anerkannte, dokumentierte Intersubjektivität umgewandelt werden. Diese stellt den Zwischenzustand zwischen vollständiger Subjektivität und idealer Objektivität. Es liegt in der Natur automatischer Verfahren, dass das ihnen zugrundeliegende Wissen in maschinenlesbarer Form mittels formaler Notation festgehalten wird. Unmittelbare Folge davon ist die Tatsache, dass Prüfverfahren und -regeln dokumentiert sind. Somit ist die Transparenz solcher Automatismen sichergestellt.

Ist die Kontrolle erfolgreich, werden die Daten endgültig aufgenommen. Je nach Qualitätsansprüchen können sie auch zusätzlich bearbeitet werden (engl. preprocessing). Auch hier finden im Sinn von Transparenz und Wiederholbarkeit die Bearbeitungsschritte vollautomatisch statt.

Um ihren Wert zu erhöhen, können die gelieferten Daten durch *Metadaten* ergänzt werden. Bei dieser Anreicherung können Markierungen (engl. tags), Vermerke (engl. annotations), Verweise (engl. links) und Codierungen hinzugefügt werden. Die Vorgänge der (Vor-)Verarbeitung und der Anreicherung sind im

54 Annahme der AGB, Vertragsunterzeichung mit digitaler Unterschrift, Annahme ohne rechtsverbindliche Unterschrift).

Rahmen einer *LOD-Strategie*[55] besonders wichtig. Die gelieferten Daten sind wertvoller, wenn sie in offenen[56], menschen- und maschinenlesbaren Formaten vorliegen und mit anderen Daten in formal definierten Beziehungen (engl. links) stehen. Ontologien[57] auf der Basis semantischer Tripeln[58] bieten geeignete Grundlagen für *wissensbasierte Datenräume*. Diese überwinden die auf Aufbewahrung und Darbietung gerichtete Funktionalität von anderen Datenräumen und erlauben den Sprung zu Wissenssystemen.

Durch die Veröffentlichung stehen die Daten zur weiteren Verwendung bereit. Konsument*innen können sie beziehen und im Rahmen der gegebenen Vereinbarungen nutzen. Somit wird der vertrauenswürdige Datenraum zu einer Datenplattform für den Austausch von Daten. Er erfüllt die Funktion eines virtuellen (Daten-)Marktes in der Datenökonomie.

Zum Lebenslauf der Daten gehört auch die ständige Pflege. Nur damit kann die Datenqualität gesichert und womöglich gesteigert werden. Ist die Aktualität der veröffentlichten Daten in Bezug auf einer gegebenen Zeitspanne nicht mehr gegeben oder erweisen sie sich als unzuverlässig, werden sie zuerst zurückgezogen. Anschliessend entscheiden Expert*innen, ob die Daten mittels Archivierung weiterhin aufbewahrt werden oder ob sie aus dem Angebot und somit von der Datenplattform endgültig entfernt werden.

5.5 Fazit

Auf der Basis der bestehenden Literatur ist es möglich, ein Modell eines vertrauenswürdigen Datenraums zu definieren. Die Schwierigkeit besteht darin, sich auf nicht allgemein anerkannten, zum grössten Teil nicht genau definierten Begriffen abstützen zu müssen. In diesem Sinn und auch wegen der Notwendigkeit, bei der Modellkonstruktion einen bestimmten Standpunkt annehmen zu müssen, ist das hier vorgestellte Modell als Vorschlag zu verstehen.

Ein wichtiger Punkt ist die Zerlegung der Prinzipien vertrauenswürdiger Datenräume in einzelne prüfbare Eigenschaften. Die Definition solcher Attribute und die Aufstellung von Prüfskalen muss angegangen werden, weil zurzeit kein für praktische Zwecke brauchbarer Eigenschaftskatalog vorhanden ist. Nach einer solchen vertieften Analyse sind die Handlungen (aufseiten der Betreiber*innen) und die Prüfverfahren (aufseiten der Nutzer*innen) festzulegen und im Detail zu dokumentieren. Erst wenn diese Elemente und ihr Zusammenspiel als Rahmenwerk vorhanden sind, kann die Erstellung eines vertrauenswürdigen Datenraums im Rahmen eines systematischen Konstruktionsverfahrens behandelt werden.

In Kap. 4.4. wurde betont, dass die Bestandesaufnahme der Umsetzung vertrauenswürdiger Datenräume in der Praxis eine Herausforderung darstellt. Erst eine breite Diskussion und Anwendung des vorgeschlagenen Modells in realen Fällen werden zeigen, ob dieses die Realität vertrauenswürdiger Datenräume passend abbildet.

55 LOD ist Akronym für "Linked and Open Data".
56 Hier im Gegensatz zu "proprietär", also Formate, die von einer Firma allein definiert sind und von denen auch keine oder eine unvollständigen Dokumentation vorhanden ist. Ein Beispiel dazu ist das RTF-Format für Dokumente der Firma Microsoft™.
57 Hier im Sinn der Informatik (und nicht der Philosophie) zu verstehen. Dazu siehe Ontologie (Informatik) – Wikipedia
58 Siehe vorhergende Fussnote und URL dazu.

6 Schlussfolgerungen

Aufgrund der Publikationsdaten der konsultierten Literatur wird rasch ersichtlich, dass die Idee zur Schaffung vertrauenswürdiger Datenräume als Alternative zur wiederholten individuellen «informierten Einwilligung» in den letzten rund fünf Jahren auf starken Zuspruch gestossen ist. Wesentlich dazu beigetragen haben dürften die diversen Datenskandale der Big-Data-Ökonomie sowie die bisherigen Erfahrungen mit der DSGVO auf EU-Ebene. So konnte ein Grundkonsens reifen, dass für die Erreichung der beiden vorrangigen Policy-Ziele – die Ermöglichung der Nutzung von (persönlichen) Daten zwecks wirtschaftlicher Innovation einerseits und die aktivere Einbindung der Individuen zwecks digitaler Selbstbestimmung andererseits – ein neuer Ansatz gefragt ist, der sowohl die Stellung der einfachen Bürgerinnen und Bürger als auch diejenige von Unternehmen und Organisationen, die nicht zu den grossen Playern der Big-Data-Ökonomie zählen, deutlich verbessert und die Beseitigung der heute bestehenden Marktungleichgewichte zumindest in Aussicht stellt.

Aufgrund der Literaturübersicht tritt allerdings auch deutlich zutage, dass die Thematik sowohl auf einer begrifflichen Ebene als auch bezüglich der inhaltlichen Vorstellungen, was vertrauenswürdige Datenräume ausmachen, noch stark im Fluss ist. Beispielhaft kann hier die teils verwirrende Namensgebung und das Definitionswirrwarr der verschiedenen im Umfeld eines Datenraumes bestehenden Funktionen und Rollen genannt werden. Dies ist auch eine Folge davon, dass Datenräume zu unterschiedlichen Zwecken gegründet und betrieben werden, was auch deren Organisationsform tangiert.

Für die Konstruktion eines technischen Modells ergeben sich dadurch Schwierigkeiten, da sie auf anerkannte, präzise Begriffsdefinitionen angewiesen ist. Wo solche fehlen, müssen diese durch Annahmen ersetzt werden, weshalb das auf dieser Basis konstruierte Modell als ein Vorschlag verstanden werden muss, der sich unter anders formulierten Annahmen verändern kann.

Erschwerend kommt hinzu, dass sich der Aufbau vertrauenswürdiger Datenräume einerseits in einem globalen, mindestens aber europäischen Kontext abspielt, sofern sich der Teilnehmerkreis (d.h. Datenanbietende und -nachfragende) nicht von vornherein rein national eingrenzen lässt (was eher die Ausnahme darstellen dürfte). Die am Datenraum Beteiligten bzw. die verwalteten Daten weisen sehr rasch eine internationale Dimension auf, weshalb die zentrale Forderung der Interoperabilität nicht nur auf die Beziehung der Datenräume untereinander abzielt, sondern ebenso auf die Rechtsräume, in denen sich die Datenräume bewegen. Andererseits fallen die Ansprüche an die auszutauschenden Daten sektoriell sehr unterschiedlich aus, weshalb Top-down-Ansätze bzw. ein alle Situationen und Ansprüche befriedigendes Modell eines vertrauenswürdigen Datenraums nicht besteht. Die in diesem Bericht aufgezeigten Praxisbeispiele haben dies bestätigt.

Daraus folgt, dass selbst die im Bericht dargelegten Grundprinzipien und Voraussetzungen für vertrauenswürdige Datenräume immer in Relation zur Zweckbestimmung des jeweiligen Datenraums flexibel auszulegen sind. Auch hierzu gilt, dass nicht alle vertrauenswürdigen Datenräume exakt dieselben Merkmale aufweisen bzw. sämtliche Grundprinzipien auf dieselbe Art und Weise umsetzen müssen. Das Ziel der Vertrauenswürdigkeit ist mit unterschiedlicher Gewichtung der Mittel zu erreichen, die sich nach den sektorspezifischen Erfordernissen richten. Wichtig ist indes, dass die am Datenraum Teilnehmenden auf geeignete Weise darüber in Kenntnis gesetzt sind, nach welchen Prinzipien der Datenraum funktioniert und wie die Einhaltung der Prinzipien garantiert wird.

Für den Erfolg vertrauenswürdiger Datenräume die grösste Herausforderung bildet insgesamt die Frage der richtigen Anreizstruktur: Diejenigen, welche Daten einbringen, müssen ebenso wie diejenigen, welche die Daten nutzen sollen, in den vertrauenswürdigen Datenräumen einen deutlichen Mehrwert gegenüber der aktuellen Situation erkennen. Dies erfordert, dass die Teilnahmebedingungen und die Governance-Struktur von vertrauenswürdigen Datenräumen die Erwartungen und Bedürfnisse aller Beteiligten befriedigen.

Der vorliegende Bericht hat aufzuzeigen versucht, in welchen Bereichen die zentralen Herausforderungen für die Schaffung vertrauenswürdiger Datenräume liegen, welche Voraussetzungen gegeben bzw. welche Grundprinzipien angewandt werden müssen, damit die erkannten Herausforderungen gemeistert werden können, welche vertrauenswürdigen Datenräume bereits existieren und wie sich deren Umsetzung gestaltet und schliesslich, welche Kernelemente ein Modell eines vertrauenswürdigen Datenraums aufweist.

Abbildungsverzeichnis

Tabellenverzeichnis

Glossar

Das Glossar besteht aus lediglich provisorischen Arbeitsdefinitionen, die anhand verschiedenster Quellen, die nachfolgend nicht einzeln kenntlich gemacht sind, erstellt wurden.

Begriff	**Definition**
Anonymisierung	Der Prozess, in dessen Verlauf Daten so verändert werden, dass sie sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen oder personenbezogene Daten, die so bearbeitet werden, dass die betroffene Person nicht oder nur mit einem unverhältnismässig grossen Aufwand oder mit gesetzlich verbotenen Mitteln identifiziert werden kann.
Big Data	Grosse Datensätze, die sich anhand der fünf "V" definieren (*Volume* (Umfang), *velocity* (Tempo der Generierung und Analyse), *variety* (Diversität bzgl. Quellen und Formaten), *veracity* (Vertrauen in Qualität und Korrektheit) und *value* (Wertsteigerung)) und zu deren Verarbeitung und Auswertung neue Methoden zur Anwendung gelangen.
Betroffene Personen	Natürliche Person, über die Personendaten bearbeitet werden (vgl. Art. 5 lit. b revDSG).
Cybersicherheit	Schutz vor unerlaubten technischen Zugriffen im digitalen Raum (Cyberangriffe).
Data Trust (Datentreuhand-Modell)	Eine Datentreuhandstelle kann mit der Aufgabe betraut sein, einen standardisierten Zugang zu *Daten* für zugelassene Stellen zu entwickeln und umzusetzen. Zudem besitzen Datentreuhänder eine Beratungsfunktion gegenüber ihren Nutzerinnen und Nutzern und bieten je nach Spezialisierung verschiedene Dienste, wie beispielsweise die Verwaltung von Daten im Sinne der Nutzerinnen und Nutzer. Datentreuhänder können aber auch datenschutzrechtliche Interessen und Gestaltungsrechte für eine Vielzahl von Verbraucherinnen und Verbrauchern geltend machen.

Datenökonomie	Wertschöpfung aufgrund der Nutzung von Daten bzw. von Big Data
Datenportabilität	Herausgabe an die betroffene Person ihrer persönlichen Daten in einem gängigen elektronischen Format oder deren Übertragung an eine Dritte natürliche oder juristische Person. Grundsätzlich kostenlos, ausser namentlich bei unverhältnismässig hohem Aufwand (vgl. Art. 28 neues DSG).
Datenraum	Technische und organisatorische Struktur, welche Bereitstellung, Austausch und Bezug von Daten aus verschiedenen Quellen und von verschiedenen Akteuren ermöglicht und regelt. Oftmals sektorenspezifisch organisiert und durch Zweck, klare Regeln und Standards definiert.
Datenzyklus	Lebenszyklus von Daten; von ihrer Verfügbarkeit, Zugänglichkeit über die Bearbeitung, bis zum Austausch und der Wiederverwendung.
De-Anonymisierung	Rückgängigmachen einer vorgängigen Anonymisierung bzw. ein mit hoher Wahrscheinlichkeit erfolgreiches Kenntlichmachen des Personenbezugs (mithilfe von Big-Data-Analysemethoden).
Dezentraler Datenraum	Konzept von mehreren, gleichberechtigten Datenräumen, die sich untereinander austauschen können, anstelle einer alleinigen Datenplattform.
Differential Privacy	Unkenntlichkeit der Identität der beteiligten Peron, wobei ein Rückschluss auf die Person auch mit Drittdaten nur mit einer gewissen, definierten Wahrscheinlichkeit möglich ist.
Digitale Selbstbestimmung	Möglichkeit für Akteure (insb. natürliche Personen, aber auch juristische Personen und öffentliche Einrichtungen) eigene Handlungsentscheidungen im digitalen Raum zu realisieren.
Geschlossenes Ökosystem (walled garden)	Systeme bzw. Plattformen, deren Nutzung mit Restriktionen versehen ist und die keine Interoperabilität mit anderen Systemen aufweisen.
Informationelle Selbstbestimmung	Recht und/oder die Möglichkeit und Fähigkeit einer Person, grundsätzlich selber über Preisgabe, Sammlung und Verwendung personenbezogener Informationen/Daten zu bestimmen sowie Kontrolle über ihr „digitales Double“ zu haben.
Informierte Einwilligung (informed consent)	Einwilligung einer betroffenen Person zur Verarbeitung ihrer personenbezogenen Daten nach zuvor vollständiger, klarer und sachlich richtiger Information durch den Datenverarbeiter.
Interoperabilität	Fähigkeit zur Zusammenarbeit verschiedener Systeme, Techniken oder Organisationen, in der Regel auf Basis gemeinsamer Standards. Vertriebssysteme sind beispielsweise dann interoperabel, wenn sie über standardisierte Schnittstellen so miteinander verknüpft werden können, dass es möglich ist, über ein Vertriebssystem Produkte aus anderen, kooperierenden Vertriebssystemen zu erwerben.
Lock-in-Effekt	Abhängigkeitsverhältnis von einem Kunden zu einem Anbieter, z.B. wenn ein Anbieterwechsel durch hohe Wechselkosten faktisch verunmöglicht wird.
Netzwerkeffekt	Nutzen eines Gutes nimmt mit steigender Nutzerzahl überproportional zu bzw. eine sinnvolle Nutzung ergibt sich erst bei grosser Nutzerzahl.
Once-Only-Prinzip	Zur Reduktion von Verwaltungsaufwand und Bürokratie sollen Bürger*innen und Unternehmen den staatlichen Stellen ihre Informationen nur noch einmal

	mitteilen müssen. Die staatlichen Stellen sind ihrerseits zur Wiederverwendung und Austausch der Daten berechtigt.
Open Data	Frei zugängliche und für jegliche Zwecke (auch kommerzielle) weiterverwendbare Daten, die auch verändert und an Dritte weitergegeben werden können. Diese Daten werden kostenlos oder zu Grenzkosten zur Verfügung gestellt.
Open Government Data	Verwaltungsdaten, die von der öffentlichen Hand als Open Data bereitgestellt werden.
Persönliche Daten	Gesamtheit der personenbezogenen und personenbeziehbaren Daten
Personendaten/ personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
Personendaten, besonders schützenswert	Besonders schützenswert sind Personendaten, bei denen eine besondere Gefahr der Persönlichkeitsverletzung besteht, z.B. Gesundheitsdaten. Eine rechtliche Definition findet sich in Art. 3 lit. c DSG.
(Digitale) Plattformen	Bestimmtes Nutzungsmodell; ein einziges Unternehmen sammelt, verknüpft und analysiert «in house» die Daten, welche über eine (meistens globale) digitale Plattform generiert werden, um daraus Dienstleistungen an verschiedene Kunden auf verschiedenen Märkten anzubieten; Dienstleistungen bauen auf dem Sammeln und Analysieren von Daten auf allen drei Märkten auf. Die Plattformen stellen i.d.R. geschlossene Daten-Ökosysteme dar.
Plattformökonomie	Datenökonomie am Beispiel geschlossener Daten-Ökosysteme
Pseudonymisierung	Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Massnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Ein Beispiel ist das Ersetzen von Namen durch ID-Nummern und das Auslagern einer Zuordnungstabelle von Namen und Nummern.
Public Value	Wertschöpfung für die Öffentlichkeit bzw. die Allgemeinheit
Stakeholder	Gesamtheit der Anspruchsgruppen bzgl. eines Unternehmens. Im Kontext von Datenräumen insbesondere alle datengebenden und datennutzenden Entitäten.
Unraveling-Prozess	Verhalten, bei dem die Preisgabe persönlicher Daten aus ökonomischem Eigeninteresse erfolgt, wodurch andere Beteiligte in Zugzwang versetzt werden.

Literaturverzeichnis

AI HLEG. (2020a). *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*. EU High-Level Expert Group on Artificial Intelligence (AI HLEG).

AI HLEG. (2020b). *Ethics guidelines for trustworthy AI*. EU High-Level Expert Group on Artificial Intelligence (AI HLEG).

Algorithm Watch. (2020). *Automating Society Report 2020*.

Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace*. https://www.eff.org/de/cyberspace-independence

BitsaboutMe. (2021). BitsaboutMe. *BitsaboutMe*. https://bitsabout.me/de/ueber-uns/

Blankertz, A. (2020). *Designing Data Trusts. Why We Need to Test Consumer Data Trusts Now*. Stiftung Neue Verantwortung e. V. https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_d.pdf

Bossmann, J., Smith, R., Gillen, M., & Reddy, S. (2018). Artificial Intelligence Ethics. In *Cyber ethics 4.0: Serving humanity with values* (S. 101–114).

Bostrom, N., & Yudkowsky, E. (2011). *The Ethics of Artificial Intelligence*. 20.

Bühlmann, M., Vatter, A., Dlabac, O., & Schaub, H.-P. (2013). Liberale Romandie, radikale Deutschschweiz? Kantonale Demokratien zwischen Repräsentation und Partizipation. *Swiss Political Science Review*, *19*(2), 157–188.

Bundesamt für Kommunikation BAKOM, Direktion für Völkerrecht DV, SATW, Swiss Data Alliance. (2020). *Digitale Selbstbestimmung*. Stand 16.10.2020.

Bundeskanzleramt. (2021). *Datenstrategie der Bundesregierung* (S. 122). Bundeskanzleramt. https://www.bundesregierung.de/resource/blob/992814/1845634/5bae389896531854c579069f9a699a8f/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1

Chambers, R. (1988). *Agriculture and Rural Problems. Sustainable Livelihoods, Environment and Development: Putting Poor Rural People First*. UNO.

Christen, M., Heitz, C., Kleiber, T., & Loi, M. (2020). *Ethik-Kodex für datenbasierte Wertschöpfung. Grundlagen.* (Data Innovation Alliance, Hrsg.).

Coase, R. H. (1937). The Nature of the Firm. *Economica*, *4*(16), 386–405. https://doi.org/10.1111/j.1468-0335.1937.tb00002.x

Data Critiques. (2019). *The Challenges of Data Custody & A Testable Plan for Data Trust*. https://www.datacritique.com/Data_Trust_RFC.pdf

Datenethikkommission der Bundesregierung. (2019). *Gutachten der Datenethikkommission*. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=5

Delacroix, S., & Lawrence, N. D. (2019). Bottom-up Data Trusts: Disturbing the „One Size Fits All" Approach to Data Governance. *International Data Privacy Law*, *9*(4), 236–252. https://doi.org/10.1093/idpl/ipz014

Dunleavy, P., & Margetts, H. (2015). *Design principles for essentially digital governance*. 111th Annual Meeting of the American Political Science Association.

EDA. (2020). *Strategie Digitalaussenpolitik 2021–2024*. Schweizerische Eidgenossenschaft.

Europäische Kommission. (2020a). *Eine europäische Datenstrategie*. Europäische Kommission. https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

Europäische Kommission. (2020b). *White Paper on Artificial Intelligence—A European approach to excellence and trust*.

Faust, D. (2021, Februar 24). *Was bedeutet Skalierung in der IT?* Biteno GmbH. https://www.biteno.com/was-ist-skalierung-in-der-it/

Goldstein, E., Gasser, U., & Budish, R. (2018). *Data Commons Version 1.0: A Framework to Build Toward AI for Good. A roadmap for data from the 2018 AI for Good Summit*. https://medium.com/berkman-klein-center/data-commons-version-1-0-a-framework-to-build-toward-ai-for-good-73414d7e72be

Hardinges, J. (2018, Oktober 19). Defining a „data trust". *Open Data Institute*. https://theodi.org/article/defining-a-data-trust/

Hardinges, J. (2020a, März 17). *Data Trusts in 2020*. https://theodi.org/article/data-trusts-in-2020

Hardinges, J. (2020b, Juni 8). *Patterns of data institution that interact with people and their rights over data*. Medium. https://medium.com/@jack.hardinges/patterns-of-data-institution-that-interact-with-people-and-their-rights-over-data-8b10279091c

Hardinges, J., Wells, P., Blandford, A., Tennison, J., & Scott, A. (2019). *Data Trusts: Lessons From Three Pilots*. Open Data Institute. https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit

Heuberger, A., Otto, B., & Waidner, M. (2021). *Daten—Rohstaoff für smarte Innovationen*. Fraunhofer-Gesellschaft. https://www.fraunhofer.de/de/forschung/aktuelles-aus-der-forschung/daten-rohstoff-fuer-smarte-innovationen.html

Heumann, S., & Jentzsch, N. (2019). *Wettbewerb um Daten. Über Datenpools zu Innovationen*. Stiftung Neue Verantwortung e. V. https://www.stiftung-nv.de/sites/default/files/wettbewerb_um_daten.pdf

Hürlimann, D. (2014). Das Google-Urteil des EuGH und die Entfernungspflicht von Suchmaschinen nach schweizerischem Recht. *sui generis*. https://doi.org/10.21257/sg.1

IDS RAM. (2019). Reference Architecture Model, Version 3.0, April 2019, IDS Ram | International Data Spaces , zuletzt besucht am 9.6.2021.

Jarchow, T., & Estermann, B. (2015). *Big Data: Chancen, Risiken und Handlungsbedarf des Bundes. Ergebnisse einer Studie im Auftrag des Bundesamts für Kommunikation*. Berner Fachhochschule. https://arbor.bfh.ch/9502/1/Jarchow_and_Estermann_2015_Big%20Data%20-%20Chancen%2C%20Risiken%20und%20Handlungsbedarf%20des%20Bundes.pdf

Jentzsch, N. (2017). *Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds: Ökonomische Rahmenbedingungen innovativer Lösungen zu Einwilligungen im Datenschutz* [Gutachten]. Deutsches Institut für Wirtschaftsforschung (DIW Berlin). https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Gutachten_Die_persoenliche_Datenoekonomie_Anhang_2_final.pdf

Lamla, J., & Ochs, C. (2019). Selbstbestimmungspraktiken in der Datenökonomie: Gesellschaftlicher Widerspruch oder ‚privates' Paradox? In B. Blättel-Mink & P. Kenning (Hrsg.), *Paradoxien des Verbraucherverhaltens* (S. 25–39). Springer Gabler.

Lange, S., & Santarius, T. (2018). *Smarte grüne Welt? Digitalisierung zwischen Überwachung, Konsum und Nachhaltigkeit*. oekom. https://www.oekom.de/buch/smarte-gruene-welt-9783962380205

Linder, W., & Mueller, S. (2017). *Schweizerische Demokratie: Institutionen – Prozesse – Perspektiven* (4. Auflage). Haupt.

Midata. (2021). MIDATA. https://www.midata.coop/

Mulgan, G., & Straub, V. (2019). *The new ecosystem of trust*. Nesta. https://www.nesta.org.uk/blog/new-ecosystem-trust/

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, *140*(4), 32–48.

O'Hara, K. (2019). *Data Trusts: Ethics, Architecture and Governance for Trustworthy Data Stewardship* [WSI White Paper #1]. Web Science Institute, University of Southampton. https://cdn.southampton.ac.uk/assets/imported/transforms/content-block/UsefulDownloads_Download/0326D18DCC9E4BD08816BB5F994FCA76/White%20Papers%20No1.pdf?_gl=1*ve56or*_ga*MjEyNDU0NjU0Ny4xNDk3NTMzNzk5*_ga_51YK64STMR*MTYwNTI3Mjc4Ni4xNjYuMS4xNjA1MjczODc4LjYw#_ga=2.3784242.343304628.1605180452-212454654

Open Data Institute. (o. J.). *Manifesto*. Abgerufen 3. Mai 2021, von https://theodi.org/about-the-odi/our-vision-and-manifesto/our-manifesto/

Open Data Institute. (2018, November 20). *UK's first 'data trust' pilots to be led by the ODI in partnership with central and local government*. https://theodi.org/article/uks-first-data-trust-pilots-to-be-led-by-the-odi-in-partnership-with-central-and-local-government/

Open Data Institute. (2019, Januar 31). *UK's first data trusts to tackle illegal wildlife trade and food waste*. https://theodi.org/article/uks-first-data-trusts-to-tackle-illegal-wildlife-trade-and-food-waste/

Picot, A., Berchtold, Y., & Neuburger, R. (2018). Big Data aus ökonomischer Sicht: Potenziale und Handlungsbedarf. In B. Kolany-Raiser, R. Heil, C. Orwat, & T. Hoeren (Hrsg.), *Big Data und Gesellschaft. Eine multidisziplinäre Annäherung* (S. 309–416). Springer VS.

Purtova, N. (2017). Do property rights in personal data make sense after the big data turn: Individual control and transparency. *Journal of Law and Economic Regulation*, *10*(2), 64–78.

Royal Academy of Engineering. (o. J.). *Towards trusted data sharing: Guidance and case studies*. Abgerufen 17. April 2021, von http://reports.raeng.org.uk/datasharing/cover/

SalusCoop. (2021). SalusCoop. https://www.saluscoop.org

Schieferdecker, I., Bruns, L., Cuno, S., Flügge, M., Isakovic, K., Klessmann, J., Lämmel, P., Stadtkewitz, D., Tcholtchev, N., Lange, C., Imbusch, B., Strauss, L., Vastag, A., Flocke, F., & Kraft, V. (2018). *Urbane Datenräume—Möglichkeiten von Datenaustausch und Zusammenarbeit im urbanen Raum*. Fraunhofer FOKUS.

Schneider, I. (2019). Governance der Datenökonomie – Politökonomische Verfügungsmodelle zwischen Markt, Staat, Gemeinschaft und Treuhand. In C. Ochs, M. Friedewald, T. Hess, & J. Lamla (Hrsg.), *Die Zukunft der Datenökonomie. Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz* (S. 143–180). Springer VS.

Schweizerische Eidgenossenschaft. (2020). *Strategie Digitale Schweiz*.

SharedStreets. (2020). *SharedStreets*. SharedStreets. https:/sharedstreets.io/

Sharing Cities. (2021). *Sharing Cities*. https://www.sharingcities.eu/sharingcities/city-profiles/london

Shiohira, K., & Dale-Jones, B. (2019). *Interoperable Data Ecosystems. An international review to inform a South African innovation*. 80.

Solidproject. (2021). Solidproject. https://solidproject.org/

Tranberg, P., Hasselbalch, G., Olsen, K., & Byrne, C. S. (2018). *Dataethics – Principles and Guidelines for Companies, Authorities & Organisations*. 38.

Wang, J. M. (2019). The Data Life Cycle. *Harvard Data Science Review*, *1*(1). https://doi.org/10.1162/99608f92.e26845b4

Weltbank. (2018). Better data for doing good: Responsible use of big data and artificial intelligence. *Information and communications for development*, *Data-driven development*(4), 33–50.

Wildlabs. (2021). *WILDLABS.NET*. WILDLABS.NET. https://www.wildlabs.net/

Williamson, O. E. (1985). *The economic institutions of capitalism: Firms, markets, relational contracting.* Free press.

WolframAlpha, (2021). Begriff "space" in: space - Wolfram|Alpha (wolframalpha.com), zuletzt besucht am 9.6.2021.

World Economic Forum. (2011). *Personal Data: The Emergence of a New Asset Class*.

World Economic Forum. (2019). *Data Collaboration for the Common Good: Enabling Trust and Innovation Through Public-Private Partnerships*. http://www3.weforum.org/docs/WEF_Data_Collaboration_for_the_Common_Good.pdf

WRAP. (2021). *WRAP*. https://wrap.org.uk/

Wylie, B., & McDonald, S. (2018, Oktober 9). What is a Data Trust? *Centre for International Governance Innovation*. https://www.cigionline.org/articles/what-data-trust

ZHAW. (2018). *«Soft Law» – Praktische Relevanz und rechtliche Bedeutung von Leitfäden und Co. 13*. https://doi.org/10.2903/j.efsa.2015.4104