Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Eidgenössisches Departement für auswärtige Angelegenheiten EDA Der Bundesrat

Bern, 30.03.2022

Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung

Bericht des UVEK und des EDA an den Bundesrat

Inhaltsverzeichnis

Executive Summary

Die Digitalisierung stellt die Gesellschaft vor viele Herausforderungen und insbesondere vor die Frage, wie eine nachhaltige Datengesellschaft aufgebaut werden kann. Wenn Daten besser genutzt werden, können in vielen Bereichen unserer Gesellschaft und Wirtschaft Bedürfnisse gezielter befriedigt, Innovation gefördert sowie Ressourcen effizienter und nachhaltiger genutzt werden. So ermöglichen Daten beispielsweise neue Diagnosemöglichkeiten in der Medizin[1] oder bessere Erkenntnisse über Düngungsmuster in der Landwirtschaft[2]. Gleichzeitig haben aber viele Menschen Angst davor, durch eine verstärkte Datennutzung die Kontrolle über ihre persönlichen Daten zu verlieren.

Die zentrale Frage lautet nun: Wie kann das Potential von Daten für Gesellschaft und Wirtschaft besser realisiert werden? Drei Tendenzen illustrieren warum das Potenzial der Datennutzung noch nicht ausgeschöpft wird: Erstens sind Daten in immer mehr Sektoren bei einigen wenigen Akteuren konzentriert. Diese Akteure können die Daten für Innovation und ihre eigene Effizienzsteigerung nutzen, haben aber keinen Anreiz ihre Daten mit weiteren Akteuren zu teilen. Zweitens können oder wollen viele private oder öffentliche Dienstanbieter das Datenpotenzial nicht nutzen, sei es aus fehlendem Know-how oder fehlenden Ressourcen, sei es aus Befürchtungen einer Schwächung ihrer aktuellen Position oder wegen administrativen, technischen oder rechtlichen Hürden. Drittens, lässt sich bei einem wachsenden Anteil der Bevölkerung ein Misstrauen gegenüber der Nutzung von Daten feststellen. Gründe dafür sind die Angst vor Manipulation, vor Missbrauch und Verlust der Privatsphäre, oder das Fehlen von Anreizen für eine gemeinsame Datennutzung (siehe Kapitel 2).

Diese Entwicklungen werden sich ohne Gegenmassnahmen voraussichtlich akzentuieren und immer mehr Bereiche unserer Gesellschaft betreffen. In einer nachhaltigen Datengesellschaft soll jedoch nicht zwischen Schutz und Kontrolle der eigenen Daten und den Vorteilen der Datennutzung gewählt werden müssen; vielmehr soll mit dem Ansatz der digitalen Selbstbestimmung beides ermöglicht werden: Individuen, Unternehmen und die Gesellschaft als Ganzes sollen über ihr Handeln im digitalen Raum selbst bestimmen können. Dies beinhaltet die Fähigkeit der Nutzerinnen und Nutzer, Relevanz und Wert der für sie wesentlichen Daten einordnen zu können sowie den Zugang zu und Kontrolle über diese Daten zu haben und schliesslich über deren Verwendung bestimmen zu können (siehe Kapitel 3).

Um diese Kontrolle zu gewährleisten und gleichzeitig das Teilen und Nutzen von Daten zu fördern, braucht es *vertrauenswürdige Datenräume*. Diese bilden eine besondere Kategorie von Datenräumen. Denn sie zeichnen sich dadurch aus, dass die Teilnehmenden in einem solchen Datenraum ihre Daten nach eigenem Willen und mit der nötigen Kontrolle zur Verfügung stellen und so die Daten für wirtschaftliche und gesellschaftliche Zwecke genutzt werden können. Damit solche vertrauenswürdigen Datenräume entstehen, braucht es bestimmte Grundanforderungen, die eingehalten werden müssen. Der Bericht schlägt dafür fünf Grundprinzipien vor: Transparenz, Kontrolle, Fairness, Verantwortlichkeit und Effizienz. Diese fünf Grundprinzipen und die dazugehörigen Indikatoren stellen den Kern der Antwort auf das Mandat des Bundesrates dar, nämlich aufzuzeigen, welche technischen, rechtlichen wirtschaftlichen und gesellschaftlichen Voraussetzungen für die Schaffung vertrauenswürdiger Datenräume gegeben sein müssen (siehe Kapitel 4).

In diversen Sektoren entwickeln sich in der Schweiz schon heute Datenräume. Die Datenraumprojekte Mobilität, Energie, Finanzen, Gesundheit und Bildung werden im Bericht als konkrete Anschauungsbeispiele auf dem Weg zur digitalen Selbstbestimmung dargestellt, und es wird aufgezeigt, wie diese als vertrauenswürdige Datenräume qualifiziert werden können (siehe Kapitel 5).

[1] *Bundesrat (2019)*, «Gesundheitspolitische Strategie des Bundesrates 2020-2030», S. 12.
[2] Siehe Agroscope Projekt *Smart Farming* <https://www.agroscope.admin.ch/agroscope/de/home/themen/wirtschaft-technik/smart-farming.html> (Zugriff am 03.02.2022), bspw. «Ortsspezfische N-Düngung».

Datenflüsse sind sehr oft transnational. In den letzten Jahren haben sich global unterschiedliche Auffassungen etabliert, wie Datenflüsse geregelt sein sollten. Dies führt zu einer verstärkten regulatorischen Fragmentierung und damit zunehmend zu Hindernissen im freien Datenfluss. Um das enorme Potenzial von internationalen Datenflüssen ausschöpfen zu können, müssen Datenräume sowohl in ihrer technischen Funktionsweise als auch in ihrer organisatorischen und normativen Ausgestaltung international kompatibel sein. Dafür braucht es Interoperabilität. Es gilt deshalb für die Schweiz, sich in internationalen und europäischen Gremien für die Festlegung von gemeinsamen Normen im Sinne der digitalen Selbstbestimmung einzusetzen. Längerfristig gilt es, Rechtssicherheit auf internationaler Ebene zu schaffen und der regulatorischen Fragmentierung entgegenzuwirken. Gerade für die Schweiz als mittlere und hochvernetzte Wirtschaftsnation ist dies wichtig und kann den Zugang zu internationalen Märkten sowie dem europäischen Binnenmarkt ermöglichen. Der Ansatz der digitalen Selbstbestimmung kann hier neue Möglichkeiten eröffnen. (siehe Kapitel 6).

Obwohl in diversen Bereichen Bestrebungen zur Ausarbeitung von aktuellen sektorübergreifenden Rahmenbedingungen laufen, sind diese zu intensivieren, um die Nutzung von Daten zu fördern, den Entwicklungstendenzen (wie bspw. Datenballungen) entgegenzuwirken und dabei gleichzeitig Transparenz, Vertrauen und zusätzliche Kontrolle für Nutzerinnen und Nutzer zu schaffen. Neu entstehende Datenräume werden richtungsweisend dafür sein, wie wir diese als Gesellschaft nutzen und den breit angelegten Austausch von Daten künftig betreiben. Auch in der Schweiz müssen deshalb entsprechende Rahmenbedingungen geschaffen werden. Der Bericht schlägt in einem ersten Schritt die nachstehenden Handlungsmassnahmen vor, um die Entstehung von vertrauenswürdigen Datenräumen auf Basis der digitalen Selbstbestimmung zu fördern (siehe Kapitel 7):

1. **Verhaltenskodex:** Die Entwicklung von Datenräumen steht in vielen Sektoren noch am Anfang, nimmt aber zunehmend Fahrt auf. Ein freiwilliger Verhaltenskodex soll erarbeitet werden und als Handlungsanleitung für die Entwicklung von vertrauenswürdigen Datenräumen gelten. Der Verhaltenskodex soll auf den Grundprinzipien dieses Berichts aufbauen, in einem Multistakeholder-Prozess auf Basis des Nationalen Netzwerks Digitale Selbstbestimmung erarbeitet und als koordinierter Selbstregulierungsansatz verstanden werden.
2. **Swiss Data Hub und Interoperabilität**: Auf europäischer Ebene werden zunehmend «Data Hubs» für Unternehmen, Forschungsinstitutionen, Verbände und die öffentliche Verwaltung eines Landes geschaffen. Diese bilden keine technische Infrastruktur, sondern fungieren als zentrale Anlaufstelle für Fragen zu Datenräumen und sollen so die Entwicklung von Datenräumen unterstützen. In Koordination mit bereits laufenden Massnahmen soll abgeklärt werden, ob ein solcher Data Hub auch in der Schweiz realisiert werden soll. Zudem sollen unter Berücksichtigung der Arbeiten der Nationalen Datenbewirtschaftung Ansätze für die Interoperabilität nationaler und internationaler Datenräume entwickelt werden.
3. **Internationale Massnahmen**: Um das Potenzial von transnationalen Datenflüssen realisieren zu können, muss sich die Schweiz für vertrauenswürdige Datenräume und die digitale Selbstbestimmung sowie deren Interoperabilität international einsetzen. Zu diesem Zweck werden geeignete Partner aus allen Stakeholdergruppen identifiziert und relevante Prozesse unterstützt bzw. weiterentwickelt. Wenn immer möglich, soll das Internationale Genf als Standort hierfür berücksichtigt werden. Gemeinsam mit Partnern soll im Rahmen eines internationalen Netzwerks Digitale Selbstbestimmung zudem internationale Richtlinien für Datenraumbetreiber erarbeitet werden. Diese sollen den nationalen Verhaltenskodex bestmöglich reflektieren.

Es ist denkbar, dass sich aus diesen ersten Massnahmen weitere Schritte ergeben, die Anpassungen insbesondere in der sektoriellen Gesetzgebung erfordern.

1 Auftrag

Mit diesem Bericht erfüllen das UVEK und das EDA den ihnen zugewiesenen Auftrag aus dem Bundesratsbeschluss vom 11. September 2020 zur Strategie Digitale Schweiz:

> *Das UVEK (BAKOM) und das EDA (DV) werden beauftragt, zusammen mit dem EDI (BFS) und der BK unter Einbezug der sektorbezogenen Arbeiten anderer Departemente und Ämter dem Bundesrat bis Ende 2021 einen Bericht zu den technischen, rechtlichen wirtschaftlichen und gesellschaftlichen Voraussetzungen für die Schaffung von vertrauenswürdigen Datenräumen unter Berücksichtigung der digitalen Selbstbestimmung vorzulegen. Der Bericht behandelt die nationale wie auch die internationale Perspektive und zeigt möglichen Handlungsbedarf auf.*

Der Bericht soll aus Erfahrungen in einzelnen Sektoren wie Mobilität, Energie, Gesundheit, Bildung und Finanzen **gemeinsame Prinzipien erarbeiten**, welche vertrauenswürdigen Datenräumen sowohl auf nationaler als auch internationaler Ebene zugrunde liegen müssten. Fragen bezüglich der nötigen **Infrastruktur** und **Gouvernanz** werden dabei ebenfalls beleuchtet. Zusammen mit dem Mitte 2022 erscheinenden Bericht «Digitale Service Public» des UVEK (BAKOM) deckt dieser Bericht auch Aspekte aus dem Postulat 19.3574 ab, insbesondere in Bezug auf die Sektoren Gesundheit und Bildung.

Im vorliegenden Bericht wird noch nicht im Detail untersucht, welche rechtlichen Voraussetzungen einzuhalten oder neu zu gestalten sind, wenn der Staat Aktivitäten zugunsten der Entwicklung vertrauenswürdiger Datenräume entfaltet. Die konkret vorgeschlagenen Massnahmen halten sich als erste Schritte im Rahmen des geltenden Rechts. Es ist jedoch denkbar, dass später neue, insbesondere sektorielle Rechtsgrundlagen geschaffen werden müssen.

1.1 Grundlagen der digitalen Selbstbestimmung

Die Grundlage für die Vision der digitalen Selbstbestimmung entstand aus einer Zusammenarbeit zwischen EDA (DV), UVEK (BAKOM) sowie der Schweizerischen Akademie für technische Wissenschaften (SATW) und der Swiss Data Alliance (SDA). Ein Diskussionspapier dieser Gruppe spezifiziert das Konzept der digitalen Selbstbestimmung und zeigt erste Ideen für deren Umsetzung auf.[3] Unter dem Konzept der digitalen Selbstbestimmung sollen teilweise neue oder neu gewichtete Handlungsansätze versammelt werden, die auf anerkannten Grundrechten sowie auf den vielseitigen Interessen an der Nutzung von Daten basieren und aufbauen.

Die Strategie Digitale Schweiz vom 11. September 2020 führt die Idee der digitalen Selbstbestimmung und des vertrauenswürdigen Datenraums erstmals auf Bundesebene ein. Der Bundesrat setzt sich darin Folgendes zum Ziel:

> *Die Schweiz verfügt über vertrauenswürdige Datenräume, in denen die Einwohnerinnen und Einwohner die Kontrolle über ihre eigenen Daten ausüben können. […] Es gibt klar geregelte Verhältnisse zwischen Datenproduzierenden, Datennutzenden und betroffenen Personen, die es allen Akteuren erlauben, existierende Datenbestände innerhalb von Ökosystemen selbstbestimmt und sicher über ihren ursprünglichen Verwendungszweck hinaus verfügbar zu machen. Diese Datenräume erlauben es, sowohl innerhalb von*

[3] *BAKOM, EDA, SDA & SATW (2020)*, «Diskussionspapier Digitale Selbstbestimmung».

Sektoren als auch sektorenübergreifend Innovationen und neue Businessmodelle voranzutreiben.[4]

Insbesondere in Bezug auf die internationalen Aspekte der digitalen Selbstbestimmung finden sich auch Verweise in der Aussenpolitischen Strategie 2020-2023 und der Strategie Digitalaussenpolitik 2021 – 2024.[5]

Im Mai 2021 wurde vom UVEK (BAKOM), dem EDA (DV), der SATW und der SDA zudem das **nationale Netzwerk Digitale Selbstbestimmung** lanciert.[6] Das Netzwerk bringt Experten unterschiedlicher Sektoren aus der Privatwirtschaft, der Verwaltung, der Akademie und der Zivilgesellschaft zusammen und nimmt bei der Verwirklichung der digitalen Selbstbestimmung in der Schweiz eine zentrale Rolle ein. Das Netzwerk entwickelt praktische Ansätze zum Aufbau von vertrauenswürdigen Datenräumen und bietet eine Plattform für den Austausch zwischen verschiedenen Akteuren und Sektoren. Es fördert somit einen interdisziplinären Diskurs und stärkt die transversale Perspektive auf das Thema.

1.2 Verhältnis zu anderen Berichten

Die Entwicklungen in der Datenpolitik beschäftigen den Bund, die Kantone und die Gemeinden in den letzten Jahren immer mehr. Der vorliegende Bericht ist als Teil einer Serie von Berichten zu sehen, die sich mit wichtigen Fragen im Bereich der Datenpolitik befassen (siehe Übersicht in Anhang 1). Insbesondere mit der Rolle der öffentlichen Hand im Bereich der Digital- und Datenpolitik wird sich der Bericht Digitaler Service Public des UVEK (BAKOM) befassen, der im zweiten Halbjahr 2022 veröffentlicht werden soll. Weitere relevante Arbeiten sind der im März 2021 erschienene Bericht des IGE betreffend den Zugang zu Sachdaten in der Privatwirtschaft[7] und die vor kurzem veröffentlichten Berichte des SIF[8] und des BFE[9]. In der Botschaft zum Mantelerlass über eine sichere Stromversorgung mit erneuerbaren Energien wurden bereits gesetzliche Grundlagen für die Schaffung einer nationalen Dateninfrastruktur Strom an das Parlament übersandt.[10] Das BAV arbeitet aktuell ebenfalls an einer Botschaft für ein Bundesgesetz über die Mobilitätsdateninfrastruktur.[11] Des Weiteren wurde 2020 die Strategie Geoinformation Schweiz verabschiedet.[12]

Der vorliegende Bericht nimmt diese unterschiedlichen Bestrebungen auf und versucht sie in einer übergeordneten Darstellung zusammenzuführen, indem gemeinsame Prinzipien für die Schaffung und Betreibung von vertrauenswürdigen Datenräumen erarbeitet werden. Dabei handelt es sich um Prinzipien, welche die Eigenverantwortung und die Datennutzung erhöhen und somit einen aktiven Beitrag zu einer schweizweiten und internationalen Datenpolitik leisten sollen.

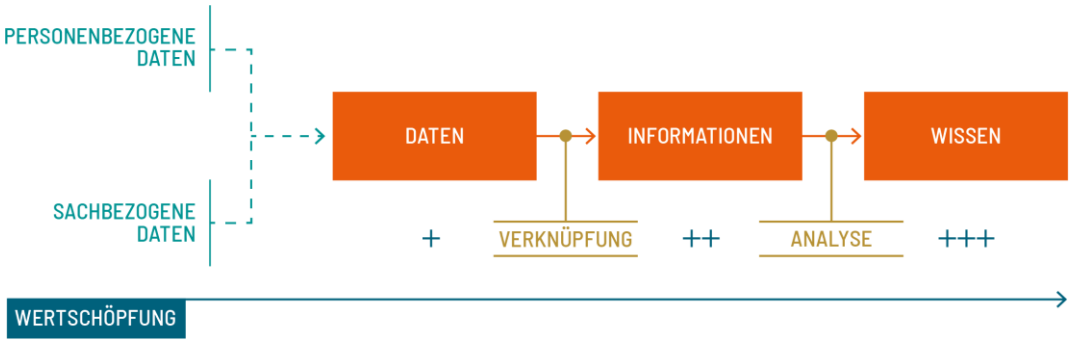
[4] *Bundesrat (2020b)*, «Strategie Digitale Schweiz», Ziel 7.5.
[5] *Bundesrat (2020a)*, «Aussenpolitische Strategie 2020-2023», S. 19; *Bundesrat (2020c)* «Strategie Digitalaussenpolitik 2021-2024», S. 14.
[6] Siehe <https://digitale-selbstbestimmung.swiss/home/> (Zugriff am 04.02.2022).
[7] *IGE (2021)*, «Zugang zu Sachdaten in der Privatwirtschaft».
[8] *SIF (2022)*, «Digital Finance: Handlungsfelder 2022+».
[9] *BFE (2021)*, «Datahub Schweiz: Kern zukünftiger Dateninfrastruktur digitalisierter Strom- und Gasmärkte».
[10] *Bundesrat (2021),* «Botschaft zum Bundesgesetz über eine sichere Stromversorgung mit erneuerbaren Energien vom 18. Juni 2021», BBl 2021, 1666 ff.
[11] *BAV (2022)*, «Erläuternde Bericht zum Bundesgesetz über die Mobilitätsdateninfrastruktur (MODIG)».
[12] *Bundesrat und BPUK (2020)*, «Strategie Geoinformation Schweiz».

2 Ausgangslage

Wirtschaft und Gesellschaft haben sich in den letzten Jahren durch die Digitalisierung und die damit verbundene Nutzung von Daten fundamental verändert. Datenvolumen, Datenvielfalt und die Geschwindigkeit der Datenverarbeitung haben rapide zugenommen und eröffnen neue Möglichkeiten. Eine vom IGE in Auftrag gegebene Studie hat die Wachstumsrate des Schweizer Datenmarkts zwischen 2017 und 2018 auf 8% beziffert, während sie im EU-Durchschnitt sogar bei 10% liegt.[13] Es erstaunt deshalb wenig, dass bereits der Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit festgehalten hat, dass Daten die «Grundeinheit der […] digitalen Revolution» sind.[14]

Als Daten werden im vorliegenden Bericht insbesondere digitale Daten bezeichnet. Dies sind *Werte, die in digitaler Form übermittelt, verarbeitet oder lesbar werden* (→ Daten). Die zunehmende Erzeugung von Daten einerseits und die verbesserten Analyse- und Nutzungsmöglichkeiten dieser Daten andererseits bilden heute eine Grundlage für Innovation und Fortschritt. Als Erkenntnisgrundlage liefern Daten die Basis, um existierende Situationen und Prozesse zu analysieren und zu verbessern oder neue Ansätze zu entwickeln. Sie geben bspw. Auskunft über die Präferenzen von Kundinnen und Kunden, den Zustand von Materialien, die Verfügbarkeit von Ressourcen oder die Wirksamkeit von Massnahmen. Sie ermöglichen damit unter anderem neue Diagnose- und Präventionsmöglichkeiten in der Medizin[15], bessere Erkenntnisse über Düngungs- und Fütterungsmuster in der Landwirtschaft[16] oder effizientere Dienstleistungen für Organisationen und Einzelpersonen.

Daten sind nicht *per se* wertvoll, sondern erhalten ihren Wert erst mit Blick auf einen spezifischen Verwendungszweck, der mithilfe der relevanten Daten erfüllt werden soll. Daten sind somit Teil einer digitalen Wertschöpfungskette (→ digitale Wertschöpfungskette): Erst durch die Verknüpfung von verschiedenen *Daten* werden *Informationen* (→ Informationen) generiert und erst durch die Analyse dieser Informationen und Daten im Hinblick auf einen bestimmten Handlungszweck entsteht *Wissen* (→ Wissen), welches einen Sinn ergibt und handlungsanleitend wirken kann (siehe Grafik 1).[17]



Grafik 1: Datenwertschöpfungskette[18]

[13] *IDC (2020)*, «Analysis of the Data Market: 2017-2018, 2025 for Switzerland and other EU28 Member States»; *IGE (2021)*, «Zugang zu Sachdaten in der Privatwirtschaft», S. 12.
[14] *Gadient B. M. et al. (2018)*, «Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit», S. 24.
[15] *Bundesrat (2019)*, «Gesundheitspolitische Strategie des Bundesrates 2020-2030», S. 12.
[16] Siehe Agroscope Projekt *Smart Farming* <https://www.agroscope.admin.ch/agroscope/de/home/themen/wirtschaft-technik/smart-farming.html> (Zugriff am 03.02.2022), bspw. «Technologien Milch und Fleischproduktion» oder «Ortsspezfische N-Düngung».
[17] *Swiss Economics (2021)*, «Vertrauenswürdige Digitale Datenräume: Schlussbericht Konzeptualisierung und Anforderungen», S. 7.
[18] Angelehnt an: *Swiss Economics (2021)*, «Vertrauenswürdige Digitale Datenräume: Schlussbericht Konzeptualisierung und Anforderungen», S. 8.

Daten haben zudem *spezifische Eigenschaften*, welche zum enormen Potenzial für ihren wirtschaftlichen und gesellschaftlichen Nutzen beitragen. Nennenswert sind die folgenden Eigenschaften:

- Daten sind grundsätzlich **nicht-rivalisierend**: Das bedeutet, dass dieselben Daten, ohne dabei an Wert zu verlieren, von verschiedenen Akteuren (unter Umständen auch zu verschiedenen Zwecken) verwendet, geteilt, verknüpft und wiederverwendet werden können.
- Daten sind zudem **nicht automatisch ausschliessbar**: Um Dritte von der Einsicht in oder der Nutzung von Daten auszuschliessen, bedarf es Massnahmen bspw. technischer, juristischer oder organisatorischer Natur. Dies kann aus verschiedenen Gründen angestrebt werden (bspw. aus regulatorischen Gründen wie dem Datenschutz oder aus wirtschaftlichen Gründen wie einem Wettbewerbsvorteil). Ohne derartige Massnahmen sind Daten prinzipiell allgemein zugänglich.
- Daten sind **einfach zu vervielfältigen und zu bearbeiten**: Daten können einfach kopiert werden. Insbesondere wenn sie maschinenlesbar und in offenen Formaten strukturiert sind, können sie auch einfach bearbeitet und weiterverbreitet werden.
- Daten als **Nebenprodukt**: Die Erzeugung von Daten ist teilweise das Nebenprodukt einer anderen wirtschaftlichen oder sozialen Haupttätigkeit (bspw. der Nutzung eines Gerätes, der Abwicklung eines Geschäftes etc.). Dies bedeutet, dass, im Gegensatz zu anderen Innovationsgrundlagen, Daten zum Teil ohne kostspielige Investitionen und ohne Forschungs- und Entwicklungskosten generiert werden können.[19]

Daten können dank diesen Eigenschaften kollektiv genutzt werden (→ kollektive Datennutzung) und damit einem breiten Spektrum von Akteuren mit unterschiedlichem Geschäftsmodell als Erkenntnis- und Innovationsgrundlage zur Verfügung stehen. Heutzutage werden Daten jedoch vorwiegend von einzelnen Akteuren genutzt. Viele der erfolgreichsten Anwendungen im Internet basieren auf einem Modell, bei welchem die Daten proprietär sind, d.h. von einer privaten Plattform verwaltet und für kommerzielle Zwecke genutzt werden. Im Folgenden wird auf Plattformen als das zurzeit dominante Geschäftsmodell der Digitalisierung näher eingegangen.

2.1 Plattformen als dominantes Geschäftsmodell der Digitalisierung

Plattformbasierte Geschäftsmodelle haben die Basis für ein neues Zusammenspiel zwischen wirtschaftlichen und gesellschaftlichen Akteuren geschaffen. Sie reduzieren die Transaktionskosten für ihre Nutzerinnen und Nutzer massiv, indem sie Daten standardisieren (→ Standardisierung) sowie Kundinnen und Kunden untereinander (bspw. *Twitter*) einfach und schnell verbinden. Plattformen liefern zudem als Intermediäre (→ Intermediäre) die Infrastruktur, die es Kundinnen und Kunden und Drittanbietern, d.h. Anbietern, die auf einer Plattform ihre eigenen Dienstleistungen anbieten, ermöglicht, einfach zu interagieren und Transaktionen zu tätigen (bspw. Marketplaces wie *ebay* oder *booking.com*). Oder sie eröffnen Intermediären selbst die Möglichkeit, Direktangebote an Kundinnen und Kunden zu tätigen (bspw. *Amazon*). Oftmals finden sich mehrere dieser Verbindungen in einer Plattform (sog. → Multi-Sided Markets). Ein Beispiel dafür sind Social-Media-Plattformen wie *Facebook*, die Nutzerinnen und Nutzer untereinander verbinden, aber Werbetreibenden auch die Möglichkeit bieten, ihre Werbung an mögliche Nutzerinnen und Nutzer zu bringen. Es gibt somit eine Vielzahl

[19] *IGE (2021)*, «Zugang zu Sachdaten in der Privatwirtschaft», S. 13.

verschiedener Plattformen, die sich nach unterschiedlichen Kriterien (Geschäftsmodell, Art der Interaktion, Gouvernanz → Gouvernanz, Grösse, etc.) kategorisieren lassen.[20]

Unternehmen sind generell daran interessiert marktrelevante Daten zu generieren, bspw. in den Bereichen Kundenverhalten, Präferenzen, Standorte, Verweildauer, optimale Preisgestaltung, etc. Durch ihren **Status als Intermediäre** haben Plattform-Unternehmen einen besonders effizienten Zugang zu diesen Daten. Plattform-Unternehmen haben sich darauf ausgerichtet, die Bedürfnisse ihrer Nutzerinnen und Nutzer auf der Grundlage, der durch die Nutzung der Plattformen generierten Daten möglichst gut zu kennen und ihnen darauf basierend optimierte personalisierte Dienstleistungen zu bieten (Effizienzgewinn, einfachere Entscheide, etc.). Aufgrund des Mehrwertes sind die Nutzerinnen und Nutzer oftmals bereit, die Dienste solcher Plattformen zu nutzen, auch wenn sie nur begrenzt nachvollziehen können, was mit ihren Daten geschieht.

Plattform-Unternehmen verfügen dank ihrer vielseitigen Interaktionen über erhebliche Datenmengen aus verschiedenen Quellen. Dies ist unter anderem auch auf den starken Netzwerkeffekt zurückzuführen: Je mehr Nutzerinnen und Nutzer auf einer Plattform aktiv sind, umso attraktiver wird diese für Drittanbieter, ihre Dienstleistungen oder Produkte vermehrt auf dieser Plattform anzubieten (→ Netzwerkeffekt). Dies wiederum erhöht die Attraktivität für Nutzerinnen und Nutzer, bspw. durch billigere Preise oder breitere Produktepaletten, kann aber auch zu einer rigiden Kundenbindung führen. Netzwerkeffekt bedeutet auch, dass diese Plattform Daten generiert, welche für neue Innovationen genutzt werden können (→ Datennetzwerkeffekt).[21] Durch diesen Datennetzwerkeffekt können sich Plattformen immer besser etablieren: Entweder weil sie die erhobenen Daten monetisieren (d.h. an Dritte verkaufen, die sie für ihre eigene Wertschöpfung benötigen, bspw. in Werbung oder Produkteentwicklung) oder weil Plattformen diese Daten nutzen, um selbst neue Dienstleistungen oder Produkte zu entwickeln.[22] Demgegenüber stehen Drittanbieter, die dank Plattforminfrastrukturen zwar eine grössere Reichweite haben (und dafür auch bezahlen), aber über keinen direkten Zugang zu Kundenbedürfnissen und Daten verfügen.

Im Gegensatz zu anderen Unternehmen, welche ihre eigenen Daten proprietär nutzen, sind Plattform-Unternehmen überdurchschnittlich effizient in der Zusammenführung von Daten aus verschiedenen Quellen. Diese dank dem Netzwerkeffekt generierten proprietären Daten stellen damit einen gewichtigen Wettbewerbsvorteil dar und können zu einer dominanten Stellung beitragen, die sogar über den ursprünglichen Sektor und Tätigkeitsbereich hinausreichen kann. Teilweise können sich datenbasierte Plattformen dadurch eine weitgehende Kontrolle über Lieferketten verschaffen (sog. → vertikale Integration). Als Beispiel dafür wird oft die Entwicklung von *Amazon* vom Buch- zum Grosshändler und Logistik- und IT-Dienstleister (*Amazon Logistics*, *Amazon WebServices*) genannt.[23] Aufgrund der grossen Effizienzgewinne durch die datengetriebene Personalisierung ist davon auszugehen, dass sich die Plattformisierung in allen Bereichen unseres wirtschaftlichen und gesellschaftlichen Lebens fortsetzen wird. Diese Dynamik bedeutet aber nicht, dass alle bestehenden Plattformen längerfristig das Rennen machen werden. Der Erfolg einer Plattform ist abhängig vom jeweiligen Geschäftsmodell. Es kann durchaus beobachtet werden, dass Nutzerinnen und Nutzer ihre Präferenzen ändern und dadurch neue Akteure ins Spiel kommen (bspw. *TikTok*).

[20] *Asadullah A., Faik I. and Kankanhalli A. (2018)*, «Digital Platforms: A Review and Future Directions».
[21] *Collovà P. et al. (2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung», S. 8.
[22] *Collovà P. et al. (2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung», S. 8; siehe auch *IGE (2021)*, «Zugang zu Sachdaten in der Privatwirtschaft», S.14.
[23] *Zhu F. and Liu Q. (2018)*, «Competing with Complementors: An Empirical Look at Amazon.com».

2.2 Ungenügende Realisierung des Datenpotenzials

Im Medien- oder Handelsbereich haben datenbasierte Plattformen die Datennutzung mit dem Zusammenführen verschiedener Datenquellen revolutioniert. Die daraus resultierenden Produkte und Dienstleistungen schaffen für die jeweiligen Unternehmen und ihre Nutzenden einen grossen wirtschaftlichen Mehrwert. Auch in anderen wichtigen Sektoren unserer Gesellschaft, wie bspw. Mobilität, Gesundheit und Bildung, sind durch personalisierte Dienstleistungen grosse Verbesserungen möglich. Daten dienen als Treiber von Innovationen und Effizienz, die von gesamtgesellschaftlichen Interesse sind. Sie können unter anderem dazu beitragen, den Auswirkungen des Klimawandels entgegenzuwirken, die Ausbreitung einer Pandemie einzudämmen sowie Dienstleistungen von öffentlichem Interesse, wie bspw. das Gesundheitssystem oder das Mobilitätssystem, effizienter und bedürfnisorientierter zu gestalten. Ebenso kann die generierte Wissensgrundlage von datenbasierten Informationen und Analysen in der Verwaltung und der demokratischen Entscheidungsfindung von grosser Bedeutung sein, sowohl als Grundlage für eine informierte Meinungsbildung, als auch zur konkreten Umsetzung und Realisierung von Projekten. Eine optimale Nutzung von Daten ist folglich aus wirtschaftlicher, gesellschaftlicher und sozialer Perspektive interessant und wichtig.

Oftmals aber können oder wollen traditionelle – private oder öffentliche – Anbieter von Leistungen in den genannten Bereichen das Datenpotenzial nicht nutzen oder Datennutzer und Datenproduzenten sind nicht bereit, die Nutzung ihrer Daten zuzulassen. Dies weil Datennutzer und Anbieter befürchten, dass andere Rückschlüsse auf ihre Geschäftsmodelle ziehen und dadurch Wettbewerbsnachteile entstehen könnten oder weil Datenproduzenten die Kontrolle über die Erhebung, Nutzung und die Weiterverwendung ihrer Daten verlieren könnten. Es fehlt an einem genügenden Vertrauen in und Verständnis für die Chancen und Vorteile, Daten zu teilen und zu nutzen.[24] Weitere Gründe liegen im ungenügenden Verständnis über die Rechtslage sowie im erschwerten Zugang zu Daten aus rechtlicher und technischer Perspektive (bspw. fehlende standardisierte Schnittstellen →Standards, → Schnittstellen und APIs → Application Programming Interface).[25] Zudem fehlt es an Know-How, Ressourcen, und Infrastrukturen (bspw. zur Speicherung und Analyse von Daten), um die Datennutzung umzusetzen und voranzutreiben. Wie ein kürzlich erschienener Bericht im Auftrag der Europäischen Kommission gezeigt hat, hinkt gerade auch die Datennutzung im öffentlichen Bereich hinterher. Gründe dafür sind technische, organisatorische und rechtliche Hürden sowie eine fehlende Kultur der gemeinsamen Datennutzung.[26]

Des Weiteren konzentrieren sich derzeit gemäss einer Studie der Berner Fachhochschule viele relevante Daten als Informations- und Wissensgrundlage für Innovation vermehrt bei grossen internationalen Plattformen. Dies, weil Letztere aufgrund des Netzwerkeffekts, ihrer Grösse und der daraus resultierenden marktbeherrschenden Stellung Daten effektiv proprietär zu nutzen wissen und insbesondere für Nutzerinnen und Nutzer einen erkennbaren Mehrwert bieten (siehe Kapitel 2.1).[27] Dies kann zu einem verzerrten Wettbewerb zwischen Unternehmen, aber auch zu einem Wissens- und Informationsungleichgewicht gegenüber Staat und Gesellschaft führen. Mittel- und längerfristig können

[24] Siehe dazu *IGE (2021)*, «Zugang zu Sachdaten in der Privatwirtschaft»; *OECD (2019)*, «Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies»; *Europäische Kommission (2016)*, «Study on Data Sharing between Companies»; *Europäische Kommission (2018a)*, «Towards a common European Data Space»; *Europäische Kommission (2018b)*, «Staff Working Document – Guidance on Sharing Private Sector Data in the European Data Economy».
[25] Das IGE hat im Rahmen seiner Arbeiten zum Zugang zu Sachdaten in der Privatwirtschaft Anstrengungen unternommen, um den rechtlichen Bedenken entgegenzuwirken. Zu erwähnen sind insbesondere die Musterverträge, welche hier eingesehen werden können: <https://www.ige.ch/de/uebersicht-geistiges-eigentum/gesellschaftliche-bedeutung/datenbearbeitung-und-datensicherheit> (Zugriff am 04.03.2022).
[26] *Europäische Kommission (2021)*, «Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest: Final Report prepared by the High-Level Expert Group on Business-to-Government Data Sharing», S. 24-28.
[27] *Collovà P. et al. (2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung», S. 9.

dadurch sektorübergreifende Datenkonzentrationen entstehen, welche aufgrund mangelnder Ideenvielfalt Innovation inner- und ausserhalb des Plattform-Ökosystems erschweren[28] und ungewollte Abhängigkeiten bei wichtigen Dienstleistungen (bspw. Service Public) von privaten Akteuren schaffen könnten.

Diese Entwicklungen sind mit Blick auf eine breite Datennutzung und damit auf das Ausschöpfen des Gesamtpotenzials nicht optimal. Sie zeigen einerseits, dass das gesamtgesellschaftliche Potenzial von Daten noch nicht vollständig ausgeschöpft wird. Andererseits aber auch, dass Individuen, Unternehmen (gerade auch KMUs) und die Wissenschaft gewillt und in der Lage sein müssten, vermehrt Daten zu teilen und zu nutzen, um das Gesamtpotenzial der Daten realisieren zu können.[29] Je nach Sektor und Unternehmen sind die Gründe für die mangelnde Realisierung des gesamtgesellschaftlichen Datenpotenzials unterschiedlich ausgeprägt. Es ist jedoch unbestritten, dass das volle Potenzial der Datennutzung in der Schweiz noch nicht optimal genutzt wird.[30] Im europäischen Vergleich kann die Schweizer Datenwirtschaft zwar als eher ausgereift beurteilt werden. In vielen Sektoren liegt sie jedoch hinter den Spitzenreitern zurück.[31]

2.3 Steigendes Misstrauen gegenüber Datennutzung

Die verstärkte Datennutzung stellt auch Bürgerinnen und Bürger vermehrt vor Herausforderungen, insbesondere bezüglich dem Schutz und der Wahrnehmung ihrer Grundrechte auf den Schutz ihrer Privatsphäre und ihrer persönlichen Daten, beziehungsweise auf informationelle Selbstbestimmung (siehe Kapitel 3.2).

Wer an der digitalen Welt teilnehmen will, hat häufig keine andere Wahl, als seine Daten preis- und seine Kontrolle darüber aufzugeben. Daten werden heute oft nicht auf der Basis von Transparenz oder Vertrauen geteilt, sondern weil Individuen nur durch das Preisgeben ihrer Daten digitale Anwendungen nutzen können.[32] Diese passive Haltung steht oft im Gegensatz zum Selbstverständnis in demokratischen und rechtsstaatlich organisierten Gesellschaften als aktive Bürgerinnen und Bürger mitentscheiden zu können. Durch diese Entwicklungen wird das formal bestehende Recht jeder Person, ihre Daten anderen Privaten nicht preiszugeben oder ihnen nur erwünschte Nutzungen zu gestatten, teilweise seiner Substanz entleert. Vorliegend sollen Ansätze untersucht werden, die die effektive Wirksamkeit dieses Rechts stützen sollen.

Auf nationaler und internationaler Ebene sehen sich private und staatliche Akteure vermehrt mit der Herausforderung konfrontiert, dass Nutzerinnen und Nutzer zunehmend skeptisch sind, Daten über sich preiszugeben. Die Gründe für die zunehmende Zurückhaltung sind nachvollziehbar: Die Verarbeitung, Verlinkung und Auswertung verschiedener Datenquellen hat nicht nur zu einer «Vermessung der Welt» geführt, sondern ermöglicht auch eine immer exaktere Abbildung vom Verhalten unserer Gesellschaft und von uns als Individuen. Die daraus entstandenen Möglichkeiten, wie bspw. die Erstellung von Persönlichkeits- oder Verhaltensprofilen auf der Basis von Daten (→ Profiling), lösen in vielen Nutzerinnen und Nutzern ein Unbehagen über mögliche und reale Missbräuche aus. Dies ist auch durch den teilweise sorglosen Umgang von privaten Unternehmen oder öffentlichen Stellen mit Nutzerdaten begründet. Beispiele hierfür sind datenbasierte Diskriminierung oder die Verstärkung bestehender

[28] Siehe dazu *IGE (2021)*, «Zugang zu Sachdaten in der Privatwirtschaft», S. 15.
[29] *OECD (2019)*, «Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies».
[30] *Gadient B. M. et al. (2018)*, «Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit».
[31] *SIF (2022)*, «Digital Finance: Handlungsfelder 2022+».
[32] *Collovà P. et al. (2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung», S. 3.

Ungleichheiten, mangelnde Transparenz darüber wie und von wem diese Daten (zukünftig) genutzt werden sowie Furcht vor Manipulation. Diese Befürchtungen stehen in einem Gegensatz zur Bereitschaft derselben Nutzerinnen und Nutzern, ihre Daten globalen Plattformen preiszugeben, um von deren Dienstleistungen zu profitieren, oftmals ohne genau zu wissen, was mit den Daten passiert (→ Privatsphären-Paradox). Dieses Phänomen wird in der Forschung teilweise mit der schwachen Marktstellung von Nutzerinnen und Nutzer gegenüber grossen Tech-Plattformen erklärt, welche Affektentscheidung entgegen eigentlichen Präferenzen und zulasten rationaler Kosten-Nutzen-Entscheidungen begünstigen.[33]

2.4 Herausforderungen in der Datennutzung

Die verstärkte Datennutzung stellt Gesellschaft, Wirtschaft und Staat vor neue Herausforderungen. Auf einer Makroebene gilt es einerseits das Datenpotenzial besser auszuschöpfen und andererseits dem stärker werdenden gesellschaftlichen Misstrauen gegenüber der zunehmenden Nutzung von Daten zu begegnen – insbesondere, wenn mächtige Akteure wie bspw. die öffentliche Hand oder transnationale Unternehmen über diese Daten verfügen.

In diesem Zusammenhang ist von folgendem Problem die Rede: Um Vertrauen und Kontrolle zu stärken, müsste der Austausch von Daten in der Regel eingeschränkt werden, die Realisierung der Wertschöpfungspotenziale würde allerdings mehr Austausch und Verlinkung von Daten erfordern.[34] In der Datenpolitik werden diese Herausforderungen unter dem wahrgenommenen Spannungsfeld von Datenschutz und Datennutzung zusammengefasst. Dieses Spannungsfeld wird generell als binär und Win-Lose-Situation dargestellt. Das bedeutet, dass der Eindruck entsteht, dass zwischen griffigem Schutz oder der verstärkten Nutzung von Daten entschieden werden muss.

Basierend auf Kapitel 2 lässt sich festhalten, dass folgende Herausforderungen dazu beitragen, dass bei einem wachsenden Anteil der Bevölkerung das nötige Vertrauen und Bewusstsein für eine nachhaltige Datennutzung aktuell fehlt:[35]

1. **Datenkonzentration und intransparente Entscheidungsstrukturen**: Daten sind ungleich verteilt und konzentrieren sich vielfach bei einigen grossen Tech-Unternehmen oder bei Akteuren, welche in Non-Tech-Sektoren über eine grosse Marktabdeckung verfügen. Daten werden in diesen Konstellationen häufig proprietär genutzt, um Mehrwerte für die entsprechende Organisation zu schaffen. Dies geschieht häufig ohne nennenswerte Kontrolle durch die betroffenen Akteure und kann deshalb zu einer Erosion der Selbstbestimmung und der Festigung einer dominanten Position des datenkontrollierenden Akteurs beitragen. Nutzen die Akteure die Daten der Nutzerinnen und Nutzer sorglos, führt dies zu einem Vertrauensverlust und damit zu einer kleineren Bereitschaft, Daten bewusst teilen zu wollen.
2. **Fehlende Organisation von Nutzerinnen und Nutzer**: In der heutigen Plattformökonomie verfügen Nutzerinnen und Nutzer (d.h. sowohl Individuen als auch Unternehmen, die auf Plattformen angewiesen sind) kaum über Organisationen, um ihre Interessen mit genügend Einfluss zu vertreten. Sie sind selten kollektiv organisiert und oft ist der individuelle

[33] *Jentzsch N. (2017)*, «Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds – Ökonomische Rahmenbedingungen innovativer Lösungen zu Einwilligungen im Datenschutz»; *Collovà P. et al. (2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung».
[34] *Mulgan G. and Straub V. (2019)*, «The New Ecosystem of Trust».
[35] Siehe dazu *Collovà P. et al. (2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung», S. 9-16.

datenbezogene Beitrag eines einzelnen Akteurs nicht bedeutend genug, um Verhaltensänderungen bei den Plattformbetreibern zu erzielen.[36] Dieses Ungleichgewicht und die wirkenden Netzwerkeffekte in Plattform-Verhältnissen können dazu führen, dass Nutzerinnen und Nutzer auch für sie ungünstige Bedingungen akzeptieren, sowohl in Bezug auf die Privatsphäre als auch in wirtschaftlicher Hinsicht. Dieses Ungleichgewicht kann zumindest teilweise durch starke Datenschutzbehörden ausgeglichen werden.[37]

3. **Ungenügender Entscheidungskontext für Nutzerinnen und Nutzer:** Nutzerinnen und Nutzer verfügen im digitalen Raum über eine eingeschränkte Entscheidungsfähigkeit. Oft fehlen ihnen die notwendigen Wissensgrundlagen, um selbstbestimmte Entscheidungen zu treffen.[38] Gleichzeitig sind Entscheidungen zur Datenfreigabe immer kontextabhängig und es treten gerade in Alltagssituationen oft Affektentscheidungen und das Privatsphären-Paradox zutage. Dies führt dazu, dass vor allem in solchen Situationen Daten unüberlegt freigegeben werden, in denen die fehlende Einwilligung persönliche Daten preiszugeben eine Einschränkung der angebotenen Dienstleistung zur Folge hat. Zudem kann die digitale Kluft (→ digitale Kluft) dazu führen, dass Menschen aus dem digitalen Leben ausgeschlossen werden.
4. **Ungenügende Anreize für gemeinsame Datennutzung**: Um ein vertrauenswürdiges System für die gemeinsame Nutzung von Daten zu schaffen, müssen, neben den nötigen Schutzmassnahmen, auch ausreichende Anreize für den Austausch von Daten gesetzt werden, sowohl für Individuen als auch für Unternehmen. Aktuell sind die Anreize der Datennutzung ungleichmässig verteilt – oftmals profitiert vornehmlich das Unternehmen, welches im Besitz der Daten ist, da es diese proprietär nutzt. Diese Unternehmen haben tendenziell wenig Anreize an ihrem privilegierten Status etwas zu ändern. Sie tragen dazu bei, dass das volle Potenzial der Daten nicht genutzt werden kann.

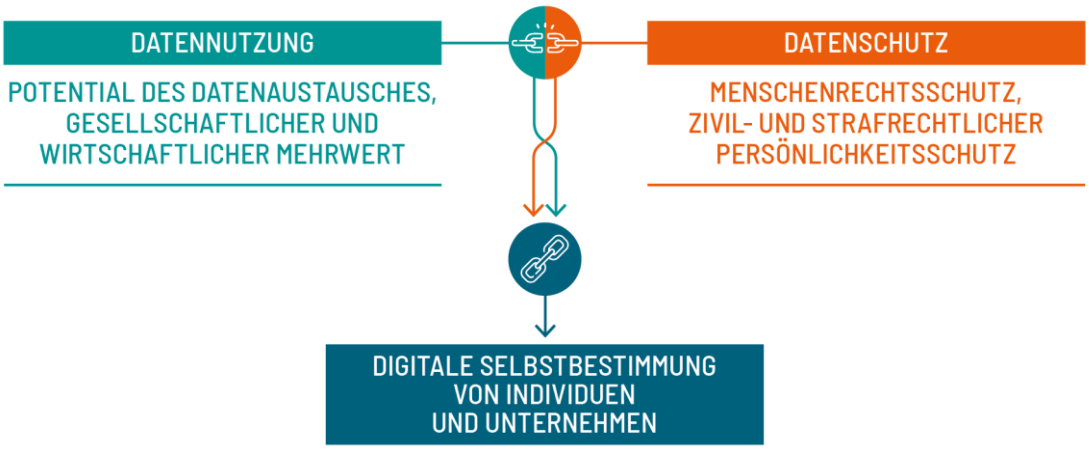
3 Digitale Selbstbestimmung

Um das gesellschaftliche und wirtschaftliche Nutzungspotenzial von Daten besser auszuschöpfen und gleichzeitig einen Kontrollverlust über die eigenen Daten zu verhindern, muss die Schweiz eine Datenpolitik entwickeln, welche den vermeintlichen Gegensatz von Datenschutz und Datennutzung überwindet.

Die digitale Selbstbestimmung soll ein neuer Ansatz einer solchen Datenpolitik sein: Individuen, Unternehmen und die Gesellschaft als Ganzes sollen über ihr Handeln im digitalen Raum selbst bestimmen können. Dies beinhaltet die Fähigkeit, die Relevanz und den Wert der für sie wesentlichen Daten einordnen zu können, Zugang zu und Kontrolle über diesen Daten zu haben und über deren Verwendung zu bestimmen. Durch eine bessere Kontrolle über die eigenen Daten soll das Vertrauen in die Datengesellschaft gestärkt und die Bereitschaft, Daten zu teilen und zu nutzen, erhöht werden. Eine verstärkte Datenteilung zwischen verschiedenen Akteuren wird den Zugang und die Wachstumschancen für Akteure und Sektoren verbessern und die Nutzung und Kombination von Daten

[36] Siehe aber *EuGH (2020)*, «Data Protection Commissioner gegen Facebook Ireland Limited und Maximilian Schrems»; Projekte und Beschwerden der seit 2018 aktiven Non-Profit Organisation *noyb* <https://noyb.eu/en> (Zugriff am 03.03.2022).
[37] In der Schweiz verpflichtet der revidierte Art. 49 revDSG den EDÖB nun, von Amtes wegen oder auf Anzeige hin eine Untersuchung einzuleiten, wenn hinreichende Anhaltspunkte dafür vorliegen, dass eine Datenbearbeitung gegen das DSG verstossen könnte. Ist die betroffene Person der Urheber der Anzeige, muss der EDÖB sie über die Folgemassnahmen und das Ergebnis einer allfälligen Untersuchung informieren. Allerdings müssen diese Behörden mit ausreichenden Ressourcen ausgestattet sein.
[38] Dies betrifft nicht nur den Zugang zu relevanten Personendaten, sondern unter Umständen auch den Zugang zu Sachdaten. Die Informationskosten sind aufgrund der grossen technischen und wirtschaftlichen Komplexität hoch und unübersichtlich. Siehe dazu *Collovà P. et al. (2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung», S. 7-9.

auf eine völlig neue Art und Weise ermöglichen. Dies schafft die Grundlage zur Entwicklung innovativer Anwendungen zum individuellen und kollektiven Nutzen.[39] Die Gesellschaft als Ganzes soll von den Effizienzsteigerungen und Innovationspotenzialen aus der Datennutzung profitieren können, ohne die demokratische Kontrolle über die gesellschaftlichen Grundfunktionen in wichtigen Sektoren zu verlieren. Die digitale Selbstbestimmung versteht sich folglich als langfristiges Ziel.



Grafik 2: Trade-Off Datennutzung und Datenschutz

3.1 Komponenten der digitalen Selbstbestimmung

Unter Selbstbestimmung versteht man gemeinhin, dass jeder Mensch mit freiem Willen selbst darüber entscheiden darf, wie er leben möchte. Selbstbestimmung bezieht sich aber nicht nur auf ein Individuum, sondern auch auf ganze Gesellschaften oder Völker, die selber ihr Schicksal bestimmen können. Die Selbstbestimmung im digitalen Raum setzt sich analog dazu aus einer individuellen und kollektiven Komponente zusammen.

Individuelle Komponente

Auf der individuellen Ebene sind Wissen, Entscheidungsfreiheit und Handlungsfähigkeit für die Selbstbestimmung im digitalen Raum massgebend:

- **Wissen** beinhaltet die Fähigkeit, digitale Anwendungen zu verstehen und zu gebrauchen, über genügend Informationen zu verfügen, um die Folgen der Nutzung einzuordnen und sich im Klaren darüber zu sein, wie man persönliche Präferenzen im digitalen Raum verwirklichen kann.[40]
- **Entscheidungsfreiheit** beinhaltet die Möglichkeit, sich im digitalen Raum eine eigene Meinung zu bilden, Wahlmöglichkeiten zu haben und Entscheidungen zu treffen.
- **Handlungsfähigkeit** beinhaltet die Fähigkeit, eigene Entscheidungen im digitalen Raum umzusetzen.

[39] *OECD (2019)*, «Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use Across Societies», S. 60-76.
[40] Ein Teil dieser Voraussetzung beinhaltet auch Aspekte, die oft unter *Digital Literacy* oder unter *Data Literacy* zusammengefasst werden – also dem Zugang zu Ausbildung und Erfahrung im Umgang mit digitalen Anwendungen und Daten. Dies ist jedoch nur ein Aspekt der Wissenskomponente. Sie muss insofern breiter verstanden werden, als dass alle Akteure dazu beitragen sollen. Für Dienstanbieter bedeutet dies bspw., dass genügend Informationen über die Funktionsweise einer Anwendung verfügbar und zugänglich sind (siehe auch Kapitel 4.1).

Kollektive Komponente
Sie beinhaltet folgende Aspekte:

- **Soziales und kulturelles Selbst:** Im digitalen Raum ist das Selbst immer nur als ein vernetztes Selbst denkbar. Das soziale und kulturelle Umfeld bildet die Basis für die Art und Weise, wie das Selbstbestimmungsrecht in Anspruch genommen wird.
- **Gemeinsame Datennutzung:** Verschiedene Akteure können Daten miteinander nutzen und austauschen. Dadurch soll die Teilnahme an kollektiven Formen der Datennutzung gefördert und der Handlungsspielraum der Akteure durch gemeinsam genutzte Daten erweitert werden.
- **Daten als öffentliches Gut:** An vielen Daten, insbesondere Sachdaten (→ Sachdaten), kann ein öffentliches Interesse bestehen. Solche Daten können dann als Gemeingut verstanden werden, auf das alle Mitglieder einer Gemeinschaft Zugriff haben sollen.[41]
- **Gemeinwohlorientierung:** Daten werden zur gemeinsamen Problemlösung (bspw. Pandemie, Klimawandel) genutzt, um zu einer Effizienz- und Wohlstandssteigerung beizutragen sowie um die demokratische Kontrolle über Kernfunktionen unserer Gesellschaft zu gewährleisten.

3.2 Rechtliche Grundlagen

Digitale Selbstbestimmung soll den vermeintlichen Gegensatz zwischen Datenschutz und Datennutzung überwinden. Rechtlich gesehen bedeutet dies, dass sich das Konzept der digitalen Selbstbestimmung aus zwei unterschiedlichen Kategorien von Rechtsgrundlagen zusammensetzt:

- Grundlagen, die vorwiegend den **Schutz der Person** und deren Privatsphäre sowie die **Partizipation im digitalen Raum** gewährleisten, und
- Grundlagen, in denen sich vorwiegend die **Datennutzung** und damit Aspekte der wirtschaftlichen Freiheit und Fortschritts- und Innovationspotenziale widerspiegeln.

3.2.1 Schutz und Partizipation im digitalen Raum

Die digitale Selbstbestimmung basiert auf Menschenrechten, die sowohl in der Schweizer Bundesverfassung als auch im Völkerrecht verankert sind. Im Vordergrund stehen das Recht auf persönliche Freiheit (Art. 10 Abs. 2 BV), die Rechte auf Privatsphärenschutz, informationelle Selbstbestimmung und Schutz vor dem Missbrauch persönlicher Daten (Art. 13 BV; Art. 8 EMRK; Art. 17 UNO-Pakt II) sowie die Informationsfreiheit (Art. 16 BV, Art. 10 EMRK, Art. 19 UNO-Pakt II). Die kollektive Komponente der digitalen Selbstbestimmung lässt sich insbesondere auf die politischen Rechte (Art. 34 BV) abstützen.

Für die digitale Selbstbestimmung ist das *Recht auf informationelle Selbstbestimmung* besonders wichtig. Es besagt, dass jeder Mensch grundsätzlich selbst entscheiden kann, wem er unter welchen Umständen und zu welchem Zweck seine Personendaten (→ Personendaten) anvertraut.[42] Dieser Schutz ist zwar nicht absolut, da erstens Einschränkungen des Grundrechts zulässig sind, sofern sie verhältnismässig und die erforderlichen gesetzlichen Grundlagen vorhanden sind, und da zweitens zunächst nur der Staat durch die Grundrechte verpflichtet wird. Diese müssen aber in der ganzen Rechtsordnung zum Tragen kommen und die Behörden haben dafür zu sorgen, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden (Art. 35 BV).

[41] Siehe auch *Datenarten* in Anhang 2.
[42] *Häfelin U. et al. (2020)*, «Schweizerisches Bundesstaatsrecht», S. 122-123; Als Personendaten gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, d.h. auch Daten, die durch Rückschlüsse einer Person zugeordnet werden können (Art. 5 lit. a revDSG).

Der Persönlichkeits- und Privatsphärenschutz und die informationelle Selbstbestimmung werden in diesem Sinn auf Gesetzesstufe durch Art. 27 und 28 des Schweizerischen Zivilgesetzbuches (ZGB) und durch das DSG näher konkretisiert. Das Datenschutzrecht bindet sowohl staatliche Behörden als auch Private bei der Bearbeitung von Personendaten und enthält für beide Kategorien teilweise unterschiedliche Regeln. Ein zentraler Unterschied besteht insofern, dass bei der Datenbearbeitung durch Private die Einwilligung als Rechtfertigungsgrund im Vordergrund steht (Art. 13 DSG bzw. Art. 31 revDSG, BBl 2020 7639), während bei der Datenbearbeitung durch staatliche Organe im Grundsatz anstelle der Einwilligung eine gesetzliche Grundlage erforderlich ist.[43] Formal hat somit die betroffene Person in der Regel das alleinige Entscheidungsrecht über die Verwendung von Daten über sie selber. Letztlich kennt auch das Schweizerische Strafgesetzbuch und Nebenstrafrecht Bestimmungen, die den missbräuchlichen Umgang mit Daten unter Strafe stellen.

3.2.2 Wirtschaftliche Freiheit und Innovation

Die digitale Selbstbestimmung ist auch in Rechtsgrundlagen verankert, die vorwiegend nutzen- und wirtschaftsorientiert sind. Besonders erwähnenswert in diesem Kontext sind das *Grundprinzip der Vertragsfreiheit* im Schweizerischen Obligationenrecht (OR), die *Wirtschaftsfreiheit* (Art. 27 und 94 BV) sowie die *Wissenschaftsfreiheit* (Art. 20 BV).

Das privatrechtliche Grundprinzip der Vertragsfreiheit und die Wirtschaftsfreiheit bezwecken die unternehmerische Freiheit, wonach die privatwirtschaftliche Tätigkeit durch natürliche und juristische Personen so frei wie möglich ausgeübt und ausgestaltet werden soll. Dies gilt auch im digitalen Raum. Beide Garantien verschreiben sich einerseits dem Grundbedürfnis einer freiheitlichen und selbstbestimmten Lebensgestaltung und anderseits einer marktwirtschaftlichen und wettbewerbsorientierten Wirtschaftsordnung.[44] Es besteht somit ein starker Konnex zwischen diesen Garantien und der Realisierung der digitalen Selbstbestimmung.

Ähnlich verhält es sich mit der Wissenschaftsfreiheit. Letztere gewährleistet die Gewinnung und Verbreitung von Forschungserkenntnissen und beinhaltet das Recht, von den Forschungsergebnissen anderer Kenntnis zu nehmen.[45] Art. 15 Abs. 1 lit. b des UNO-Pakt I anerkennt zudem das Recht eines jeden, «an den Errungenschaften des wissenschaftlichen Fortschritts und seiner Anwendungen teilzuhaben». Die Wissenschaftsfreiheit unterstreicht demnach zentrale Kernelemente der digitalen Selbstbestimmung (Datennutzung und Datenaustausch) und unterstützt deren Ansatz, dass durch die Ausschöpfung des Datenpotenzials ein wirtschaftlicher und gesellschaftlicher Mehrwert entsteht.

3.2.3 Digitale Selbstbestimmung als Realisierung bestehender Rechte

Die digitale Selbstbestimmung bettet sich breit in den bestehenden völker- und landesrechtlichen Rahmen ein und ist Ausdruck der gesellschaftlichen Werte und Grundprinzipien der Schweiz. Diese breite Einbettung – gerade auch in nutzen- und wirtschaftsorientierte Grundlagen – macht deutlich, dass es sich bei der digitalen Selbstbestimmung um mehr als nur Fragen des Datenschutzrechts handelt. Sie setzt ein Ökosystem mit geeigneten Rahmenbedingungen voraus, in welchen sich Individuen und

[43] *Häfelin U. et al. (2020)*, «Schweizerisches Bundesstaatsrecht», S. 122-123; *Ghielmini S. et al. (2021)*, «Grund-und Menschenrechte in einer digitalen Welt», S. 41-42.
[44] *Häfelin U. et al. (2020)*, «Schweizerisches Bundesstaatsrecht», S. 196-201.
[45] *Häfelin U. et al. (2020)*, «Schweizerisches Bundesstaatsrecht», S. 161-162; *Ghielmini S. et al. (2021)*, «Grund-und Menschenrechte in einer digitalen Welt», S. 70.

Unternehmen selbstbestimmt gemäss den genannten Grundlagen unserer Rechts- und Gesellschaftsordnung entfalten können.

3.3 Potential von Datenräumen

Die Realisierung der digitalen Selbstbestimmung kann auf verschiedenen Wegen erfolgen. So gibt es bspw. Ansätze, die digitale Selbstbestimmung über die Schaffung und Verwaltung eines persönlichen Datenkontos zu verwirklichen.[46] Dieses Unterkapitel fokussiert auf das Potenzial von vertrauenswürdigen Datenräumen zur Realisierung der digitalen Selbstbestimmung.

3.3.1 Datenräume

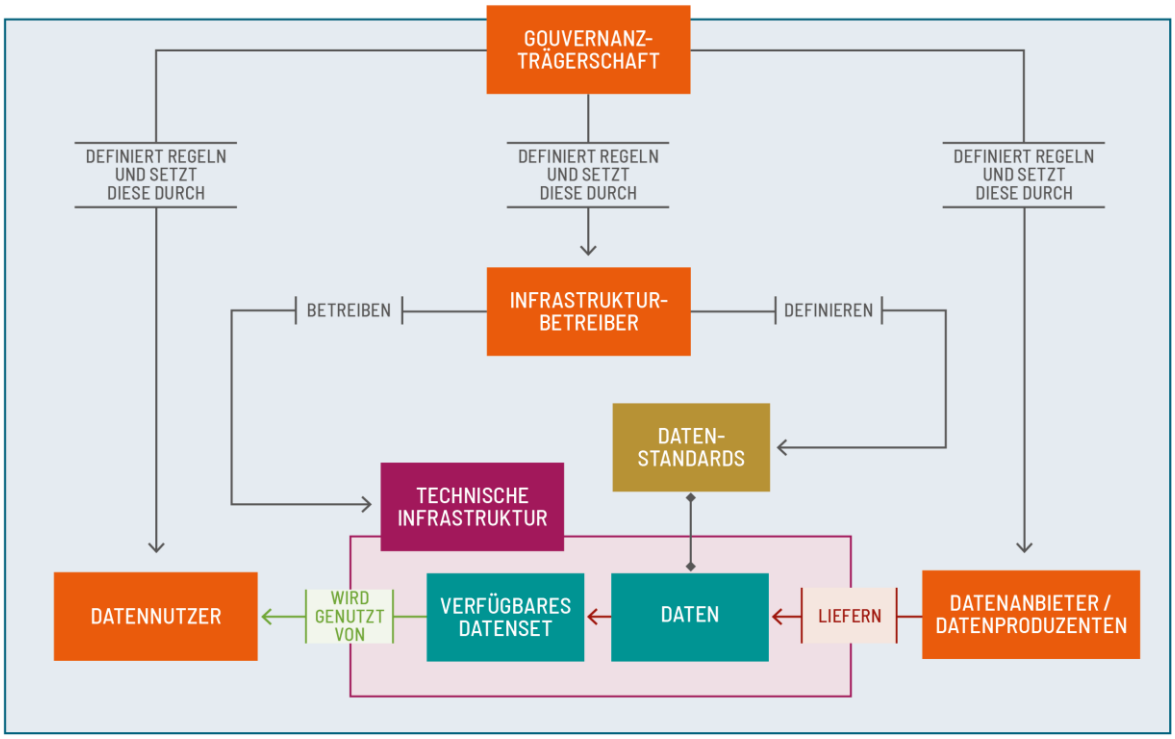
Daten können nur dann gemeinsam genutzt werden, wenn sie einfach und schnell verfügbar gemacht werden. Dazu dienen Datenräume: Durch die direkte Verbindung zwischen Datenangebot und -nachfrage, können Datenräume Individuen, Unternehmen und weiteren Organisationen dabei helfen, einen besseren Datenzugang zu bekommen und neue Datenquellen zu erschliessen.

Ein *Datenraum* (→ Datenraum) kann als organisatorische Struktur mit technischen und physischen Komponenten verstanden werden, die Datennutzer und Datenanbieter mit ihren Datenquellen verbindet und den Zugang, die Bearbeitung und Weiterverwendung von Daten regelt.

Die technischen und physischen Aspekte eines Datenraumes werden dabei durch eine *Dateninfrastruktur* (→ Dateninfrastruktur) abgedeckt. Diese dient dazu sicherzustellen, dass ein Datenraum funktionsfähig ist.[47] Sie soll das Datenangebot und die Datennachfrage auf einer technischen Ebene möglichst effizient, bspw. durch Schnittstellen und gemeinsame Standards, verbinden. Eine Dateninfrastruktur ermöglicht es ebenfalls, mittels gewissen Operationen (bspw. Speicherung, Zuweisung von Metadaten, Transformationen, Import und Export) Daten innerhalb dieses Raumes aus verschiedenen Quellen zirkulieren zu lassen und die gemeinsame Nutzung von Daten durch verschiedene Akteure zu gewährleisten. Gleichzeitig besteht in einem Datenraum immer auch eine *Gouvernanzstruktur*, welche die organisatorischen Aspekte umfasst. Sie definiert die Rahmenbedingungen unter welchen Daten ausgetauscht werden können und legt die Rollen, Pflichten und Rechte aller involvierten Akteure fest.

Entsprechend ist ein Datenraum eine Umgebung, in dem Datenangebot und -nachfrage unter definierten Rahmenbedingungen und Regeln (d.h. einer Gouvernanzstruktur) über eine Dateninfrastruktur zur Nutzung verbunden werden. Für die einzelnen Komponenten eines Datenraumes, siehe Anhang 2.

[46] Bspw. Anwendungen wie *BitsaboutMe AG*, *digi.me* oder *Solid*, welche Daten von Kundinnen und Kunden dezentral speichern und ihnen die vollständige Kontrolle über den Zugang zu diesen Daten überlassen.
[47] Ein Datenraum braucht nicht unbedingt eine eigene physische Infrastruktur. Insbesondere dezentrale funktionierende Datenräume können auch auf Basis bereits bestehender physischer Infrastruktur der beteiligten Akteure aufgebaut werden.



Grafik 3: Modell einer typischen Ausprägung eines Datenraumes

3.3.2 Vertrauenswürdige Datenräume

Die Vorteile von Datenräumen in verschiedenen wirtschaftlichen und gesellschaftlichen Bereichen werden zunehmend erkannt. So setzt sich bspw. auch die EU für die Schaffung von Datenräumen in verschiedenen Sektoren ein, um wirtschaftliche Effizienzgewinne zu realisieren (siehe Kapitel 6.1).[48] Über die Ausschöpfung wirtschaftlichen Potenzials hinaus können Datenräume jedoch, wenn sie vertrauenswürdig organisiert sind, noch erheblichen weiteren Mehrwert generieren. Mit den entsprechenden Vorkehrungen in Daten- und Gouvernanzinfrastruktur können zentrale Elemente der digitalen Selbstbestimmung – wie Verständnis und Wissen über die Datennutzung, die Entscheidungsfreiheit und Handlungsfähigkeit einzelner Akteure – gefördert und gestärkt werden.

Um neben der Funktionsfähigkeit auch die Realisierung der digitalen Selbstbestimmung von Individuen, Unternehmen und der Gesellschaft als Ganzes gewährleisten zu können, braucht es also *vertrauenswürdige Datenräume*. Vertrauenswürdige Datenräume sind eine besondere Kategorie von Datenräumen. Die Vertrauenswürdigkeit eines Datenraums kann insbesondere darauf beruhen, dass die Mitglieder des Datenraums ihre Daten nach eigenem Willen und mit der nötigen Kontrolle zur Verfügung stellen, und die Daten für wirtschaftliche und gesellschaftliche Zwecke genutzt werden können. Damit solche Datenräume entstehen, braucht es bestimmte Grundanforderungen, sog. Grundprinzipien, die eingehalten werden müssen, und die das Vertrauen aller involvierten und betroffenen Akteuren steigern. Datenräume sollen somit das Ökosystem bilden, in dem sich die digitale Selbstbestimmung entfalten kann. Kapitel 4 stellt diese Grundprinzipien vor.

[48] *Europäische Kommission (2018a)*, «Towards a common European Data Space»; *Europäische Kommission (2018b),* «Staff Working Document: Guidance on Sharing Private Sector Data in the European Data Economy».

4 Grundprinzipien für vertrauenswürdige Datenräume

Um vertrauenswürdige Datenräume zu schaffen und damit die digitale Selbstbestimmung realisieren zu können, müssen – wie im Auftrag des Bundesrates ausgeführt – bestimmte Voraussetzungen technischer, rechtlicher, wirtschaftlicher und gesellschaftlicher Art erfüllt werden. Diese Voraussetzungen sind dann erfüllt, wenn ein Datenraum bestimmten Grundanforderungen an die Ausgestaltung, Funktionsweise, Zuteilung von Rechten und Pflichten, etc. entspricht. Diese Grundanforderungen werden in diesem Kapitel als Grundprinzipien dargestellt. Es handelt sich dabei um **Transparenz, Kontrolle, Fairness, Verantwortlichkeit** und **Effizienz**. Anzustreben ist dabei im Sinn des vorliegenden Berichts nicht bloss die Einhaltung der bestehenden rechtlichen Verpflichtungen insbesondere des Datenschutzrechts, sondern es ist im Sinne der Vertrauenswürdigkeit ein hoher Massstab anzulegen.

Neben den fünf Grundprinzipien sollen vertrauenswürdige Datenräume im Sinne der Agenda 2030 für nachhaltige Entwicklung und ihren 17 Nachhaltigkeitszielen (Sustainable Development Goals - SDGs)[49] ökologisch und sozialverträglich ausgestaltet sein, um so zu einer Steigerung unseres Gemeinwohls, der Reduzierung der digitalen Kluft, sowie zur nachhaltigen Nutzung natürlicher Ressourcen und zur Chancengerechtigkeit beizutragen. Die Nachhaltigkeit von Datenräumen ist ein wichtiger Aspekt der Datengesellschaft als Ganzes. Dies wird auch im Rahmen der Grundprinzipien deutlich, die ebenfalls Aspekte der Nachhaltigkeitsthematik umreissen (siehe bspw. die Grundprinzipien Fairness und Effizienz mitsamt Indikatoren in Kapitel 4.3 und 4.5).

Die Vielfältigkeit möglicher vertrauenswürdiger Datenräume und ihrer Zwecke verunmöglicht eine starre Typologie bzw. die Erarbeitung eines einzigen Idealmodells eines vertrauenswürdigen Datenraumes. Vielmehr muss den vielseitigen Herausforderungen und Ausgangslagen unterschiedlicher Datenräume Rechnung getragen werden. Die konkrete Ausgestaltung eines vertrauenswürdigen Datenraums, d.h. *die Gewichtung und Umsetzung der verschiedenen Grundprinzipien und ihren Indikatoren*, wird entsprechend je nach Sektor unterschiedlich ausfallen.

4.1 Transparenz

Transparenz ist eine Grundlage für Vertrauen und schafft sowohl Verständlichkeit als auch Vorhersehbarkeit. Transparenz ermöglicht Nutzerinnen und Nutzern einerseits, das nötige Wissen und Verständnis über die Funktionsweise eines Datenraumes aufzubauen (*Verständlichkeit*) und andererseits die zu erwartenden Abläufe und Konsequenzen klar nachzuvollziehen (*Nachvollziehbarkeit*). Transparenzmassnahmen sollten somit die Indikatoren *Umfang, Wirksamkeit Nachvollziehbarkeit* sowie *Überprüfung* berücksichtigen. In der Folge werden die einzelnen Indikatoren erklärt).[50]

[49] *UNGA (2015)*, «Transforming our World: The 2030 Agenda for Sustainable Development (A/RES/70/1)».
[50] Siehe auch die explizite Anforderung an die Einwilligung nach Art. 6 Abs. 6 revDSG sowie die Art. 19 und 20, 21, 24 Abs. 4, 25 und 26.

Erstens soll der **Umfang** der zur Verfügung stehenden Information ausreichend sein. Konkret müssen Datenraumbetreiber (→ Datenraumbetreiber) die nötigen Angaben und Auskünfte bereitstellen, damit Nutzerinnen und Nutzern sich ein klares Bild der zu erwartenden Datennutzung und -bearbeitung machen können (bspw. mit Informationen über den Datenbearbeitungszweck, den Zugang von Dritten, die Rechte der involvierten Akteure sowie das Businessmodell des Datenraums).[51]

Zweitens sollen die publizierten Informationen **wirksam** sein. Das bedeutet, dass Transparenzauskünfte proaktiv und vor der Datenfreigabe kommuniziert werden und jederzeit einfach und schnell aufzufinden sind.[52] In gewissen Situationen (bspw. bei Sicherheitslücken) ist es zudem wichtig, dass Kommunikationskanäle genutzt werden, welche es erlauben, die betroffenen Akteure möglichst schnell zu informieren (bspw. via Push-Nachricht oder SMS).

Drittens sollen die bereitgestellten Auskünfte **nachvollziehbar** sein. Nutzerinnen und Nutzer müssen die Informationen möglichst leicht verstehen und allfällige Risiken schnell erkennen können. Neben einfacher und verständlicher Sprache und der Sicherstellung der Barrierefreiheit könnten auch dem Zielpublikum angepasste Informationskanäle (bspw. niederschwellige Informationen für durchschnittliche Nutzerinnen und Nutzer neben weitereichenden Dokumentationen für Expertinnen und Experten) und visuelle Hilfsmittel eingesetzt werden.

Viertens soll eine gewisse **Überprüfung** garantiert sein. Nutzerinnen und Nutzer müssen sich darauf verlassen können, dass die zur Verfügung gestellten Informationen möglichst genau und wahrheitsgetreu sind. Um dies sicherzustellen, sind verschiedene Ansätze wie bspw. Transparenzberichte, Zertifizierungen oder unabhängige Prüfstellen denkbar. Diese sind als Ergänzung der Mechanismen, welche im Rahmen der Datenschutzgesetzgebung bestehen, zu verstehen.

Als Beispiel zur Veranschaulichung der Umsetzung der dargelegten Indikatoren dient die Föderation *Edulog* im Bildungsbereich. Bei der Nutzung von Edulog steht ein Dashboard zur Verfügung, wo Nutzerinnen und Nutzer jederzeit einsehen können, welche Informationen an welchen Drittanbieter übermittelt wurden. Die Indikatoren Umfang und Nachvollziehbarkeit werden damit abgedeckt und Edulog fördert die Verständlichkeit und Vorhersehbarkeit, wo und wie die Daten genutzt werden.

4.2 Kontrolle

Das Grundprinzip der Kontrolle erlaubt es, dass Individuen ihre Rechte – wenn sie dies wollen – auch effektiv wahrnehmen können.[53] Es schafft die Möglichkeit, wenn nötig aktiv zu werden und so über blosse Informiertheit hinauszugehen. Kontrolle bedeutet somit einerseits Handlungsfähigkeit, um

[51] Siehe für die datenschutzrechtlichen Anforderungen insbesondere auch Art. 19 und 20 revDSG.
[52] Siehe auch Art. 19 revDSG.
[53] Siehe zu den rechtlichen Möglichkeiten insbesondere Art. 28 ff. ZGB sowie Art. 25 und 32 revDSG.

einzugreifen und andererseits Handlungsfreiheit, um Entscheidungen tatsächlich autonom zu treffen. Um diesem Anspruch gerecht zu werden, sind die Indikatoren *Steuerungsmöglichkeiten, Freiwilligkeit und Wahlfreiheit* sowie *Schutz vor Kontrollverlust* bei Kontrollmassnahmen zu berücksichtigen.

Erstens sollen **Steuerungsmöglichkeiten** gegeben sein, welche es ermöglichen, eine direkte Entscheidung darüber zu fällen, ob und unter welchen Umständen Daten genutzt werden können, für wen diese Daten freigegeben sind und um was für Daten es sich handelt. Wo immer möglich, sollte die Bearbeitung von Daten – insbesondere, wenn sie sensitiver Art sind – auch eingeschränkt werden können (bspw. durch verschiedene Zugriffs- oder Vertraulichkeitsstufen). Um die Handlungsfreiheit garantieren zu können, müssen Entscheidungen zur Datenfreigabe zudem immer zurückgezogen werden können und in der Dauer beschränkt sein. Eine Einwilligung muss deshalb entzogen werden können und bei einem allgemein gefassten Datennutzungszweck periodisch erneuert werden.

Zweitens sollen **Freiwilligkeit** und **Wahlfreiheit** gewährleistet sein. Die Teilnahme an einer gemeinsamen Datennutzung soll auf eigenen Wunsch und ohne äusseren Druck erfolgen. Nutzerinnen und Nutzer sollten ebenfalls die Möglichkeit haben, unter verschiedenen Angeboten frei zu wählen, d.h. auch ohne dass diese Entscheidung zukünftige Möglichkeiten verbaut oder zu Abhängigkeiten führt. Folglich muss es immer möglich sein, ohne Hindernisse Anbieter zu wechseln und die eigenen Daten an neue Anbieter zu übertragen, wie es auch im revDSG mit Artikel 28 neu vorgesehen ist. Echte Wahlfreiheit bedeutet ebenfalls, dass die Entscheidung, wie die eigenen Daten verwaltet werden, auch an Dritte delegiert werden kann, bspw. im Rahmen der Aktivitäten eines Datentreuhänders (→ Datentreuhänder).

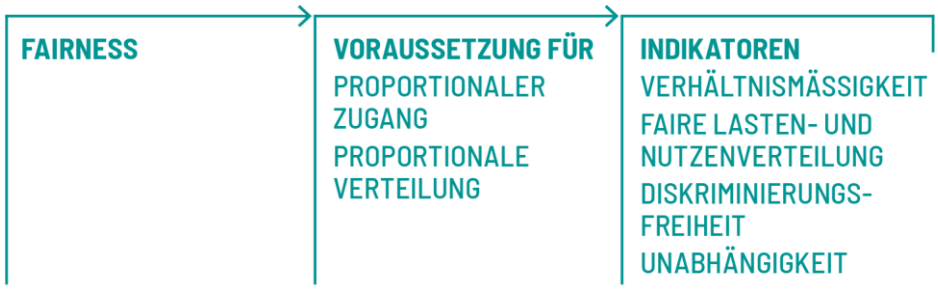
Drittens soll ein effektiver **Schutz vor Kontrollverlust** bestehen. Dies beinhaltet, dass die Integrität des Datenraumes und damit die Sicherheit der Daten durch die nötigen (Cyber-)Sicherheitsvorkehrungen und klare Risikomanagement-Prozesse gewährleistet ist. Ebenso müssen auch verbindliche Abläufe und Eventualmassnahmen zum Schutz der Nutzerinnen und Nutzern bestehen, falls die Sicherheit eines Datenraums kompromittiert wurde (bspw. sofortige Benachrichtigung).[54]

Zur Veranschaulichung des Grundprinzips Kontrolle dient das *Elektronische Patientendossier (EPD)*, welches hohen Wert auf Kontrolle legt und einzelne Indikatoren bereits umsetzt. So haben die Nutzerinnen und Nutzer Steuerungsmöglichkeiten, wem und für wie lange sie ein Zugriffsrecht erteilen wollen. Dieses kann jederzeit widerrufen werden. Auch die Freiwilligkeit und Wahlfreiheit ist gegeben, indem es einem Individuum primär freigestellt ist, ein EPD zu eröffnen und es danach frei bestimmen kann, in welchem Umfang eine Gesundheitsfachperson im Behandlungskontext Zugriff auf die Daten hat.

[54] Siehe die Minimalanforderung nach Art. 24 Abs. 4 revDSG.

4.3 Fairness

Fairness als Grundprinzip garantiert allen Akteuren eine gerechte Behandlung. Hingegen bedeutet Fairness nicht eine Gleichbehandlung innerhalb eines Datenraums. Denn verschiedene Rollen oder Gouvernanzformen können unterschiedliche Pflichten und/oder Privilegien bedeuten. Nichtsdestotrotz müssen gewisse Minimalstandards im Zusammenhang mit dem Zugang zu einem Datenraum und der Verteilung der Vorteile garantiert werden, damit diese im Verhältnis zur Rolle des betroffenen Akteurs stehen. Die identifizierten Indikatoren für das Grundprinzip Fairness umfassen die *Verhältnismässigkeit*, die *Diskriminierungsfreiheit*, eine *faire Lasten- und Nutzungsverteilung* sowie die *Unabhängigkeit*.



Erstens soll die **Verhältnismässigkeit** garantiert sein, sowohl in Bezug auf die Bearbeitung von Daten als auch in der Ausgestaltung der verschiedenen Rollen.[55] Im Zusammenhang mit Daten ist stets zu prüfen, ob eine Alternative zur Nutzung von gewissen Daten vorhanden ist (bei Personendaten bspw. durch *anonymisierte Daten* → Anonymisierung oder *differential privacy* → Differential Privacy) und ob das Prinzip der Datensuffizienz (d.h. nur so viele Daten wie nötig sammeln → Privacy-by-Design) bestmöglich umgesetzt wird. Auch eine allfällige Ungleichbehandlung in einem Datenraum (bspw. aufgrund unterschiedlicher Rollen) muss immer verhältnismässig sein (siehe auch Diskriminierungsfreiheit).

Zweitens sollen **Lasten und Nutzen fair verteilt** sein. Das bedeutet einerseits gleich lange Spiesse, wenn es um den Zugang zu Datenräumen und die Nutzung derer Vorteile geht. Andererseits betrifft dies auch Fragen der Kostenteilung für beteiligte Akteure (sowohl Individuen als auch Unternehmen). Unternehmen können bspw. durch integrierte Lieferketten oder durch Effizienzsteigerungen bei Zulieferern einen Mehrwert erfahren. Denkbar wären auch Ansätze wie Kompensationen für Unternehmen, die ihre Daten zur Verfügung stellen. Solche Ansätze werden jedoch kontrovers diskutiert, umso mehr wenn es sich um monetäre Anreize oder Entschädigungen für Individuen handelt.[56] Dies einerseits aufgrund des Ausnützungspotenzials von verwundbaren und schwächer gestellten Personen sowie des Enttäuschungspotenzials, da der Wert einzelner Datensätze oft viel niedriger ist als erhofft. Andererseits könnte ein monetärer Anreiz zu einer grösseren Datenverfügbarkeit führen und Unternehmen damit einen besseren Datenzugang zu individualisierten Produkten und Dienstleistungen verschaffen.[57]

Drittens sollen vertrauenswürdige Datenräume **diskriminierungsfrei** operieren. Dies betrifft sowohl Fragen des Zugangs zu Daten als auch Fragen der repräsentativen Datenbasis für Entscheidungen. Datenraumbetreiber müssen sicherstellen, dass alle involvierten Akteure nach objektiven und fairen

[55] Siehe auch Art. 6 Abs. 2 revDSG.
[56] *Collovà P. et al. (2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung», S. 12.
[57] Siehe dazu die *BitsaboutMe AG* <https://bitsabout.me/de/> (Zugriff am 02.01.2022), wo wer seine Daten zu Forschungszwecken mit akademischen Institutionen oder Unternehmen teilt, Geld verdienen kann.

Kriterien Zugang zu den nötigen Daten erhalten. Im Zusammenhang mit Datenqualität (→ Datenqualität) können unzureichende Daten zu einem verzerrten digitalen Bild eines Individuums führen, sodass das physische Selbst mit dem digitalen Selbst nicht mehr übereinstimmt (→ Data Bias). Dies kann in Bezug auf bestimmte Handlungen im digitalen Raum diskriminierend wirken, da sich das digitale Selbst rein über die von ihm gesammelten Daten definiert. Weiter ist eine hohe Datenqualität wichtig, um diskriminierende Auswirkungen der Datennutzung auf gefährdete Gruppen zu verringern. Datenraumbetreiber müssen somit sicherstellen, dass Ungleichheiten abgebaut werden, wenn Daten in Situationen mit bereits bestehender struktureller Diskriminierung verwendet werden.[58]

Viertens soll der Betrieb eines Datenraumes **unabhängig**, d.h. von allfälligen Interessenskonflikten befreit und gegen Machtmissbrauch geschützt sein. Die für die Technik und die Regelsetzung verantwortlichen Stellen dürfen nicht einseitig von bestimmten Akteuren abhängig sein. Die Gouvernanz eines Datenraums muss also so angelegt sein, dass ein Datenraumbetreiber in der Ausübung transparent ist und darüber allenfalls auch Rechenschaft ablegen muss. Zudem sollte sichergestellt werden, dass Datenraumbetreiber keine anderen Interessen und Zwecke verfolgen als diejenigen, die in den Statuten festgelegt sind.[59] Auch die Wahl der Architektur kann einen Einfluss haben: Eine dezentrale bzw. verteilte Nutzungsarchitektur kann das Potenzial für einen Machtmissbrauch unter Umständen erheblich verringern. Weiter trägt die Repräsentation aller Akteure zur Unabhängigkeit eines Datenraumes bei. Insbesondere für Akteure mit kleinem oder limitierten Einfluss (bspw. KMUs oder Einzelpersonen) können einfache und transparente Repräsentationsverfahren (bspw. durch Beiräte) die inklusive Entscheidungsfindung stärken.

Die *nationale Dateninfrastruktur im Stromsektor (Datahub-Strom)*[60] sowie die *Nationale Datenvernetzungsinfrastruktur Mobilität* (NADIM) dienen als Beispiele, wie die Indikatoren für das Grundprinzip Fairness umgesetzt werden können. Der Datahub-Strom soll allen Akteuren einen diskriminierungsfreien klar geregelten Zugang zur Dateninfrastruktur im Stromsektor ermöglichen und die NADIM, welche als neutrale und unabhängige öffentliche Anstalt ausgestaltet ist, garantiert so die Unabhängigkeit.

4.4 Verantwortlichkeit

Das Grundprinzip der Verantwortlichkeit ermöglicht es, dass Rechte und Pflichten zugeordnet und eingefordert werden können. Die identifizierten Indikatoren für das Grundprinzip Verantwortlichkeit umfassen klare *Gouvernanzmechanismen und Durchsetzungsmechanismen*.

[58] *Findlay M. und Remolina N. (2021)*, «The Paths to Digital Self-Determination: A Foundational Theoretical Framework", S. 27-28.
[59] *Collovà P. et al. (2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung»; *Blankertz A. (2020)*, «Designing Data Trusts: Why We Need to Test Consumer Data Trusts Now»; *Schneider I. (2019)*, «Governance der Datenökonomie: Politökonomische Verfügungsmodelle zwischen Markt, Staat, Gemeinschaft und Treuhand».
[60] *BFE (2021)*, «Datahub Schweiz: Kern zukünftiger Dateninfrastruktur digitalisierter Strom- und Gasmärkte».

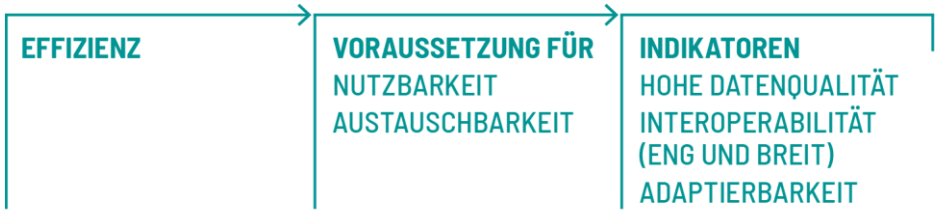
Erstens setzen klare **Gouvernanzmechanismen** voraus, dass die organisatorische Funktionsweise eines vertrauenswürdigen Datenraumes für alle Akteure definiert und bekannt ist. Dabei können verschiedene Gouvernanzformen existieren (siehe Anhang 2). Unabhängig davon, müssen die Rechte und Pflichten für die verschiedenen Akteure sowie die Entscheidungsstrukturen innerhalb eines Datenraumes klar definiert sein. Idealerweise werden zudem die grundlegenden Mechanismen sowie Rollen und Verantwortlichkeiten festgelegt (bspw. in verbindlichen Statuten oder Verträgen oder in spezifischen Fällen durch Orientierungshilfen wie Checklisten, oder in bestimmten Fällen durch gesetzliche Vorschriften).

Zweitens sollen **Durchsetzungsmechanismen** bestehen, welche es den involvierten Akteuren erlauben, die Einhaltung der im Datenraum gültigen Vorgaben einzufordern, auch wo es nicht um Verstösse gegen anwendbares Recht geht.[61] Dies beinhaltet auch, dass Massnahmen innerhalb eines Datenraums (bspw. der Ausschluss eines Akteurs) klar und nachweisbar begründet werden. Akteure, die mit einer Massnahme nicht einverstanden sind, sollten zudem einfache Möglichkeiten haben, sich dagegen zu wehren, um langwierige Abläufe möglichst zu verhindern. Diese können unterschiedlich ausgestaltet sein und von internen Beschwerdeverfahren bis zu vorgängig definierten externen Schlichtungsstellen reichen. In besonderen Fällen, bspw., wenn höchstsensitive Daten betroffen sind, könnte die Einrichtung einer unabhängigen Beschwerdestelle zusätzliches Vertrauen schaffen.

Sowohl das Elektronische Patientendossier (*EPD)* wie auch die Föderation *Edulog* sehen Massnahmen zur Verantwortlichkeit vor. So enthält das EPD einen Durchsetzungsmechanismus: Wer unberechtigt, d.h. ohne von der Nutzerin oder dem Nutzer entsprechende Zugriffsrechte erhalten zu haben, in einer Situation, die keine medizinische Notfallsituation ist, auf das EPD zugreift, wird mit Busse bestraft. Edulog schafft mit vertraglichen Regelungen zwischen den teilnehmenden Dienstleistungsanbietern transparente Gouvernanzmechanismen, um die persönlichen Daten der Nutzerinnen und Nutzer zu schützen.

4.5 Effizienz

Das fünfte Grundprinzip betrifft die Effizienz. Datenräume sind nur dann nützlich, wenn die relevanten Daten ohne Probleme ausgetauscht und genutzt werden können. Um die Effizienz eines Datenraumes zu definieren, werden die Indikatoren *Hohe Datenqualität*, *Austausch*, *Interoperabilität* und *Adaptierbarkeit* betrachtet.



Erstens sollen Daten in einer genügend **hohen Qualität** verfügbar sein oder es soll zumindest ausgewiesen werden, welche Genauigkeit oder Qualität die jeweiligen Daten haben.[62] Daten müssen direkt verwendet werden können, ohne dass zusätzliche Massnahmen zur Steigerung der Datenqualität

[61] Siehe dazu Art. 32, 41 und 49 revDSG.
[62] Der Begriff der «hohen Qualität» hängt massgeblich vom bestimmten Zweck der Datennutzung ab. Einen Ausweis über die Qualität oder Genauigkeit der jeweiligen Daten ist deshalb essentiell, indem bspw. erkenntlich ist, von wem sie erzeugt oder wann sie zuletzt ergänzt wurden.

nötig sind. Eine hohe Datenqualität bedingt, dass Daten möglichst vollständig und intakt sind – einerseits strukturell, also in Bezug auf den Umfang der Daten, andererseits inhaltlich, d.h. in Bezug auf die beschriebene Information. Zur Sicherstellung der nötigen Datenqualität sind klare Verfahren und Prozesse zum Qualitätsmanagement nötig. Datenraumbetreiber müssen klare Standards setzen, die nötigen Verfahren regelmässig überprüfen und Verantwortlichkeiten bezüglich Datenunterhalt klar festsetzen. Ebenfalls können Datenraumbetreiber selbst, bspw. durch Datenbearbeitung, zur Datenqualität beitragen.

Zweitens soll die **Interoperabilität** (→ Interoperabilität) zwischen den Akteuren eines Datenraums sowie zwischen verschiedenen Datenräumen garantiert sein. Damit Daten effizient genutzt werden können, müssen Redundanzen und Diskrepanzen innerhalb und zwischen Systemen reduziert werden. Dabei wird generell zwischen verschiedenen Ebenen der Interoperabilität unterschieden (siehe Kapitel 6.3).

Drittens sollen vertrauenswürdige Datenräume **adaptierbar** ausgestaltet sein. In einem dynamischen Umfeld müssen sie sich schnell ändernden Gegebenheiten flexibel anpassen. Ein Zuwachs an Akteuren oder die Integration neuer Datenquellen sollen keine Kompromisse in Bezug auf die Vertrauenswürdigkeit und Funktionalität nach sich ziehen. Entsprechend sollen Gouvernanzmechanismen und technische Infrastruktur zukunfts- und wachstumsfähig ausgestaltet werden. Zusätzlich gilt es zu beachten, dass sich das Risikoprofil eines Datenraumes durch externe Einflüsse ebenfalls verändern kann. Entsprechend muss regelmässig evaluiert werden, ob die aktuellen Massnahmen angemessen sind, allenfalls auch unter Einbezug von Dritten (bspw. Auditoren oder anderen Datenraumbetreibern).

Zur Veranschaulichung des Grundprinzips Effizienz kann die Nationale Datenvernetzungsinfrastruktur Mobilität (NADIM) genannt werden. Als zentrale Infrastruktur ermöglicht sie die Nutzung möglichst vieler, für die multimodale Mobilität relevanter Daten. Sie garantiert Interoperabilität, um den Datenaustausch und die Datennutzung für alle Akteure (insbesondere Unternehmen) möglichst effizient zu gestalten. Ähnlich dazu ist der Datahub-Strom ausgestaltet, für welchen ebenfalls ein hohes Mass an Standardisierung angestrebt wird.

4.6 Zwischenfazit

Die fünf dargestellten Grundprinzipien und die dazugehörigen Indikatoren stellen den Kern der Antwort auf das Mandat des Bundesrates dar, die Voraussetzungen für die Schaffung vertrauenswürdiger Datenräume darzulegen. Sie sind als Leitlinien zu verstehen und können als Handlungsanstoss für die Gesamtarchitektur, die Gouvernanz und die technische Gestaltung eines vertrauenswürdigen Datenraumes dienen. Im Anhang des Berichts (siehe Anhang 3) sind für jeden oben genannten Indikator *Empfehlungen* festgehalten. Grundprinzipien, Indikatoren und Empfehlungen bilden den Orientierungsrahmen für die konkrete Umsetzung und können für zukünftige Arbeiten an einem freiwilligen Verhaltenskodex zur Schaffung und dem Betrieb von vertrauenswürdigen Datenräumen dienen (siehe Kapitel 7.1). Sie sind folglich als Werkzeugkasten für weitere Arbeiten zu verstehen.

5 Datenräume in der Schweiz

In der Schweiz sind in diversen Sektoren Datenräume im Begriff zu entstehen. In diesem Kapitel werden die Datenraumprojekte Mobilität, Energie, Finanzen, Gesundheit und Bildung vorgestellt, wobei es sich um eine Auswahl handelt. Es sei an dieser Stelle erwähnt, dass auf nationaler Ebene bereits einzelne Datenräume bestehen, so bspw. der Geodatenraum.[63]

Bei der Darstellung soll auch herausgearbeitet werden, wie die digitale Selbstbestimmung beim Aufbau dieser sektorspezifischen Datenräume in der Schweiz eine Rolle spielen kann. Es gilt dabei zu beachten, dass die ausgewählten Beispiele alle eine vertrauenswürdige Datennutzung beabsichtigen und somit eine Affinität zur digitalen Selbstbestimmung aufweisen. Dies ist nicht bei allen Datenraumprojekten in der Schweiz der Fall.

5.1 Mobilität

Mobilitätsdaten sind sowohl für das Funktionieren des Mobilitätssystems als Ganzes wie auch in der Entwicklung neuer Mobilitätsdienstleistungen unabdingbar. Sie erfüllen somit eine wichtige Doppelfunktion: einerseits werden sie benötigt, um ein funktionierendes Gesamtverkehrssystem zu ermöglichen und andererseits dienen sie als Innovationstreiber zur Verbesserung und Effizienzsteigerung. So ermöglichen allgemein verfügbare Mobilitätsdaten eine bessere Abstimmung zwischen verschiedenen Verkehrsmitteln, eine optimale Auslastung der Kapazitäten sowie Angebote, die besser auf die Kundenbedürfnisse ausgerichtet sind.

Heute sind rund 90% der Fahrten monomodal, d.h. Reisende benutzen nur *ein* Verkehrsmittel, um an ihr gewünschtes Ziel zu kommen. Die durchschnittliche Auslastung des öV liegt bei 30% und die Besetzung von Autos bei ca. 1.5 Personen.[64] Mit der entsprechenden Datenbasis könnten freie Kapazitäten effizienter genutzt und die Kombination verschiedener Verkehrsmittel (wie öV, motorisierter Individualverkehr, Sharing-Autos/-Bikes/-Miniscooter, Mitfahrgelegenheiten, Taxis sowie Fuss- und Veloverkehr) gefördert werden. Die koordinierte Nutzung der Kapazitäten könnte damit auch einen Beitrag zur Erreichung der verschiedenen Ziele für Verkehr, Klima und Umwelt leisten.

Zentrale Voraussetzung für eine vernetzte Mobilität ist, dass die entsprechenden Daten und Dienste zu den verschiedenen Mobilitätsangeboten einfach zu finden und zu verwenden sind. Der Bundesrat hat das UVEK (BAV) diesbezüglich damit beauftragt, die Rechtsgrundlagen für eine schrittweise Realisierung einer **Nationalen Datenvernetzungsinfrastruktur Mobilität (NADIM)** zur Bereitstellung und Nutzung von Mobilitätsdaten zu schaffen. Die NADIM soll Mobilitätsdaten unterschiedlicher Mobilitätsanbieter miteinander vernetzen, um die Grundlagen dafür zu schaffen, dass der Zugang zur Gesamtmobilität für die Reisenden einfacher und effizienter gestaltet werden kann.

Die NADIM verbindet Anbieter von Mobilitätsdienstleistungen und Endkundensystemen mit verschiedenen relevanten Datenquellen und Datensammlungen. Die Nutzung durch Datenlieferanten ist freiwillig. Datenlieferanten haben die Wahl über die Kerndaten hinaus auch weitere, komplementäre Daten über die NADIM bereitzustellen. Die Betreiberin der NADIM nimmt dabei die Rolle der

[63] Siehe für weitere Informationen <https://www.swisstopo.admin.ch/de/wissen-fakten/geoinformation/geo-daten-infrastruktur.html> (Zugriff am 04.03.2022).
[64] *BAV (2022)*, «Erläuternde Bericht zum Bundesgesetz über die Mobilitätsdateninfrastruktur (MODIG)», S. 6.

Datenraumbetreiberin ein und soll sowohl den technischen Betrieb als auch die Gouvernanz sicherstellen.

Akteure	- Anbieter von Mobilitätsdienstleistungen (bspw. öV und private Anbieter) - Betreiber von Endkundensystemen (bspw. von Webdiensten und Apps) - Öffentliche Anstalt als Betreiberin der NADIM (Infrastruktur und Gouvernanz)
Datenarten	- Sachdaten: bspw. Geodaten, Fahrpläne, Verfügbarkeiten von Fahrzeugen und Angeboten, Ankunfts- und Abfahrzeiten in Echtzeit - Personendaten spielen in einem ersten Schritt eine untergeordnete Rolle
Datenzweck	- Verkehrsmanagement (Kapazitätsauslastung und Benutzerlenkung) - Innovationstreiber und Effizienzsteigerung von Mobilitätsdienstleistungen - Förderung der multimodalen bzw. vernetzten Mobilität
Infrastruktur	- Dateninfrastruktur, welche eine standardisierte Nutzung der Daten ermöglicht insbesondere durch die Schaffung von Schnittstellen (sog. APIs)
Gouvernanz	- Die Betreiberin der NADIM ist eine staatliche, unabhängige und unparteiische nicht-gewinnorientierte Anstalt des Bundes - Auch wenn die Daten in der Regel dezentral gespeichert werden, ist die Gouvernanzstruktur durch die Betreiberin zentral organisiert

5.2 Energie

Daten spielen auch eine zentrale Rolle für die Transformation des Schweizer Energiesektors. Der Klimawandel und das Netto-Null Ziel der Schweiz benötigen fundamentale Veränderungen im Strom- und Gassektor, in der Mobilität und in der Wärmeversorgung bzw. im Gebäudebereich. Ein zentraler Faktor für die Schweiz ist der Ausbau erneuerbarer Energien. Sie verändern die Erzeugungs- und Verbrauchsstruktur im Energiesektor enorm. Anstatt wenige zentrale Erzeugungseinheiten an das Energienetz anzubinden, gilt es in Zukunft immer mehr dezentrale Erzeuger einzubinden und deren Energie über die Netzinfrastruktur an die verschiedenen Endverbraucher zu verteilen.[65]

Verfügbare, qualitativ hochwertige Daten leisten vor dem Hintergrund dieses dezentral geprägten Energiesystems einen entscheidenden Beitrag: Sie ermöglichen eine bessere Planung des Systembetriebs, feingranulare Abrechnung der Energieflüsse und den so wichtigen Einbezug der Konsumentinnen und Konsument, bspw. bei der Zusammenstellung ihres Energiemix. Dazu bedarf es einer Dateninfrastruktur, die den erforderlichen Austausch der dazu notwendigen Energiedaten bewerkstelligen kann und die Transparenz im System erhöht. Historisch gewachsen und wenig zukunftskompatibel findet im Stromsektor der Datenaustausch zwischen den für die Datenaufnahme bzw. Messung verantwortlichen Verteilnetzbetreibern und Dritten heute noch auf bilateralem Wege statt. Gerade für kleine Marktakteure, Konsumentinnen und Konsumenten und nicht zuletzt die Wissenschaft ist dieser Zustand mehr als nur hemmend. Er wirkt als Markt-, Innovations- und Digitalisierungsbarriere für ein nachhaltiges ausgestaltetes Energiesystem. Darüber hinaus ist auch der Gassektor sowie andere Sektoren von ähnlichen Herausforderungen betroffen.

Mit der Botschaft zum Mantelerlass über eine sichere Stromversorgung mit erneuerbaren Energien in der Schweiz soll der Aufbau einer nationalen Dateninfrastruktur im Stromsektor erfolgen, deren Kernelement ein Datahub ist (Datahub Strom). Dieser Datahub stellt eine nationale Vernetzung der

[65] *BFE (2021)*, «Datahub Schweiz: Kern zukünftiger Dateninfrastruktur digitalisierter Strom- und Gasmärkte».

Datensilos im Strommarkt sicher, indem er nur bestimmte statische Daten zentral enthält, um die stromwirtschaftlichen Prozesse zu automatisieren, die Datenqualität und Markttransparenz zu verbessern sowie die Markteffizienz wesentlich zu steigern. Die so wichtigen Messdaten zu Verbrauch, Produktion und Speicherung verbleiben dezentral. Der Zugang zu den Daten wird national einheitlich sichergestellt und die Rechte der Konsumentinnen und Konsumenten als Datenproduzenten werden gestärkt. Mittels standardisierter Schnittstelle können Marktakteure direkt, einheitlich und fair auf die Daten zugreifen, sofern sie von Konsumentinnen und Konsumenten dazu berechtigt wurden. Im Sinne des öffentlichen Interesses und der Transparenz können gewisse aggregierte Daten zum Stromsystem über den Datahub verfügbar gemacht werden. Der Vorschlag zur nationalen Dateninfrastruktur im Stromsektor setzt erstmals regulatorische Leitplanken für die zukünftige Ausbildung eines vertrauenswürdigen Datenraumes im Stromsektor. Perspektivisch könnte auch für den Gassektor ähnliches aufgebaut werden.

Akteure	- Endkunden, Konsumentinnen und Konsumenten - Verteilnetzbetreiber (bspw. Stadtwerke) - Energielieferanten - Energiedienstleister und Start-Ups (bspw. Flexibilitätsdienstleister) - Hochschulen und Innovatoren - Betreiber Datahub
Datenarten	- Daten zu Stromverbrauch, -produktion und Speicherung - Daten zu verfügbaren Flexibilitäten - Technische Daten, bspw. zu Anschlussleistung - Datenaggregate auf Stufe Gemeinde, Kanton, Bund
Datenzweck	- Verbesserung der Prognose- und Abrechnungsprozesse - Energieplanungen und Statistiken - Bilanzierung und Betriebsplanung - Unterstützung von Wissenschaft und Innovation - Energieeffizienz und andere Dienstleistungen
Infrastruktur	- Dateninfrastruktur, welche eine standardisierte Nutzung der Daten ermöglicht insbesondere durch Schnittstellen (sog. APIs) - Zentrale Register, wie bspw. Benutzerregister, Messstellenregister oder Bedarfsträgerdatenregister
Gouvernanz	- Von Strombranche unabhängiges, privates Konsortium als Dateninfrastrukturbetreiberin, schweizerisch beherrscht, neutral im Markt - Vorgaben auf Stufe Verordnung geplant - Aufsicht der Regeleinhaltung und Kosten durch Regulator

5.3 Gesundheit

Die Notwendigkeit der Kommunikation zwischen und die Involvierung von verschiedenen Akteuren prägen das Schweizer Gesundheitswesen. Das **elektronische Patientendossier (EPD)** stellt deshalb einen wichtigen Meilenstein dar. Behandlungsrelevante Informationen der Patientin oder des Patienten werden im EPD bereitgestellt und stehen so jederzeit zum Abruf bereit.

Das EPD ist ein virtuelles Dossier, welches dezentral abgelegte behandlungsrelevante Daten aus der Krankengeschichte einer Patientin oder eines Patienten den behandelnden Gesundheitsfachpersonen

zugänglich macht (bspw. Labordaten, Rezepte, radiologischer Bericht). Die Patientin oder der Patient hat zudem die Möglichkeit, eigene Daten (bspw. Informationen über Allergien oder Kontaktdaten von im Notfall zu benachrichtigenden Personen) in das elektronische Patientendossier hochzuladen und diese damit den behandelnden Gesundheitsfachpersonen zugänglich zu machen.[66] Das EPD verbindet somit die *Gesundheitsfachpersonen* und die jeweiligen *Gesundheitseinrichtungen* mit den Patientinnen und Patienten.

Akteure	- Patientin und Patient - Gesundheitsfachpersonen mit ihren jeweiligen Gesundheitseinrichtungen - (Stamm-)Gemeinschaften (= Anbieter des EPD), organisatorische Zusammenschlüsse von Gesundheitsfachpersonen und deren Einrichtungen - Herausgeber von Identifikationsmitteln - Plattformanbieter (stellen EPD-Betriebssysteme zur Verfügung) - Anbieter von Primärsystemen - Zertifizierungsstellen - Schweizerische Akkreditierungsstelle - Bund (Aufbau und Betrieb zentraler technischer Komponenten, Information der Bevölkerung, Evaluation des EPDG, Finanzhilfen für den Aufbau und die Zertifizierung der (Stamm-)Gemeinschaften) - eHealth Suisse (Kompetenz- und Koordinationsstelle Bund und Kantone) - Kantone
Datenarten	- Besonders schützenswerte Personendaten (→ Personendaten, besonders schützenswert): Behandlungsrelevante Gesundheitsdaten
Datenzweck	- Verbesserung der Qualität der medizinischen Behandlung - Erhöhung der Patientensicherheit - Vereinfachung des Behandlungsprozesses und Effizienzsteigerung des ganzen Gesundheitssystems - Förderung der Gesundheitskompetenz der Patientin und des Patienten
Infrastruktur	- Zertifizierte EPD-Anbieter bieten die technische und organisatorische Infrastruktur für das EPD. Sie ermöglichen unter anderem die Anbindung zwischen dem EPD-Anbieter und der IT-Struktur der Gesundheitseinrichtung. Der Bund führt zudem die zentralen Abfragedienste, welche die für die Kommunikation zwischen (Stamm-)Gemeinschaften und Zugangsportalen notwendigen Referenzdaten liefern.
Gouvernanz	- Das EPD wird von dezentralen (Stamm-)Gemeinschaften angeboten. Diese werden vor der Aufnahme des Betriebs zertifiziert und regelmässig kontrolliert. - Das Bundesgesetz über das elektronische Patientendossier (EPDG) legt dabei die Rahmenbedingungen für den Aufbau und die Verbreitung des elektronischen Patientendossiers in der Schweiz fest. - Transnationale Ausrichtung durch die Verwendung von international anerkannten Standards wie IHE-Profile, FHIR etc.

[66] Art. 2 lit. a EPDG.

5.4 Finanzen

Veränderte Kundenbedürfnisse, neue Akteure sowie innovative Technologien fordern die etablierten Finanzmarktinstitute (unter anderem Banken) heraus. Vor diesem Hintergrund wird **Open Finance** die Finanzbranche nachhaltig verändern.[67] Open Finance basiert auf dem Prinzip des Finanzdatenaustauschs über standardisierte Schnittstellen auf Wunsch der Kundinnen und Kunden.[68]

Das Potenzial von Open Finance ist vielfältig. Geschäfts- aber auch Privatkunden können von einem Gesamtüberblick der eigenen finanziellen Situation profitieren, indem verschiedene Konten bei diversen Anbietern in einer Ansicht integriert werden. Open Finance ermöglicht somit ein verbessertes Kundenerlebnis dank nahtlosem Übergang zwischen unterschiedlichen Angeboten. Aber auch Banken und Drittanbieter profitieren: Dank des gegenseitigen Datenaustauschs können Banken auf Daten Dritter zugreifen und damit innovative Produkte anbieten. Drittanbietern wie FinTechs bietet Open Finance die Möglichkeit, ihre Produkte und Dienstleistungen mit geringerem technischem und regulatorischem Aufwand zu lancieren.[69]

Bei dieser Förderung des Finanzdatenaustausches stellen sich verschiedene Herausforderungen. Zu nennen sind insbesondere die Standardisierung von Schnittstellen, die Abwehrhaltung etablierter Akteure, die zögern, Kundendaten an potenzielle Wettbewerber weiterzugeben oder die Reputationsrisiken, die mit einem Ausfall von Drittanbietern verbunden sind.

Open Finance verbindet Kundinnen und Kunden über Drittanbieter mit ihren Banken, Versicherungen und anderen Finanzinstituten. Und umgekehrt: Finanzdienstleister können so auch Dienstleistungen von Dritten anbieten. Drittanbieter nehmen dabei eine Scharnier- und Intermediär-Funktion wahr. Ihre Zwischenstellung führt dazu, dass Kundinnen und Kunden nicht einzeln mit den unterschiedlichen Banken, Versicherungen und anderen Finanzinstituten in Kontakt treten müssen, sondern ihre persönlichen finanziellen Angelegenheiten und Geschäfte über einen einzigen Drittanbieter oder über eine einzige Bank mehrere Dienstleistungen abwickeln und verwalten können.

Akteure	- Kundinnen und Kunden - Finanzmarktinstitute (bspw. Banken und Versicherungen) - Drittanbieter (Services & Technische Infrastruktur Provider) - Branchenverbände für Standardsetting
Datenarten	- Personendaten: Bankdaten aber auch Daten zu Versicherungen, Wertpapieranlagen, Hypothekarkrediten oder Pensionskassen inkl. Positions- und Transaktionsdaten, die jedoch nicht zwingend einen Personenbezug aufweisen.
Datenzweck	- Förderung der Kontrolle von Kundinnen und Kunden über ihre Finanzdaten - Stärkung der Wettbewerbsfähigkeit des Schweizer Finanzplatzes, insbesondere durch die Verbindung verschiedener Dienstleistungen
Infrastruktur	- Die technische Infrastruktur wird von etablierten Finanzmarktinstituten, den Drittanbietern und anderen Infrastrukturanbietern zur Verfügung gestellt und verwaltet.

[67] *SBVg (2020)*, «Open Banking: Eine Auslegeordnung für den Schweizer Finanzplatz», S. 7.
[68] Open Finance birgt grosses Potenzial, siehe <https://www.sif.admin.ch/sif/de/home/dokumentation/fokus/open-finance.html> (Zugriff am 03.02.22).
[69] *SBVg (2020)*, «Open Banking: Eine Auslegeordnung für den Schweizer Finanzplatz», S. 7-8.

	- Die offene Standardisierung von Schnittstellen (APIs) stellt dabei eine wichtige Voraussetzung für das reibungslose Andocken von Drittparteien und den fehlerfreien Austausch von Daten dar.
Gouvernanz	- Gegenwärtig gibt es zumindest in der Schweiz, anders als in der EU, keine gesetzliche Verpflichtung für Finanzinstitute, Kundendaten über standardisierte Schnittstellen mit Drittanbietern auszutauschen. Der Bundesrat hat das EFD/SIF beauftragt, weiterhin den Handlungsbedarf zur Förderung und Ausweitung von Open Finance regelmässig zu prüfen. - Ein gemeinsames Rollenverständnis für die weitere Zusammenarbeit wurde zusammen mit dem Privatsektor entwickelt, insbesondere im Hinblick auf die API-Standardisierung.

5.5 Bildung

Die Selbstbestimmung steht in der Bildung in einem besonderen Kontext. Einerseits trägt sie ihren Teil dazu bei, die Lernenden – und damit die gesamte Gesellschaft – zu einem mündigen Umgang mit Daten zu befähigen. Die digitalen Kompetenzen sind in den Lehrplänen sämtlicher Bildungsstufen integriert. Andererseits werden im Bildungssektor selbst personenbezogene Daten schulpflichtiger Kinder und Jugendlichen bearbeitet. Sie haben Anspruch auf besonderen Schutz ihrer Unversehrtheit und auf die Förderung ihrer Entwicklung. Entsprechend wichtig ist es, dass die verantwortlichen Akteure im Umgang mit Daten sensibilisiert und befähigt sind.

Im Bildungswesen liegt aktuell eine der grössten Herausforderungen für die digitale Selbstbestimmung in der Klärung des Verhältnisses zwischen privaten und öffentlichen Akteuren. Besonders relevant ist diese Frage im Zusammenhang mit grundlegenden Infrastrukturdiensten (Clouddienste, etc.). Eine kleine Anzahl marktzentraler Konzerne übt mit ihren proprietären Ökosystemen in vielen Fällen faktische Kontrolle über Daten aus. Eine weitere Herausforderung ist der Aufbau schweizweiter organisatorisch-struktureller Lösungsansätze. Diese haben zum Ziel, die Kontrolle über Daten zu stärken und überhaupt erst den Zugang zu bzw. den Austausch von Daten zu ermöglichen (Datenföderationen, Interoperabilitätsstandards, flächendeckende Identitätslösung). Verschiedene Ansätze sind in Planung, um die genannten Herausforderungen anzugehen. Neben der Schaffung einer Datenföderation in der Berufsbildung[70], welche den Datenaustausch zwischen einzelnen Akteuren technisch ermöglichen soll, sind auch Bestrebungen zur Entwicklung einer schweizweiten Datennutzungspolitik in der Bildung[71] am Laufen. Die Herausforderung besteht in der Anschlussfähigkeit zu anderen Politikbereichen.

Das am weitesten fortgeschrittene Projekt im Rahmen der Umsetzung der digitalen Selbstbestimmung im Bildungsbereich ist **Edulog**. Edulog bringt als Föderation Kantone, Gemeinden und Schulen zusammen, welche die digitalen Identitäten für ihre Schulangehörigen ausstellen. Dies ermöglicht es den Nutzerinnen und Nutzer mittels ihrer kantonalen, kommunalen oder schulischen digitalen Identität und dem von Edulog zur Verfügung gestellten Pseudonym, verschiedene Online-Dienstleistungen in Schulen und Ausbildungen (Lernapplikationen, Bibliothekzugänge etc.) zu nutzen. Edulog beabsichtigt so einen Vertrauensraum zu schaffen.

[70] Siehe <https://www.educa.ch/taetigkeiten/datenfoederation-der-berufsbildung> (Zugriff am 03.01.2022).
[71] Siehe <https://www.educa.ch/taetigkeiten/fachstelle-datennutzung> (Zugriff am 03.01.2022); *EDUCA (2021)*, «Digitalisierung in der Bildung: Bericht im Auftrag des SBFI und der EDK im Rahmen des Bildungsmonitorings».

Akteure	- Kantone, Gemeinden oder Schulen, welche die digitalen Identitäten für ihre Schulangehörigen ausstellen und authentifizieren (Identitätsanbieter) - private oder öffentliche Anbieter von Online-Diensten (bspw. Online-Angebote von Lehrmittelverlagen, Cloud-Lösungen oder Lern-Apps), mit denen im Unterricht gearbeitet wird (Dienstleistungsanbieter) - Föderation Edulog, die das Pseudonym zur Verfügung stellt
Datenarten	- Personendaten: Die digitale Identität der Kantone, Gemeinden und Schulen setzt sich aus verschiedenen Attributen (bspw. Name, Geburtsdatum, Rolle, etc.) zusammen.
Datenzweck	- Vereinfachung des Zugangs zu Online-Diensten in Schulen und Unterricht - Erleichterung der Mobilität im Bildungsraum
Infrastruktur	- Der technische Betrieb von Edulog wird von einem privaten Akteur (ELCA Informatik AG) verwaltet, d.h. die Identitäts- und Dienstleistungsanbieter werden über eine zentrale IT-Infrastruktur miteinander verbunden. - Edulog schaltet sich als Vermittler der Attribute zwischen die Identitäts- und Dienstleistungsanbieter.
Gouvernanz	- Edulog ermöglicht eine kontrollierte, zweckgebundene Datennutzung in Bezug auf den Zugang zu Online-Diensten. - Edulog als Föderation speichert mit Ausnahme eines generierten technischen Identifikators des Identitätsanbieters und des Pseudonyms selber keine Informationen. Alle weiteren Informationen (Attribute) bleiben unter der Kontrolle der Identitätsanbieter (Kanton, Gemeinde oder Schule).

5.6 Zwischenfazit

Werden die dargestellten Anwendungsbeispiele von Datenräumen mit den in Kapitel 4 entwickelten Grundprinzipien und deren Indikatoren in Verbindung gebracht, so ergeben sich folgende Einsichten:

- **Transparenz:** Das Grundprinzip Transparenz ist überall präsent, es werden aber unterschiedliche Schwerpunkte gesetzt. Bei EPD und Edulog wird Transparenz so verstanden, dass für die betroffene Person ersichtlich werden sollte, wer auf die Daten Zugriff hat, bzw. im Fall von Open Finance, bspw. welche Transaktionen man als Kundin und Kunde getätigt hat. NADIM und SHED wollen hingegen die Transparenz des Systems als Ganzes fördern, um Angebot und Nachfrage bestmöglich aufeinander abzustimmen. Im Fall der NADIM geht es primär um die Vereinfachung des Zugangs zur Gesamtmobilität für die Reisenden sowie um die optimale Kapazitätsauslastung und Koordination der verschiedenen Verkehrsmittel (multimodale Mobilität). Im Fall des SHED steht die Transparenz hinsichtlich Verbrauch und Produktion von Energie, um Einsparungen und Versorgungssicherheit zu erzielen, im Vordergrund. Die unterschiedlichen Schwerpunkte ergeben durchaus Sinn: Bei den Anwendungsbeispielen Gesundheit, Bildung und Finanzen handelt es sich um Dienstleistungen, die Individuen direkt betreffen und bei denen höchst sensible Daten im Spiel sind. Im Gegensatz dazu steht in den Bereichen Mobilität und Energie das Gesamtsystem im Zentrum. Transparenz spielt somit in allen Anwendungsbeispielen eine wichtige Rolle, sie wird aber abhängig vom Zweck des Datenraums und der Sensitivität der Daten unterschiedlich ausgestaltet.

- **Kontrolle:** Eine ähnliche Tendenz zeigt sich beim Grundprinzip Kontrolle. Dieses Grundprinzip wird primär in Anwendungsbeispielen mit sensitiven persönlichen Daten umgesetzt, also beim EPD und Open Finance. In diesen Beispielen bestehen verschiedene Mechanismen, um Handlungsfähigkeit und Handlungsfreiheit zu gewährleisten. Namentlich können die betroffenen Personen im Datenraum entscheiden, wem sie wann welche Daten zu welchem Zweck zur Verfügung stellen. Besonders ausgeprägt ist dies beim EPD. Bei NADIM und SHED ist das Kontrollelement bisher weniger ausgeprägt, da einerseits Sachdaten im Zentrum stehen und andererseits die primären Datenanbieter und Nutzniesser nicht Endkunden, sondern verschiedene Mobilitäts- oder Energieunternehmen sind.

- **Fairness und Verantwortlichkeit:** Insbesondere bei NADIM und SHED zeigen sich die Grundprinzipien Fairness und Verantwortlichkeit als Schwerpunkte. Der Betrieb der NADIM soll bspw. durch eine neutrale und unabhängige öffentliche Anstalt sichergestellt werden. Auch in der Entwicklung der SHED steht institutionelle Unabhängigkeit im Zentrum. Diese Ansätze garantieren einen diskriminierungsfreien Zugang zu Daten, die Verhältnismässigkeit der Datenerhebung und eine Unabhängigkeit gegenüber den beteiligten Akteuren. Im Fall der NADIM soll zudem eine entsprechende Ombudsstelle geprüft werden. Diese Schwerpunkte sind nicht zufällig gewählt: Sowohl in den Sektoren Mobilität als auch Energie sind bereits unterschiedliche Marktakteure mit verschiedenen systemrelevanten Rollen und einer entsprechenden Marktmacht präsent. In einem solchen Kontext sind Prinzipien wie Fairness und Verantwortlichkeit von besonderer Bedeutung. Dies trifft auch auf Open Finance zu, wo Drittanbieter wie bspw. Fin-Tech-Unternehmen die traditionellen Akteure herausfordern. Auch das EPD und Edulog schreiben Fairness und Verantwortlichkeit hoch. Dies insbesondere durch die Wahrung des Indikators der Verhältnismässigkeit, durch Datensuffizienz und indem an die Selbstverantwortung der Dienstleistungsanbieter appelliert bzw. der ungerechtfertigte und unberechtigte Datenzugriff ohne vorgängig erteilte Zugriffsberechtigung im Zusammenhang mit dem EPD mit Busse bestraft wird.

- **Effizienz:** Effizienzsteigerungen durch Standardisierung und Schnittstellen sind bei allen Beispielen präsent und stehen im Zentrum. Die NADIM schafft durch Schnittstellen eine Dateninfrastruktur, welche eine standardisierte Nutzung der Daten ermöglicht. Dabei wird ein Kerndatenset definiert; ähnlich bei Edulog, wo die Standardisierung durch die Festlegung verschiedener Attribute für jede Nutzerin und jeden Nutzer erfolgt. Die offene Standardisierung von Schnittstellen ist bei Open Finance ebenfalls eine zentrale Voraussetzung, sodass traditionelle Finanzmarktinstitute und Drittanbieter bei den Finanzinstituten andocken können und ein reibungsloser Datentransfer gefördert werden kann. Beim EPD ermöglicht die direkte technische Anbindung zwischen dem EPD-Anbieter und der IT-Struktur der Gesundheitseinrichtung die Effizienzsteigerung.

Die Darstellung zeigt, dass die Anwendungsbeispiele von Datenräumen bis anhin **unterschiedliche Schwerpunkte setzen in der Umsetzung der Grundprinzipien der digitalen Selbstbestimmung**. Dies ist teilweise aus Sicht der unterschiedlichen Zwecke der Datenräume, der Art und Sensitivität der Daten oder der relevanten Marktstruktur im Sektor erklärbar.

Es zeigt sich auch, dass die Grundprinzipien der digitalen Selbstbestimmung sich teilweise gegenseitig bedingen, in bestimmten Fällen aber auch in einem Spannungsverhältnis zueinanderstehen können. So bedingt die Kontrolle über die eigenen Daten bspw., dass Transparenz besteht, welche Daten wo und

zu welchem Zweck genutzt werden. Andererseits kann ein zu hohes Mass an Kontrolle dazu führen, dass der freie Datenfluss gehemmt wird und somit Abstriche bei der Effizienz zu verzeichnen sind.

Schliesslich ist ersichtlich, dass die Anwendungsbeispiele von Datenräumen auf einen bestimmten Sektor (Mobilität, Energie, Gesundheit, Bildung, Finanzen) und auf einen bestimmten geographischen Raum (Kanton, Nationalstaat) begrenzt sind. Dies steht im Gegensatz zur Tendenz, dass gerade globale Datenplattformen immer mehr auch Daten über verschiedene Sektoren miteinander verknüpfen, um weitere Effizienzgewinne zu erzielen. Es besteht deshalb ein **ungenutztes Potenzial in der Schweiz, Datenräume über den Sektor und den geographischen Raum hinaus mit anderen Datenräumen zu koppeln und Interoperabilität herzustellen**.[72] Auf Verwaltungsebene sind bereits Bestrebungen gegenwärtig, um dieses Potenzial auszuschöpfen. So sichert der bereits bestehende Geodatenraum die standardisierte Bereitstellung von Geodaten und ermöglicht dadurch ein erhöhtes Analyse- und Nutzungspotenzial dieser raumbezogenen Daten. Auch die i14y Interoperabilitätsplattform, welche als Schnittstelle den Datenaustausch fördert und verschiedene Akteure vernetzt, trägt damit zu einer verstärkten Datennutzung, insbesondere einer Mehrfachnutzung von Daten bei.[73]

Zudem kann eine nationale Koordinationsstellte dazu beitragen, Akteure bei der Beantwortung von Fragen zu verschiedenen Konzeptualisierungsmöglichkeiten eines Datenraumes sowie zur Interoperabilität zu unterstützen. In verschiedenen europäischen Ländern sind solche nationale Koordinationsstellen (Data Hub) bereits im Begriff zu entstehen. Auch in der Schweiz laufen Abklärungen für ein Koordinationsstelle für Verwaltungseinheiten und administrative Aufgaben (DataHub4Gov)[74]. Es gilt nun auch abzuklären, ob eine solche nationale Koordinationsstelle, ein «Swiss Data Hub», auch für weitere Akteure geschaffen werden sollte (siehe Kapitel 7.2).

6 Internationale Datengouvernanz und Interoperabilität

Datenflüsse sind oft transnational. Die Gründe können unterschiedlich sein: So werden in manchen Fällen Daten aus verschiedenen Länder zusammengeführt, um repräsentativere und diversifiziertere Daten als Erkenntnisgrundlage zur Verfügung zu haben. In anderen Fällen sind es Verarbeitungsschritte entlang der Wertschöpfungskette, welche regional oder gar global verteilt sind und eines grenzüberschreitenden Datenaustauschs bedürfen. Nicht zuletzt spielt der Standort der Infrastruktur eine Rolle: Wo lokal keine Infrastruktur (bspw. Cloud → Cloud) vorhanden ist, muss auf ausländische Anbieter zurückgegriffen werden, was oft zur Internationalisierung der Datenflüsse führt.

Das Potenzial von Daten, welche international genutzt werden können, ist enorm. Gerade für die Schweiz als mittelgrosse und hochvernetzte Wirtschaftsnation ist die transnationale Nutzung von Daten wichtig und kann den Zugang zum europäischen Binnenmarkt und weiteren internationalen Märkten ermöglichen. Um dieses Potenzial auszuschöpfen, sollten Datenräume international kompatibel sein. Das bedeutet, dass es grenzüberschreitende Rahmenbedingungen braucht, um eine gemeinsame Nutzung realisieren zu können. Wesentliche Grundlagen, auf die aufzubauen ist, sind das

[72] In jedem Fall einzuhalten sind dabei das DSG sowie das Europaratsübereinkommen 108+, und es ist darauf zu achten, dass die Anerkennung des schweizerischen Datenschutzniveaus durch die EU nicht gefährdet wird.
[73] Für weitere Informationen, siehe <www.i14y.admin.ch> (Zugriff am 04.03.2022).
[74] *Digitale Verwaltung Schweiz (2022)*, «E-Government Architektur für den strategischen Umsetzungsplan erarbeiten und führen».

Europaratsübereinkommen 108+, die Artikel 14 ff. revDSG und die Kriterien der EU für die Anerkennung des schweizerischen Datenschutzniveaus.

Das folgende Kapitel beleuchtet den internationalen Kontext, die Herausforderungen, welche im internationalen Bereich einheitlichen Rahmenbedingungen im Wege stehen und identifiziert mögliche Lösungsansätze.

6.1 Unterschiedliche datenpolitische Ansätze

In den letzten Jahren hat die Polarisierung im internationalen und multilateralen Kontext angesichts von geopolitischen Rivalitäten zugenommen. Diese Tendenz zeigt sich in der Digital- und Datenpolitik, wo verschiedene – teilweise gegensätzliche – Ansätze aufeinandertreffen. Wie in anderen Bereichen verhindern unterschiedliche Interessen und Werte derzeit einen notwendigen minimalen Konsens, der eine gemeinsame internationale Datenpolitik ermöglichen würde. Die derzeit vorherrschenden datenpolitischen Stossrichtungen können – grob vereinfacht – in die drei folgenden Ansätze unterteilt werden:

1. Einige Staaten wie die USA verfolgen eine Datenpolitik, welche stark auf **unternehmerische Freiheit bei der Datennutzung** ausgerichtet ist. Daten sollen möglichst ohne staatliche Einschränkungen genutzt werden können, um Innovation und Wettbewerbsfähigkeit zu steigern. Daten werden dabei in erster Linie als wirtschaftliche Ressource verstanden, welche dem datenkontrollierenden Akteur gehört. Dementsprechend werden gewisse rechtliche Bestimmungen, wie bspw. der Schutz des geistigen Eigentums und von Geschäftsgeheimnissen als wichtig befunden. Ansonsten wird ein international uneingeschränkter Datenfluss, als prioritär erachtet und weitere regulatorische Eingriffe generell als innovationshemmend abgelehnt.

2. Andere Staaten wie China fassen den Zugang und die Kontrolle zu Daten in weitreichenden Teilen des Lebens als **staatliches Primat und als Ausübung der eigenen Souveränität** auf. Daten werden dabei vor allem zur staatlichen Steuerung der Gesellschaft genutzt. Im internationalen Umfeld versuchen diese Akteure, die Rolle und den Einfluss des Staates im Bereich der Datenpolitik auf Kosten von anderen Anspruchsgruppen zu stärken.

3. Die EU sowie weitere europäische und aussereuropäische Staaten haben sich für einen Ansatz entschieden, der **stärker auf eine werte- und menschenzentrierte Datenpolitik** ausgelegt ist. Dabei soll eine angemessene Balance zwischen Freiheit für Individuen und Unternehmen, einer gewissen Transparenz sowie dem Schutz der Privatsphäre und anderen Grundrechten erreicht werden. Durch die bewusste Regulierung gewisser Bereiche soll das Vertrauen der Bevölkerung in den Umgang mit Daten gestärkt werden (siehe Box unten).

Die EU ist hier für die Schweiz in vielen Bereichen ein natürlicher Partner: Beide setzen sich für eine werte- und menschenzentrierte Datengesellschaft ein. Die Nutzung des wirtschaftlichen und gesellschaftlichen Potenzials von Daten soll unter Gewährleistung allfälliger geistiger Eigentumsrechte sowie unter Schutz und Wahrung der Grundrechte und demokratischen Werte geschehen. Zudem ergibt der Einbezug der Schweiz in europäische Datenräume aufgrund der gemeinsamen wirtschaftlichen

Beziehungen und den starken Verbindungen zwischen Sektoren (bspw. aufgrund geteilter Lieferketten) für beide Seiten Sinn.[75]

Hingegen hat die Schweiz mit der digitalen Selbstbestimmung einen eigenen Ansatz entwickelt, den sie in die Gestaltung europäischer Datenräume einbringen kann. Während die EU oftmals mit neuen regulatorischen Massnahmen auf Herausforderungen in der Datenpolitik reagiert, soll in der Schweiz im Rahmen der digitalen Selbstbestimmung im Austausch mit allen Anspruchsgruppen die richtige Balance zwischen Innovationsfreiheit und Schutz ermöglicht werden. Die digitale Selbstbestimmung und die in diesem Bericht dargestellten Grundprinzipien und Indikatoren (siehe Kapitel 4) können somit einen direkten Beitrag zur Entwicklung europäischer Datenräume leisten.

Anschauungsbeispiel EU

Die Europäische Kommission möchte im Rahmen des *Data Governance Act* Rahmenbedingungen für Anbieter einer gemeinsamen Datennutzung (sog. → Datenmittler) und für Anbieter von Datenspenden einführen. Diese umfassen einen Anmelde- und Aufsichtsrahmen für Datenmittler und eine freiwillige Eintragung von datenaltruistischen Organisationen für Datenspender. Der Data Governance Act soll damit als Rahmen das Vertrauen in diese Einrichtungen fördern.

Ebenfalls will die Kommission die Entwicklung und Interoperabilität gemeinsamer europäischer Datenräume in bestimmten strategischen Wirtschaftszweigen und Bereichen von öffentlichem Interesse fördern (diese sind: Industrielle Fertigung, Gesundheit, Finanzdaten, Grüner Deal, Mobilität, Energie, Agrarsektor, öffentliche Verwaltung und Bildung). In diesen neun Bereichen sollen Datenräume gebildet werden, welche Behörden, Unternehmen und der Wissenschaft die Nutzung und Weitergabe von Sachdaten erleichtern. Im Gegensatz zur digitalen Selbstbestimmung, welche die vertrauenswürdige Nutzung von Sach- und Personendaten fördern möchte, setzt die Europäische Kommission im Bereich der Datenräume in einem ersten Schritt vor allem auf die Verknüpfung von Sachdaten.

6.2 Fragmentierung der globalen Datenpolitik

Aufgrund der unterschiedlichen Ansätze bei der Datenpolitik gibt es derzeit auf internationaler Ebene keinen Konsens zur Entwicklung einer globalen Gouvernanz für Daten und Datenräume. Obwohl völkerrechtliche Normen (wie etwa der Schutz der Privatsphäre) im digitalen Raum genauso wie im physischen Raum gelten, gibt es derzeit keine Einigung für die Zuständigkeiten und Prozesse der bestehenden internationalen Organisationen zur Konkretisierung solcher Normen im digitalen Bereich. Entsprechend unklar ist, in welchen internationalen Gremien, welche Digitalisierungsthemen mit welchem Ziel behandelt werden sollen.

Hinzu kommt, dass Datenräume oftmals bereits von Beginn an, aufgrund territorialer Rechtsunterschiede, geographisch begrenzt konzeptualisiert und aufgebaut werden. Datenräume entstehen vor diesem Hintergrund regelmässig entlang unterschiedlichen politischen oder rechtlichen Gebieten. Vor diesem Hintergrund des geographisch begrenzten Ursprungs von Datenräumen wird sich eine Kompatibilität von Datenräumen auf internationaler Ebene nicht einfach ergeben, sondern muss erarbeitet werden.

[75] Siehe dazu *Bundesrat (2020a)*, «Aussenpolitische Strategie 2020-2023».

Jüngste Beispiele für regulatorische Herausforderungen, die auf Fragmentierung zurückgeführt werden können, sind inkompatible Datenschutzanforderungen oder Lokalisierungsmassnahmen für gewisse Datensätze. So wurde in einem kürzlich erschienenen Urteil des EuGH[76] die EU-US-Datenschutzvereinbarung *Privacy Shield* (→ Privacy Shield) für ungültig erklärt. In der Folge erklärte der EDÖB auch, dass das äquivalente *Swiss-US-Privacy Shield* nicht mehr den Anforderungen eines angemessenen Schutzes unter dem Schweizer Datenschutzrecht genügt.[77] Deshalb ist die Inkompatibilität des EU- und US-Ansatzes auch eine Herausforderung für die Schweiz. Diese Entwicklungen beschränken sich jedoch nicht nur auf persönliche Daten.

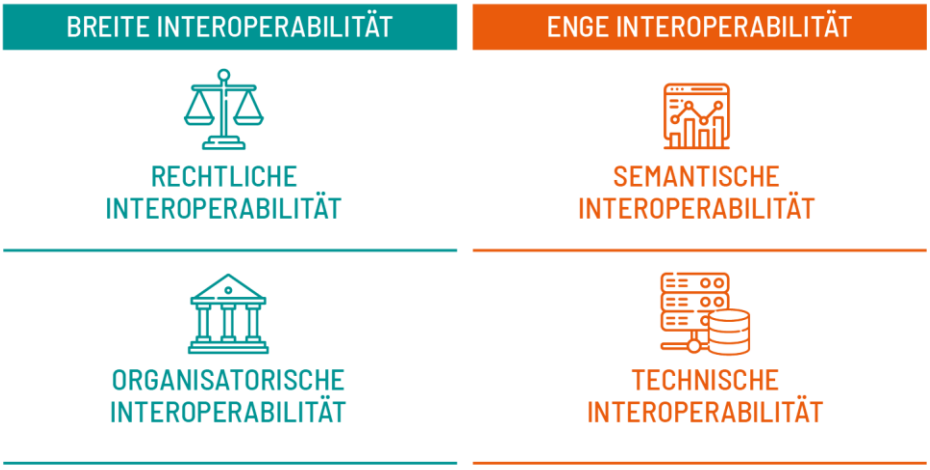
Neben Massnahmen zum Schutz der Privatsphäre nehmen auf internationaler Ebene auch Anforderungen für Datenlokalisierungen (→ Datenlokalisierung) zu. Datenlokalisierungen sind zwingende Rechts- oder Verwaltungsvorschriften, welche die Speicherung oder Verarbeitung in einem bestimmten Land vorschreiben.[78] Die Gründe für Massnahmen im Bereich Datenlokalisierung sind dabei unterschiedlicher Art: so spielen unter anderem Sicherheitsbedenken (bspw. Cybersicherheit oder nationale Sicherheit), die Durchsetzung regulatorischer und rechtlicher Anforderungen oder die Schaffung eines geopolitischen oder wirtschaftlichen Vorteils eine Rolle.[79]

Während es durchaus legitime politische Gründe geben kann, um grenzüberschreitende Datenflüsse einzuschränken, führen Entwicklungen wie Datenlokalisierung zu neuen Hürden im Datenaustausch und vergrössern die Fragmentierung der Datenpolitik.[80]

6.3 Interoperabilität

Um die unterschiedlichen datenpolitischen Ansätze und die daraus resultierende regulatorische Fragmentierung zu überbrücken, müssen internationale Datenräume kompatibel ausgestaltet werden. Die Fähigkeit von Datenräumen, trotz unterschiedlicher geographischer und sektorenabhängiger Entstehung, miteinander kommunizieren und interagieren zu können, nennt man *Interoperabilität*. Gemäss dem European Interoperability Framework (EIF) wird zwischen vier Ebenen differenziert, nämlich die *technische*, *semantische*, *organisatorische* und *rechtliche* Interoperabilität.[81] Diese lassen sich wiederum in **enge Interoperabilität** und **breite Interoperabilität** unterscheiden.[82]

[76] *EuGH (2020)*, «Data Protection Commissioner gegen Facebook Ireland Limited und Maximilian Schrems».
[77] *EDÖB (2020)*, «Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG».
[78] Dabei wird zwischen «ausschliesslichen» Lokalisierungsmassnahmen (d.h. keine Kopien der relevanten Daten dürfen die Gerichtsbarkeit verlassen) und «nicht ausschliesslichen» Lokalisierungsmassnahmen (d.h. eine Kopie der relevanten Daten muss immer innerhalb der Gerichtsbarkeit gehalten werden) unterschieden.
[79] *Svantesson D. (2020)*, «Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines», S. 14.
[80] *Svantesson D. (2020)*, «Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines», S. 13.
[81] *Europäische Kommission (2017)*, «New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations».
[82] *Goldstein E., Gasser U. and 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».



Grafik 4: Interoperabilitäts-Ebenen[83]

Die **enge Interoperabilität** beschreibt die technische und semantische Kommunikationskapazität zwischen Datenräumen. Es geht einerseits darum, dass technische Infrastrukturen miteinander kompatibel sind. Dafür können Anwendungssysteme bspw. über entsprechende elektronische Schnittstellen (API) verfügen, um den Datenaustausch möglichst einfach und effizient zu gestalten. Andererseits müssen Daten auf semantischer Ebene so hinterlegt und beschrieben sein, dass sie von einem anderen Datenraum interpretiert werden können. Anders gesagt müssen Format und Bedeutung der ausgetauschten Daten auch durch den Austausch erhalten und interpretierbar bleiben.

Ein wichtiger Aspekt der engen Interoperabilität sind Standards. Eine Standardisierung der Datenerfassung, -ablage und -aufbereitung sowie des Datenaustausches ermöglicht es, Daten in unterschiedlichen Datenräumen und für verschiedene Zwecke wiederzuverwenden. Ebenfalls relevant für die semantische Interoperabilität sind einheitliche Metadatenstandards, welche Formate und Bedeutung von Daten korrekt erfassen und beschreiben. Als Beispiel hierzu kann die in der Schweiz im Rahmen der Nationalen Datenbewirtschaftung etablierte i14y-Interoperabilitätsplattform[84] genannt werden. Mit ihrer entwickelten Gouvernanz und den Prozessen der Harmonisierung sowie (in ihrer zukünftigen Funktion) als API Schnittstellenverzeichnis des Bundes berücksichtigt sie bereits Faktoren der semantischen Interoperabilität. Die Entwicklung von Standards geschieht entweder projektbezogen (bspw. für einen neuen Datenraum), was Flexibilität und eine spezifische Anpassung erlaubt oder aber es werden existierende Standards übernommen.[85] Der grosse Vorteil der Übernahme von existierenden Standards ist, dass damit die Interoperabilität mit allen anderen Systemen, welche diesen Standard auch verwenden, garantiert ist. Insbesondere in Bezug auf interoperable Datenräume ist daher die Übernahme existierender Standards zu bevorzugen. Heute beschäftigen sich verschiedene Gremien mit der Festlegung von Standards: weltweit die ISO/IEC, IEEE, IETF, ITU oder die W3C. Auf europäischer Ebene sind es die CEN und ETSI oder im spezifischen Bereich der Datenräume Gaia-X und IDSA.

Fragen der Interoperabilität zwischen Datenräumen sind jedoch nicht auf technische Aspekte begrenzt. Vielmehr braucht es gewisse rechtliche und gesellschaftliche Rahmenbedingungen sowie eine organisatorische Interoperabilität, damit Daten ohne grösseren administrativen Aufwand über

[83] Grafik angelehnt an *Europäische Kommission (2017),* «New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations».
[84] Siehe dazu auch <www.i14y.admin.ch> (Zugriff am 04.03.2022).
[85] *Collovà P. et al. (2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung», S. 23.

Datenraumgrenzen hinweg zirkulieren können. Dieser Aspekt wird als **breite Interoperabilität** bezeichnet.

Technische Standards haben in der breiten Interoperabilität eine wichtige Funktion: Sie tragen dazu bei, rechtliche und ethische Vorgaben umzusetzen und erlauben im Falle einer verbreiteten Akzeptanz dieser Standards eine vereinfachte Kompatibilität zwischen verschiedenen nationalen Rechts- und Regulierungssystemen. In den letzten Jahren stellten sich neben rechtlichen Fragen (bspw. im Bereich Datenschutz oder geistiges Eigentum) zunehmend Herausforderungen im Zusammenhang mit grundsätzlich unterschiedlichen datenpolitischen Regulierungsansätzen (siehe Kapitel 6.1). Dabei spielen gesellschaftliche Wertvorstellungen und geopolitische Interessen eine zentrale Rolle. Die Bevölkerung muss darauf vertrauen können, dass Daten aller Art im Ausland nicht zweckentfremdet genutzt werden oder nur, weil sie die Landesgrenzen überschreiten, nicht weniger geschützt sind.

Breite Interoperabilitätsansätze ermöglichen es, international unterschiedlich strukturierte Datenräume zu koppeln. Verstärkte Kooperation und Koordination der Rechtsordnungen, gegebenenfalls in Form bilateraler Abkommen oder mittels anderen internationalen Instrumenten, ermöglichen gewisse Herausforderungen zu überwinden und Eingrenzungen des Datenflusses zu eliminieren bzw. zu minimieren. Dies ist insbesondere möglich, wenn es sich um gleich- oder ähnlich gesinnte Partner handelt. Auf globaler Ebene bleiben jedoch grosse Herausforderungen bestehen. Hier gilt es neue Ansätze zu entwickeln, welche eine breite Interoperabilität erwirken können, ohne dass dabei die für die Schweiz zentralen Grundsätze und Werte untergraben werden.

6.4 Zwischenfazit

Das Potenzial von internationalen Datenflüssen ist enorm. Wie die Schweiz sind viele andere Staaten darum bemüht, eine bessere Nutzung dieses Datenpotenzials für ihre Gesellschaft und Wirtschaft sicherzustellen und das Vertrauen der Bevölkerung im Umgang mit Daten durch entsprechende Massnahmen zu stärken. In den letzten Jahren stieg das Bewusstsein, dass die politische und regulatorische Fragmentierung im Bereich der Datenpolitik die Realisierung dieses Potenzials hindert. Entsprechend häufen sich die Forderungen nach neuen, effektiven Rahmenbedingungen auf internationaler Ebene und einer funktionierenden Gouvernanzstruktur, um Herausforderungen zu diskutieren und gemeinsam Lösungen im Sinne einer breiten Interoperabilität entwickeln zu können.[86]

Verschiedene Stimmen haben bereits darauf hingewiesen, dass trotz der laufenden Arbeiten im Bereich des internationalen Handels (wie bspw. bei den multilateralen Verhandlungen zu E-Commerce in der WTO) weitgehende Differenzen zur digitalen Gouvernanz bestehen bleiben, sowohl inhaltlicher als auch prozeduraler Natur.[87] Diese drohen mittel- oder längerfristig zu einer fortschreitenden Fragmentierung der Datenpolitik zu führen und dadurch weitere Hürden für den grenzüberschreitenden Datenfluss nach sich zu ziehen. Vor diesem Hintergrund sind dogmatische Forderungen wenig zielführend: Weder Lokalisierungsmassnahmen noch ein vollständig freier Datenfluss werden die unterschiedlichen politischen Ziele und Erwartungen erfüllen können. Vielmehr sind neue Ansätze nötig, welche es ermöglichen, einen Mittelweg zu finden.

[86] *UNCTAD (2021)*, «Digital Economy Report 2021: Cross-Border Data Flows and Development – For Whom the Data Flow»; *De La Chappelle B. and Porciuncula L. (2021)*, «We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty».
[87] *UNCTAD (2021)*, «Digital Economy Report 2021: Cross-Border Data Flows and Development – For Whom the Data Flow»; *De La Chappelle B. and Porciuncula L. (2021)*, «We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty».

Die Schweiz kann in den laufenden Diskussionen zur digitalen Gouvernanz mit der Vision der digitalen Selbstbestimmung einen wichtigen Beitrag leisten. Die digitale Selbstbestimmung ist klar im werte- und menschenzentrierten Ansatz zu verorten, kann aber – dank der Bedeutung, die sie sowohl den Individuen, den Unternehmen sowie der Gesellschaft als Ganzes einräumt – auch auf verschiedene andere Anliegen eingehen. Mit dem Ansatz der digitalen Selbstbestimmung nimmt die Schweiz verschiedene Anliegen auf, die in den drei dargestellten Ansätzen unterschiedlicher Datenmodelle präsent sind. Auch wenn die Ziele der Schweiz dabei der EU am nächsten sind, bringt sie mit der digitalen Selbstbestimmung auch im Verhältnis zur EU neue Gesichtspunkte ein. Um die digitale Gouvernanz im Sinne der digitalen Selbstbestimmung mitzugestalten, kann die Schweiz diese Vision nach aussen tragen und das Konzept auf internationaler Ebene verankern.

Dies soll in zweierlei Hinsicht geschehen, normativ und operationell:

1. Auf der **konzeptionell-normativen Ebene** will die Schweiz die Relevanz und Bedeutung des Konzepts der digitalen Selbstbestimmung erklären und mit gleichgesinnten Akteuren für diese Idee einstehen. Sie arbeitet darauf hin, dass *sich* die *digitale Selbstbestimmung als Leitidee für die Datengouvernanz (→ Datengouvernanz) auf internationaler Ebene etabliert*. Dafür wird die Schweiz weiterhin relevante Gremien und Prozesse im Bereich der internationalen Datengouvernanz unterstützen, entwickeln und wo nötig neu schaffen. Wo immer möglich, sollen dabei auch Synergien mit dem Standort Genf genutzt werden. Auf inhaltlicher Ebene sollen auch Organisationen genutzt werden, in denen ähnliche Themen bereits etabliert sind (bspw. Europarat oder die OECD).
2. Auf **operationeller Ebene** möchte die Schweiz mit gleichgesinnten Akteuren einen Beitrag zur praktischen Verwirklichung der digitalen Selbstbestimmung und der Implementierung von vertrauenswürdigen Datenräumen leisten. Die Aktivitäten in diesem Bereich zielen auf praktische Massnahmen für die *Schaffung von interoperablen und transnational ausgerichteten Datenräumen* ab. Konkret soll die Erarbeitung von internationalen Richtlinien für Datenraumbetreiber dabei behilflich sein. Dabei sollen auch bereits entwickelte oder im Entstehen befindliche Initiativen, wie bspw. die Arbeiten im Rahmen der Nationalen Datenbewirtschaftung, berücksichtigt werden. In einem ersten Schritt sollen dafür gleichgesinnte Partner aus allen Stakeholdergruppen identifiziert werden.

7 Handlungsempfehlungen

Die digitale Selbstbestimmung kann auf unterschiedliche Arten umgesetzt werden. Im vorliegenden Bericht wird auf die Schaffung von vertrauenswürdigen Datenräumen fokussiert. Die entstehenden Datenräume zeigen dabei, dass in der Funktionsweise von Datenräumen insbesondere zwei Rollen ein grosser Einfluss zukommt: Einerseits der Betreiberin der technischen Infrastruktur und andererseits der für die Gouvernanz zuständigen Einrichtung.[88] Um vertrauenswürdige Datenräume zu schaffen und entsprechend die Einhaltung der Grundprinzipien zu fördern, gilt es bei diesen Rollen anzusetzen.

Obwohl in diversen Bereichen (bspw. Mobilität, Energie) Bestrebungen zur Ausarbeitung von angemessenen sektorübergreifenden Rahmenbedingungen laufen, sind diese zu intensivieren, um einerseits die Nutzung von Daten besser zu fördern und andererseits die Entwicklungstendenzen (wie

[88] Diese beiden Rollen können auch zusammenfallen, sodass derselbe Akteur für den Betrieb der technischen Infrastruktur, als auch für die Sicherstellung der Gouvernanz zuständig ist. In diesem Fall spricht man von einer Datenraumbetreiberin (siehe Anhang 2).

bspw. Datenballungen) zu minimieren und dabei gleichzeitig Transparenz, Vertrauen und zusätzliche Kontrolle für Nutzerinnen und Nutzer zu schaffen.[89] Ohne Gegenmassnahmen werden sich bereits bestehende Herausforderungen verstärken und folglich das Vertrauen in die Datennutzung zusätzlich schwächen.

Die Bedeutung der Entwicklungen in den nächsten Jahren sollte nicht unterschätzt werden: Neu entstehende Datenräume werden die Standards dafür setzen, wie wir als Gesellschaft Datenräume nutzen und den breit angelegten Austausch von Daten zukünftig betreiben. Auch in der Schweiz können richtungsweisende Massnahmen dazu beitragen, dass Datenräume sich auf der Basis von den in diesem Bericht definierten Grundprinzipien entwickeln.

Es stellt sich daher die Frage, welche Rolle die öffentliche Hand im Zusammenhang mit digitalen Dienstleistungen einnehmen soll. Denkbar sind zunächst verschiedenste staatliche Handlungsformen von der Abgabe von Empfehlungen (vgl. den hier vorgeschlagenen Verhaltenskodex) über zahlreiche Zwischenstufen wie Subventionen bis hin zu einer strikten rechtlichen Regelung aller Aspekte. Im Vordergrund stehen aus heutiger Sicht zwei Ansätze:

1. **Öffentliche Hand als Leistungserbringer:** Die öffentliche Hand könnte als Leistungserbringer auftreten (z.B. öffentliche Anstalt) und die nötigen Dienstleistungen im Zusammenhang mit vertrauenswürdigen Datenräumen selbst gewährleisten. In diesem Fall würde sie auch die erforderlichen Regelungen in der Form der Gesetzgebung im politischen Prozess festlegen.
2. **Angemessene Rahmenbedingungen:** Die öffentliche Hand definiert angemessene Rahmenbedingungen, um die Entwicklungen in eine politisch erwünschte Richtung zu fördern, bzw. unerwünschte Entwicklungen zu verhindern. Sie legt dabei Grundsätze für die Organisation und Operation von vertrauenswürdigen Datenräumen fest und überwacht deren Einhaltung. In einer frühen Phase soll dies hingegen insbesondere durch Selbstregulierungsmassnahmen geschehen, um Innovation und Entwicklung nicht einzuschränken.

Der Staat oder die **öffentliche Hand als Leistungserbringer**, also als exklusiver oder in Konkurrenz zu privaten Angeboten stehender Betreiber von Datenräumen für private Unternehmen oder Einzelpersonen, ist zumindest in gewissen Bereichen weder realistisch noch wünschenswert. Ein liberaler und wettbewerbsorientierter Ansatz führt in vielen Fällen eher zu einer Vielfalt an Angeboten, die flexibel auf unterschiedliche Bedürfnisse reagieren können. Es gibt jedoch Bereiche (bspw. vernetzte Mobilität), in denen es politisch als opportun und wünschenswert erachtet wird, dass die öffentliche Hand eine bestimmte Rolle übernimmt oder eine Grundversorgung im Sinne eines Service Public abdeckt. Dabei ist die Kompetenzverteilung zwischen Bund, Kantonen und Gemeinden zu beachten, und es sind die erforderlichen gesetzlichen Grundlagen zu schaffen. Der Bundesrat ist sich diesen Entwicklungen bewusst und hat dem BAKOM den Auftrag erteilt, einen Bericht zur Entwicklung eines digitalen Service Public zu erarbeiten. Dieser Bericht soll im Juni 2022 veröffentlicht werden.

In der Literatur wird es teilweise als sinnvoll erachtet, dass auf dem Weg der Gesetzgebung oder mit anderen, weniger verbindlichen Mitteln **angemessene Rahmenbedingungen** geschaffen oder mitgestaltet werden.[90] In gewissen Netzwerksektoren wie Telekommunikationen, Energie, Mobilität oder Postdienstleistungen bereits vorhanden, können auch angemessene Rahmenbedingungen im

[89] *Collovà P. et al. (2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung»; *Jentzsch N. (2017)*, «Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds – Ökonomische Rahmenbedingungen innovativer Lösungen zu Einwilligungen im Datenschutz».
[90] *Collovà P. et al. (2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung».

Zusammenhang mit Datenräumen erforderlich sein. In dieser Rolle ist es der öffentlichen Hand möglich, grundlegende Ziele von öffentlichem Interesse zu setzen und diese mit richtungsweisenden Massnahmen zu fördern. Der Bund soll dabei die grundlegenden Rahmenbedingungen, nach denen Datenräume organisiert sein müssen und operieren sollen, festlegen und überwachen. Diese Rahmenbedingungen sollen es erlauben, die Realisationsmöglichkeiten des Datenpotenzials zu maximieren und gleichzeitig negative Entwicklungstendenzen zu minimieren. Es ist dabei auch zu beachten, dass unter Umständen, so bspw. je nach Sektor oder involvierten Akteuren, auch Limitationen eines solchen Ansatzes in Kauf zu nehmen sind. Entsprechend wichtig ist eine laufende Beobachtung und Beurteilung dieser Rahmenbedingungen, um festzustellen, ob diese stets zielführend bleiben oder weitergehende Massnahmen zu treffen sind. Neben der Regulierung fällt dem Staat auch die Rolle der Durchsetzung der selbst aufgestellten Regeln zu. Die konkrete Ausgestaltung der Durchsetzungsmechanismen soll dabei effektive Mittel zur Verfügung stellen, um eine Verletzung berechtigter Ansprüche durch die Datenraumbetreiber bzw. die datennutzenden Organisationen nötigenfalls anzuzeigen und zu beseitigen.

7.1 Einführung von Rahmenbedingungen

Die Entwicklungen im Bereich Datenräume stehen noch am Anfang – sie sind in vielen Sektoren erst im Begriff zu entstehen und es sind weiterhin noch nicht alle Herausforderungen bekannt. Obschon die Schaffung von Rahmenbedingungen sinnvoll erscheint, ist in diesem Kontext eine umfassende und horizontale Regulierung von Datenräumen zum jetzigen Zeitpunkt wenig zielführend. Dies bedeutet jedoch nicht, dass für bestimmte Sektoren oder Teilbereiche keine Regulierungsansätze entwickelt werden können oder sollen: Je nach Situation kann dies durchaus auch bereits heute angebracht sein.

Auf nationaler und horizontaler Ebene scheint in der heutigen Situation jedoch ein koordinierter Selbstregulierungsansatz am besten geeignet. Dabei soll der Bund zusammen mit den betroffenen Akteuren freiwillige Rahmenbedingungen festlegen. Dies würde es erlauben, richtungsweisende Massnahmen zu ergreifen ohne dabei Innovationen einzuschränken. Entsprechend soll als erster Schritt ein freiwilliger **Verhaltenskodex** für vertrauenswürdige Datenräume erarbeitet werden. Ein solcher *Verhaltenskodex* soll unter Koordination des Bundes in Zusammenarbeit mit allen relevanten Akteuren entwickelt werden und dient dazu die dargestellten Grundprinzipien für Datenraumbetreiber weiter zu konkretisieren (siehe Kapitel 4). Dabei ist auf Eigenheiten einzelner Sektoren (insbesondere auch bestimmte internationale Standards, die für diese Sektoren bereits gelten) Rücksicht zu nehmen. Es sind verschiedene Elemente eines *Verhaltenskodex* denkbar. Die Empfehlungen zu den Grundprinzipien (siehe Anhang 3) könnten hier erste Anknüpfungspunkte liefern. Mit dem Nationalen Netzwerk Digitale Selbstbestimmung steht für die Erarbeitung eines solchen *Verhaltenskodex* zudem bereits ein passendes Gefäss zur Verfügung. Die Einhaltung dieses *Verhaltenskodexes* soll durch ein Monitoring via Selbstberichterstattung überprüft werden können. Es soll auch abgeklärt werden, ob die Einhaltung dieses Verhaltenskodexes für Bundesbehörden verbindlich sein soll.

Der Erfolg eines solchen freiwilligen *Verhaltenskodexes* wird dann die weiteren Schritte des Bundes prägen. Entsprechend müssen die Entwicklungen im Zuge eines *Verhaltenskodexes* eng beobachtet und die Erreichung der zentralen Ziele überprüft werden. Zudem soll regelmässig evaluiert werden, ob der Selbstregulierungsansatz dem gewünschten Ergebnis Vortrieb leistet oder ob andere Formen der Regulation in Betracht gezogen werden müssen.

7.2 Errichtung eines Swiss Data Hub und Förderung der Interoperabilität

Auf europäischer Ebene stellt das deutsch-französische Projekt *Gaia-X* einen Bezugspunkt für die Schaffung von sektor- und grenzüberschreitenden Datenräumen dar. Gaia-X setzt sich aus einem Datenraum- und einem Infrastrukturteil zusammen. Was die Datenräume betrifft, so will Gaia-X über die Schaffung von gemeinsamen Standards, eines gemeinsamen Registers, einem Katalog von Dienstleistungen etc. die technischen Voraussetzungen schaffen, so dass Datenräume auf einer gemeinsamen Grundlage aufgebaut werden und von Beginn an interoperabel ausgestaltet sind. Die Interoperabilität soll den Datenaustausch über verschiedene Branchen und über Landesgrenzen hinweg gewährleisten.

Nationale Data Hubs sollen die zentrale Anlaufstelle für Unternehmen, Forschungsinstitutionen, Verbände und die öffentliche Verwaltung eines Landes werden, welche Datenräume kreieren und nutzen wollen. Ein Vergleich mit bestehenden nationalen Hubs in Europa hat gezeigt, dass diese unterschiedlich ausgestaltet sind, vor allem mit Blick auf das Ausmass der staatlichen Beteiligung (vollständige Finanzierung durch die öffentliche Hand über Teilfinanzierung durch öffentliche Beiträge) sowie die Rolle der öffentlichen Hand (Führungsrolle im nationalen Rahmen bis hin zu reinem Herstellen von Kontakten unter interessierten Gruppen). Den meisten bestehenden Hubs ist gemeinsam, dass sie nicht spezifisch für Gaia-X geschaffen werden sondern als generelle Anlaufstelle für Fragen zu Datenräumen.

Wie dargelegt (Kapitel 5 und 6) ist es auch in der Schweiz wichtig, dass Datenräume sektor- sowie grenzüberschreitend interoperabel sind. Im Behördenbereich laufen mit dem DataHub4Gov sowie im Rahmen des Programmes Nationale Datenbewirtschaftung bereits Anstrengungen, um dies zu bewerkstelligen.[91] Es stellt sich aber auch die Frage, ob in der Schweiz eine solche Anlaufstelle, welche sich mit der Ausgestaltung von Datenräumen befasst, generell für alle Akteure geschaffen werden sollte. Hierzu könnte von den bereits bestehenden Koordinations- und Innovationsstellen ausgegangen werden: So befassen sich bereits der Delegierte des Bundesrates für digitale Transformation und IKT-Lenkung, der Beauftragte Digitale Verwaltung Schweiz, das Kompetenzzentrum für Datenwissenschaft (Data Science Competence Center, DSCC), das Koordinationsorgan für Geoinformation des Bundes (GKG), das nationale Netzwerk Digitale Selbstbestimmung oder interkantonale Gremien mit einzelnen Aspekten von Datenräumen. Ein nationaler **«Swiss Data Hub»** könnte diese bestehenden Stellen vernetzen und für alle Stakeholder als Anlaufstelle für Fragen zu Datenräumen fungieren. Namentlich könnte der Swiss Data Hub die betroffenen Akteure miteinander verbinden, die Erarbeitung des *Verhaltenskodexes* (siehe Kapitel 7.1) begleiten, diesen verbreiten und somit die Entstehung vertrauenswürdiger Datenräume unterstützen. Der «Swiss Data Hub» könnte auch die Verbindung zu internationalen Datenraumprojekten, wie Gaia-X oder das Internationale Netzwerk Digitale Selbstbestimmung, sicherstellen.

Daneben müssen Ansätze entwickelt werden, wie die sich im Aufbau befindenden Datenräume sowohl national als auch international interoperabel ausgestaltet werden können. Dabei soll insbesondere auf die Erfahrung bereits bestehender (bspw. Geodatenraum) und entstehender Datenräume (bspw. im Mobilitäts- und Energiebereich) zurückgegriffen werden. Diese Ansätze und die daraus entstehenden Erkenntnisse sollten auch in die Erarbeitung des Verhaltenskodexes wie auch in die Aktivitäten eines allfälligen «Swiss Data Hub» eingebracht werden.

[91] *Digitale Verwaltung Schweiz (2022),* «E-Government Architektur für den strategischen Umsetzungsplan erarbeiten und führen».

7.3 Massnahmen auf internationaler Ebene

Das Potenzial von transnationalen Datenflüssen ist enorm und kann der Schweizer Wirtschaf zu mehr Wachstum verhelfen. Es gilt deshalb im Einklang mit der Schweizer Aussenwirtschaftsstrategie und der Datenschutzgesetzgebung sicherzustellen, dass Schweizer Unternehmen einfachen Zugang zu internationalen Märkten, insbesondere dem europäischen Binnenmarkt, haben. Die politische und regulatorische Fragmentierung im Bereich der Datenpolitik erschwert jedoch die Realisierung dieses Ziels (siehe Kapitel 6.2). Entsprechend muss sich die Schweiz auf internationaler Ebene verstärkt mit Fragen der Datengouvernanz beschäftigen. Die Digitalaussenpolitik der Schweiz hat hier einen wichtigen ersten Schritt gemacht.

Weitere konkrete Massnahmen sind jedoch notwendig. Um eine breite Interoperabilität zwischen Datenräumen zu ermöglichen, wird eine einheitlichere internationale Datengouvernanz (→ internationale Datengouvernanz) benötigt. Die Schweiz hat hier mit der digitalen Selbstbestimmung eine klare Vision, die es auch international zu stärken gilt, um auf deren Basis konkrete Lösungen für datenpolitische Herausforderungen präsentieren zu können. Zu diesem Zweck gilt es gleichgesinnte Partner zu identifizieren sowie relevante Prozesse und Gremien zu unterstützen, weiterzuentwickeln oder, falls nötig, neu zu schaffen. Wenn immer möglich soll dabei das Internationale Genf als Standort für eine globale Daten- und Digitalpolitik berücksichtigt werden. Des Weiteren hat die Schweiz analog zum nationalen Netzwerk mit dem Aufbau eines internationalen Netzwerks Digitale Selbstbestimmung begonnen. Dieses besteht zurzeit aus akademischen Akteuren und soll auf Akteure des öffentlichen und privatwirtschaftlichen Sektors ausgeweitet werden. Dieses internationale Netzwerk ist bereits dabei, anhand von konkreten *Use Cases* in verschiedenen sektoriellen Bereichen, das Konzept der digitalen Selbstbestimmung auf internationaler Ebene zu testen und weiterzuentwickeln.

Ein wichtiger Aspekt der Interoperabilität sind internationale Standards. Neben Fragen der Gouvernanz sind deshalb Fortschritte im Bereich der Standards zentral. Die Bedeutung von Datenräumen soll dabei in laufenden Arbeiten zur Stärkung von Standards und Normungen berücksichtigt werden (siehe auch Prüfauftrag des WBF (SECO) in Zusammenarbeit mit dem EDA, dem EFD (BBL) und dem UVEK (BAKOM) zur Arbeit und Förderung internationaler Normungsorganisationen). Darüber hinaus sollen die Entwicklung von Standards im Bereich vertrauenswürdiger Datenräume in Zusammenarbeit mit existierenden Normierungsorganisationen gefördert werden.

Längerfristig gilt es mit internationalen Richtlinien für vertrauenswürdige Datenräume und für die digitale Selbstbestimmung auch Rechtssicherheit auf internationaler Ebene zu schaffen. Gerade für die Schweiz als mittelgrosse und vernetzte Wirtschaftsnation ist dies wichtig. Dazu sollen in einem ersten Schritt gleichgesinnte Partner identifiziert werden. In der Erarbeitung von internationalen Richtlinien unter Mitwirkung entsprechend identifizierten Partner sollen die Grundprinzipien der digitalen Selbstbestimmung sowie der nationale Verhaltenskodex bestmöglich reflektiert werden.

8 Glossar

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

Algorithmus	Eine eindeutige Handlungsvorschrift zur Lösung eines Problems, welche aus endlich vielen, eindeutig definierten Einzelschritten besteht. Damit können sie zur Ausführung in ein Computerprogramm implementiert werden.
Anonymisierung	Prozess, in dessen Verlauf → *Daten* so verändert werden, dass sie sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen oder → *personenbezogene Daten* so bearbeitet werden, dass die betroffene Person nicht oder nur mit einem unverhältnismäßig grossen Aufwand oder mit gesetzlich verbotenen Mitteln identifiziert werden kann.
Application Programme Interface (API)	Programmierschnittstelle, die die Anbindung von einem Softwaresystem an ein anderes System bezweckt. Siehe auch → *Schnittstellen*
Closed Data	→ *Daten*, welche unter striktem Verschluss und einzig für einen eingeschränkten Benutzerkreis innerhalb einer Unternehmung oder Verwaltung zugänglich sind. Zugriff hat nur der Datenverantwortliche.
Cloud	Modell der Datenverarbeitung, mit dem bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (bspw. Netze, Server, Speichersysteme, Anwendungen und Dienste) zugegriffen werden kann. Diese können schnell und mit minimalem Verwaltungsaufwand bzw. geringer Serviceprovider-Interaktion zur Verfügung gestellt werden.
Data Bias	Phänomen, wonach Daten zu einem verzerrten Bild zwischen dem physischen und dem digitalen Selbst führen.
Data as Commodity	→ *Daten*, welche zu einem wirtschaftlichen Zweck eingesetzt werden.
Data as Infrastructure	Eine Gesamtheit von → *Daten*, welche einen Bereich oder einen Teilbereich (bspw. die Mobilität oder die Elektromobilität) umfassend abbilden. Diese Daten sind eine zwingende Grundlage für das Funktionieren eines Systems (bspw. Mobilitätssystem in der Schweiz).
Data as Public Good	→ *Daten*, die der Öffentlichkeit als Ganzes zugänglich gemacht werden, da sie als Teil des Gemeinwohls betrachtet werden. Sie fallen somit betreffend Zugänglichkeit zwingend unter → *open data* und es handelt sich immer um Sachdaten.
Data Sharing	→ *Shared Data*
Daten	In der Informatik und Datenverarbeitung versteht man Daten als (maschinen-) lesbare und -bearbeitbare, in der Regel digitale Repräsentation von Information.
Datenanbieter	→ *Datenlieferant*
Datenbearbeitung	Jeder Umgang mit → *Daten* (sowohl → *Personendaten* als auch → *Sachdaten)* unabhängig von den angewandten Mitteln und Verfahren,

	insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.
Datengouvernanz	Darunter wird die Etablierung, Gestaltung bzw. Festigung von Institutionen- und Regelsystemen sowie von Mechanismen innerhalb der Datengesellschaft verstanden, siehe auch → *Internationale Datengouvernanz.*
Dateninfrastruktur	Die notwendigen technischen und organisatorischen Systeme und Strukturen, um → *Daten* auszutauschen und nutzbar zu machen.
Datenlieferant	Juristische oder natürliche Personen, die → *Daten* über eine → *Dateninfrastruktur* anbieten oder bereitstellen.
Datenlokalisierung	Zwingende Rechts- oder Verwaltungsvorschriften, welche die Speicherung oder Verarbeitung in einem bestimmten Land vorschreiben.
Datenmittler	Anbieter oder Dienste für eine gemeinsame Datennutzung. Somit eine Art von → *Intermediären*, die jedoch ausschliesslich mit Daten handeln.
Datennetzwerkeffekt	Siehe → *Netzwerkeffekt*
Datennutzer	Juristische oder natürliche Personen, die → *Daten* für einen bestimmten Zweck nutzen.
Datensatz	Eine Zusammenfassung von → *Daten*, die zu einem Objekt gehören und in einer Datei abgelegt sind.
Datenproduzent	Natürliche oder juristische Personen, welche → *Daten* generieren und erfassen.
Datenqualität	Bewertung von → *Daten* hinsichtlich ihrer Eignung, einen bestimmten Zweck zu erfüllen. Als Kriterien gelten dabei die Korrektheit, die Relevanz und die Verlässlichkeit der Daten, sowie ihre Konsistenz und Verfügbarkeit auf verschiedenen Systemen.
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. Wird von → *Datenraumbetreiberin* verwaltet.
Datenraumbetreiberin	Verantwortliche des → *Datenraums.* Man spricht nur dann von einer Datenraumbetreiberin, sofern dieselbe Organisation sowohl die technische Infrastruktur eines Datenraums betreibt als auch für die Sicherstellung der Gouvernanz zuständig ist.
Datentreuhänder	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 bspw. 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.
Datenzyklus	Lebenszyklus von → *Daten*; von ihrer Verfügbarkeit, Zugänglichkeit über die Bearbeitung, zum Austausch sowie der Wiederverwendung bis hin zur Löschung, Sperrung oder Archivierung.

Differential Privacy	Unkenntlich machen von → *Daten,* d.h. ein Rückschluss auf die Person ist auch mit Drittdaten nur mit einer gewissen, definierten Wahrscheinlichkeit möglich.
Digitale Kluft	Beschreibt die Ungleichheiten im Zugang und den Nutzungsmöglichkeiten von digitalen Technologien.
Digitale Wertschöpfungskette	Die drei Elemente – → *Daten*, → *Informationen*, → *Wissen* – entsprechen einer Wertschöpfungskette. Denn mit jedem Schritt, d.h. im Übergang von Daten zu Information sowie von Informationen zu Wissen nimmt die Werthaltigkeit (gesellschaftliche Sicht) oder die Wertschöpfung (ökonomische Sicht) zu.
Dynamische Daten	→ *Datensätze*, die sich ändern sobald neue Informationen verfügbar werden (zeitliche Komponente von Daten). Im Gegensatz dazu → *statische Daten.*
Gouvernanz	Effiziente Mechanismen, welche gemeinsame Regeln (inkl. die Regelung der Verantwortlichkeiten und Risiken) für den Datenzugriff bzw. den Datenaustausch und die Datennutzung festlegen. Siehe auch → *Datengouvernanz* und → *Internationale Datengouvernanz.*
Informationen	Resultat der Verknüpfung von → *Daten*. Daten, denen mittels Decodierung eine Bedeutung zukommt. In einem konkreten Bedeutungskontext interpretierte → *Daten*.
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. Grundrechtlicher Anspruch jeder Person auf Schutz vor Missbrauch ihrer persönlichen Daten (Anspruch aus Art. 13 Abs. 2 BV).
Intermediäre	Einrichtungen, die die Gewährung des Zugang zu → *Daten* und eine Verwendung von Daten durch andere Nutzerinnen und Nutzer miteinander verbinden und in vermittelnder Funktion auftreten. Intermediäre sind die Oberkategorie – sie umfassen Institutionen mit Treuhandfunktionen und/oder Marktplatzfunktionen sowie andere Methoden der Datenvermittlung.
Internationale Datengouvernanz	Entwicklung eines Institutionen- und Regelsystems sowie von Mechanismen internationaler Zusammenarbeit, um globale Probleme und grenzüberschreitende Angelegenheiten zu bewältigen. Einbezogen werden das UNO-System, internationale Organisationen, staatliche und nichtstaatliche Akteure sowie regionale Organisationen.
Interoperabilität, enge und breite	Fähigkeit zur Zusammenarbeit verschiedener Systeme, Techniken oder Organisationen, in der Regel auf Basis gemeinsamer → *Standards.* Vertriebssysteme sind bspw. 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.

	Die *enge* Interoperabilität beschreibt die technische Kommunikationskapazität zwischen → *Datenräumen*. Die *breite* Interoperabilität umfasst rechtliche und gesellschaftliche Rahmenbedingungen, damit → *Daten* ohne grösseren administrativen Aufwand über Datenraumgrenzen hinweg zirkulieren können.
Kollektive Datennutzung	Einmal gesammelte → *Daten* können für einen weiteren Zweck oder von anderen Personen bzw. Organisationen verwertet werden, siehe auch → *Data Sharing*.
Multi-Sided-Markets	Ein Unternehmen, das auf einem mehrseitigen Markt tätig ist, muss im Allgemeinen mindestens zwei verschiedene Kundengruppen bedienen (die die verschiedenen "Seiten" des Marktes darstellen). Zudem wird oft vorausgesetzt dass es indirekte → *Netzwerkeffekte* zwischen diesen zwei oder mehr Kundengruppen gibt.
Netzwerkeffekt	Beschreibt das Phänomen, dass ein Produkt oder eine Dienstleistung an Wert oder Nutzen gewinnt, je mehr Nutzerinnen und Nutzer es hat. Im Zusammenhang mit → *Daten* beschreibt der → *Datennetzwerkeffekt* das Phänomen, dass Daten für Innovation genutzt werden, die wiederum mehr Daten generieren um das Produkt oder die Dienstleistung zu verbessern.
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.
Personendaten	Personendaten sind Angaben, → *Informationen* und Aussagen, die sich auf eine bestimmte oder mittels der Informationen bestimmbare Person beziehen. Eine rechtliche Definition findet sich in Art. 3 lit. a DSG.
Personendaten, besonders schützenswert	Besonders schützenswert sind Personendaten, bei denen eine besondere Gefahr der Persönlichkeitsverletzung besteht, bspw. Gesundheitsdaten. Eine rechtliche Definition findet sich in Art. 3 lit. c DSG.
Plattformen	Bestimmtes Nutzungsmodell; ein einziges Unternehmen sammelt, verknüpft und analysiert «in house» die → *Daten*, welche über eine (meistens globale) Plattform generiert werden, um daraus Dienstleistungen an Kundinnen und Kunden auf verschiedenen Märkten anzubieten; Dienstleistungen bauen auf dem Sammeln und Analysieren von Daten auf allen drei Märkten auf; es kann, muss sich aber nicht um einen → *Datenraum* handeln.
Profiling	Jede Art der automatisierten Bearbeitung von → *Personendaten*, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Eine rechtliche Definition wird im neuen Datenschutzgesetz verankert sein in Art. 5 lit. f revDSG.

Privacy-by-Design	Übergreifender Grundsatz und Ausgangspunkt der Betrachtung (Metagrundsatz). Im Wesentlichen soll der Verantwortliche sich frühzeitig Gedanken machen, wie er die Einhaltung des Datenschutzes über den gesamten → *Datenzyklus* sicherstellt.
Privacy Shield	Das Privacy Shield («Datenschutzschild») bietet einen Rechtsrahmen für die Übermittlung von → *Personendaten* aus der Schweiz in die USA (Swiss-US Privacy Shield) oder von der EU in die USA (EU-US Privacy Shield).
Privatsphären-Paradox	Häufig zu beobachtendes Phänomen, wonach 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.
Pseudonymisierung	Verarbeitung → *Personendaten* in einer Weise, dass diese 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.
Sachdaten	→ *Daten*, welche keinen Personenbezug haben und somit nicht vom Datenschutzgesetz erfasst sind.
Schnittstellen	Teil eines Softwaresystems, welcher der Kommunikation mit anderen Systemen oder anderen Teilen eines Systems dient. In der Regel handelt es sich um Funktionen, die auf eine parametrisierte Anfrage einen Datenauszug in standardisierter Form zurückliefern.
Shared Data	→ *Daten*, die für bestimmte Gruppen oder nur zu bestimmten Bedingungen bereitgestellt werden.
Standards	Dokumentierte, konsistente und etablierte Vereinbarung über die Struktur und das Format gemeinsamer → *Daten*, → *Schnittstellen* und Prozesse.
Standardisierung	Entwicklung von → *Standards*.
Statische Daten	→ *Daten* in einem festen → *Datensatz*, d.h. Daten, die nach ihrer Generierung und Erfassung unverändert bleiben (zeitliche Komponente von Daten). Im Gegensatz dazu → *dynamische Daten.*
Vertikale Integration	Bezeichnet die vor- oder nachgelagerte Eingliederung von Wertschöpfungsstufen in ein Unternehmen, welche zuvor von anderen Marktakteuren erbracht wurden.
Wissen	Resultat der Analyse von → *Informationen* – oder direkt von → *Daten* – auf der Basis eines Analyse-Rasters, einer Theorie, einer bestimmten «Perspektive». Erst die Anwendung einer «Perspektive» führt dazu, dass Daten und/oder Informationen einen Sinn ergeben und handlungsanleitend wirken.

9 Abkürzungsverzeichnis

API	Application Programming Interface
Art.	Artikel
Abs.	Absatz
BAV	Bundesamt für Verkehr
BAKOM	Bundesamt für Kommunikation
BBL	Bundesamt für Bauten und Logistik
BBl	Bundesblatt
BFE	Bundesamt für Energie
BPUK	Schweizerische Bau-, Planungs- und Umweltdirektoren-Konferenz
bspw.	beispielsweise
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft (SR 101)
bzw.	beziehungsweise
CEN	European Committee for Standardization / Europäisches Komitee für Normung
d.h.	das heisst
DSG	Bundesgesetz über den Datenschutz (SR 235.1)
revDSG	revidierte Fassung zum Bundesgesetz über den Datenschutz
DSCC	Data Science Competence Center / Kompetenzzentrum für Datenwissenschaft
DV	Direktion für Völkerrecht
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDK	Schweizerische Konferenz der kantonalen Erziehungsdirektoren
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFD	Eidgenössischen Finanzdepartement
EIF	European Interoperability Framework / Europäischer Interoperabilitätsrahmen
EMRK	Konvention zum Schutz der Menschenrechte und Grundfreiheiten (SR 0.101)
EPD	Elektronisches Patientendossier
EPDG	Bundesgesetz über das elektronische Patientendossier (SR 816.1)
ETSI	European Telecommunications Standards Institute / Europäisches Institut für Telekommunikationsnormen
et al.	et alii = und weitere
etc.	et cetera
EuGH	Europäische Gerichtshof
EU	Europäische Union
ff.	fortfolgende
FHIR	Fast Healthcare Interoperability Resources
FinTech	Finanztechnologie
GKG	Koordinationsorgan für Geoinformation des Bundes
IDSA	International Data Spaces Association
IEC	International Electrotechnical Commission / Internationale Elektrotechnische Kommission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGE	Eidgenössisches Institut für Geistiges Eigentum
IHE	Integrating the Healthcare Enterprise

IKT	Informations- und Kommunikationstechnik
inkl.	inklusive
ISO	International Standards Organisation / Internationale Organisation für Normung
IT	Informationstechnik
ITU	International Telecommunication Union / Internationale Fernmeldeunion
KI	Künstliche Intelligenz
KMU	Kleine und mittlere Unternehmen
lit.	litera
MODIG	Bundesgesetz über die Mobilitätsdateninfrastruktur
MRI-Daten	Magnetresonanztomographie Daten
NADIM	Nationale Datenvernetzungsinfrastruktur Mobilität
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) (SR 220)
öV	öffentlicher Verkehr
S.	Seite
SATW	Schweizerische Akademie für Technische Wissenschaften
SBFI	Staatssekretariat für Bildung, Forschung, und Innovation
SBVg	Schweizerische Bankiervereinigung
SDA	Swiss Data Alliance
SECO	Staatssekretariat für Wirtschaft
SHED	Swiss Hub for Energy Data
SIF	Staatssekretariat für internationale Finanzfragen
sog.	sogenannte
UNCTAD	United Nations Conference on Trade and Development
UNGA	United Nations General Assembly
UNO-Pakt I	Internationaler Pakt über wirtschaftliche, soziale und kulturelle Rechte (SR 0.103.1)
UNO-Pakt II	Internationaler Pakt über bürgerliche und politische Rechte (SR 0.103.2)
US	United States
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
WBF	Eidgenössische Departement für Wirtschaft, Bildung und Forschung
W3C	World Wide Web Consortium
WTO	World Trade Organisation / Welthandelsorganisation
ZGB	Schweizerisches Zivilgesetzbuch (SR 210)

10 Quellenverzeichnis

Asadullah A., Faik I. and Kankanhalli A. (2018), «Digital Platforms: A Review and Future Directions», Conference Paper for the Twenty-Second Pacific Asia Conference on Information Systems, Japan, <https://www.researchgate.net/publication/327971665_Digital_Platforms_A_Review_and_Future_Directions> (Zugriff am 03.01.2022)

BAKOM, EDA, SDA und SATW (2020), «Diskussionspapier Digitale Selbstbestimmung», <https://digitale-selbstbestimmung.swiss/home/245-2/> (Zugriff am 03.01.2022)

BAV (2022), «Erläuternde Bericht zum Bundesgesetz über die Mobilitätsdateninfrastruktur (MODIG)», <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2022/2/cons_1/doc_5/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2022-2-cons_1-doc_5-de-pdf-a.pdf> (Zugriff am 03.02.2022)

BFE (2021), «Datahub Schweiz: Kern zukünftiger Dateninfrastruktur digitalisierter Strom- und Gasmärkte», <https://www.bfe.admin.ch/bfe/de/home/news-und-medien/publikationen.exturl.html/aHR0cHM6Ly9wdWJkYi5iZmUuYWRtaW4uY2gvZGUvcHVibGljYX/Rpb24vZG93bmxvYWQvMTA2MjI=.html> (Zugriff am 03.01.2022)

Blankertz A. (2020), «Designing Data Trusts: Why We Need to Test Consumer Data Trusts Now», Stiftung Neue Verantwortung, <https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_d.pdf> (Zugriff am 03.01.2022)

Bundesrat (2019), «Gesundheitspolitische Strategie des Bundesrates 2020-2030», <https://www.bag.admin.ch/bag/de/home/strategie-und-politik/gesundheit-2030/gesundheitspolitische-strategie-2030.html> (Zugriff am 03.01.2022)

Bundesrat (2020a), «Aussenpolitische Strategie 2020-2023», <https://www.eda.admin.ch/dam/eda/de/documents/publications/SchweizerischeAussenpolitik/Aussenpolitische-Strategie-2020-23_DE.pdf> (Zugriff am 03.01.2022)

Bundesrat (2020b), «Strategie Digitale Schweiz», <https://www.digitaldialog.swiss/de/> (Zugriff am 03.01.2022)

Bundesrat (2020c), «Strategie Digitalaussenpolitik 2021-2024», <https://www.eda.admin.ch/dam/eda/de/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_DE.pdf> (Zugriff am 03.01.2022)

Bundesrat (2021), Botschaft zum Bundesgesetz über eine sichere Stromversorgung mit erneuerbaren Energien vom 18. Juni 2021, BBl 2021, 1666 ff.

Bundesrat und BPUK (2020), «Strategie Geoinformation Schweiz» <https://www.geo.admin.ch/de/ueber-geo-admin/leistungsauftrag/strategie-und-umsetzung.html> (Zugriff am 03.03.2022)

Collovà P. et al. (2021), «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung», Berner Fachhochschule

De La Chapelle B. and Porciuncula L. (2021), «We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty», Internet and Jurisdiction Policy Network, <https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf> (Zugriff am 03.01.2022)

Digitale Verwaltung Schweiz (2022), «E-Government Architektur für den strategischen Umsetzungsplan erarbeiten und führen», <https://www.digitale-verwaltung-schweiz.ch/umsetzungsplan/umsetzungsplan-e-government-schweiz/uz14-e-govenment-architektur> (Zugriff am 04.03.2022)

EDÖB (2020), «Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG», <https://www.newsd.admin.ch/newsd/message/attachments/64258.pdf> (Zugriff am 03.01.2022)

EDUCA (2021), «Digitalisierung in der Bildung: Bericht im Auftrag des SBFI und der EDK im Rahmen des Bildungsmonitorings», Bern, <https://www.educa.ch/sites/default/files/2021-10/Digitalisierung_in_der_Bildung.pdf> (Zugriff am 05.01.2022)

EuGH (2020), «Data Protection Commissioner gegen Facebook Ireland Limited und Maximilian Schrems», <https://curia.europa.eu/juris/liste.jsf?num=C-311/18> (Zugriff am 03.01.2022)

Europäische Kommission (2016), «Study on Data Sharing between Companies», <http://publications.europa.eu/resource/cellar/2d6d436e-4832-11e8-be1d-01aa75ed71a1.0002.01/DOC_1> (Zugriff am 03.01.2022)

Europäische Kommission (2017), «New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations», <https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf> (Zugriff am 01.02.2022)

Europäische Kommission (2018a), «Towards a common European Data Space», <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0232&from=EN> (Zugriff am 03.01.2022)

Europäische Kommission (2018b), «Staff Working Document: Guidance on Sharing Private Sector Data in the European Data Economy», <https://digital-strategy.ec.europa.eu/en/news/staff-working-document-guidance-sharing-private-sector-data-european-data-economy> (Zugriff am 03.01.2022)

Europäische Kommission (2021), «Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest: Final Report prepared by the High-Level Expert Group on Business-to-Government Data Sharing», <https://op.europa.eu/en/publication-detail/-/publication/d96edc29-70fd-11eb-9ac9-01aa75ed71a1> (Zugriff am 03.01.2022)

Finck M. and Pallas F. (2020), «They Who Must Not Be Identified: Distinguishing Personal from Non-Personal Data under GDPR» in International Data Privacy Law, Vol. 10, Issue 1, S. 11-36

Findlay M. and Remolina N. (2021), «The Paths to Digital Self-Determination: A Foundational Theoretical Framework», SMU Centre for AI & Data Governance Research Paper, Issue 3

Gadient B. M. et al. (2018), «Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit», <https://www.newsd.admin.ch/newsd/message/attachments/53591.pdf> (Zugriff am 03.01.2022)

Ghielmini S. et al. (2021), «Grund-und Menschenrechte in einer digitalen Welt», Schweizerisches Kompetenzzentrum für Menschenrechte, <https://www.skmr.ch/cms/upload/pdf/2021/210518_Grund_und_Menschenrechte_in_einer_digitalen_Welt.pdf> (Zugriff am 03.01.2022)

Goldstein E., Gasser U. and 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», Berkman Klein Center, <https://medium.com/berkman-klein-center/data-commons-version-1-0-a-framework-to-build-toward-ai-for-good-73414d7e72be> (Zugriff am 01.02.2022)

Häfelin U. et al. (2020), «Schweizerisches Bundesstaatsrecht», Schulthess, Zürich/Basel/Genf

IDC (2020), «Analysis of the Data Market: 2017-2018, 2025 for Switzerland and other EU28 Member States», <https://www.ige.ch/fileadmin/user_upload/recht/gesellschaft/e/200327_Data_Market_in_CH.pdf> (Zugriff am 03.01.2022)

IGE (2021), «Zugang zu Sachdaten in der Privatwirtschaft», <https://www.ige.ch/fileadmin/user_upload/recht/gesellschaft/d/20210301_Bericht_IPI_Zugang_zu_Sachdaten_in_der_Privatwirtschaft.pdf> (Zugriff am 03.01.2022)

Jentzsch N. (2017), «Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds – Ökonomische Rahmenbedingungen innovativer Lösungen zu Einwilligungen im Datenschutz», Deutsches Institut für Wirtschaftsforschung, <https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_Gutachten_Die_persoenliche_Datenoekonomie_Anhang_2_final.pdf> (Zugriff am 03.01.2022)

Mulgan G. and Straub V. (2019), «The New Ecosystem of Trust», Nesta, <https://www.nesta.org.uk/blog/new-ecosystem-trust/> (Zugriff am 03.01.2022)

OECD (2019), «Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use Across Societies», <https://www.oecd-ilibrary.org/sites/276aaca8-en/index.html?itemId=/content/publication/276aaca8-en> (Zugriff am 03.01.2022)

Purtova N. (2017), «The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law» in Law, Innovation and Technology, Vol. 10, Issue 1, S. 40-81

SBVg (2020), «Open Banking: Eine Auslegeordnung für den Schweizer Finanzplatz», <https://www.swissbanking.ch/_Resources/Persistent/6/7/c/e/67ce5ff1973209d0a55ab42d5f52b15955e3dab1/SBV_Auslegeordnung_OpenBanking_DE.pdf> (Zugriff am 03.02.2022)

Schneider I. (2019), «Governance der Datenökonomie: Politökonomische Verfügungsmodelle zwischen Markt, Staat, Gemeinschaft und Treuhand» in *Ochs C. et al.* (Hrsg.), «Die Zukunft der Datenökonomie: Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz», Springer VS, Wiesbaden, S. 143-180

SIF (2022), «Digital Finance: Handlungsfelder 2022+», <https://www.newsd.admin.ch/newsd/message/attachments/70095.pdf> (Zugriff am 02.02.2022)

Svantesson D. (2020), «Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines», OECD Digital Economy Papers, No. 301, OECD Publishing, Paris, <https://www.oecd-ilibrary.org/docserver/7fbaed62-en.pdf?expires=1641307122&id=id&accname=guest&checksum=E58EE358750DCA2DC01122DFD6D1BD8F> (Zugriff 03.01.2022)

Swiss Economics (2021), «Vertrauenswürdige Digitale Datenräume: Schlussbericht Konzeptualisierung und Anforderungen» (liegt Autorenteam vor)

UNCTAD (2021), «Digital Economy Report 2021: Cross-Border Data Flows and Development – For Whom the Data Flow», <https://unctad.org/system/files/official-document/der2021_en.pdf> (Zugriff am 03.01.2022)

UNGA (2015), «Transforming our World: The 2030 Agenda for Sustainable Development (A/RES/70/1)»,<https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1%20&Lang=E> (Zugriff am 03.01.2022)

Zhu F. and Liu Q. (2018), «Competing with Complementors: An Empirical Look at Amazon.com» in Strategic Management Journal, Vol. 39, Issue 10, S. 2618-2642

Anhang 1: Übersicht relevante Berichte

Bereich	Titel	Zuständiges Amt	Datum
Datenpolitik generell	Bericht Auslegeordnung Datenpolitik	BAKOM	Juni 2016
	Eckwerte einer Datenpolitik	BAKOM	Mai 2018
	Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit	Expertengruppe	September 2018
	Zugang zu Sachdaten in der Privatwirtschaft	IGE	März 2021
Datenpolitik sektoriell	Daten in der Bildung – Daten für die Bildung: Grundlagen und Ansätze zur Entwicklung einer Datennutzungspolitik für den Bildungsraum Schweiz	Educa im Auftrag vom SBFI und EDK	Mai 2019
	Strategie Geoinformation Schweiz	Bundesrat und BPUK	Dezember 2020
	Data Hub Schweiz – Kern zukünftiger Dateninfrastrukturen digitalisierter Strom- und Gasmärkte	BFE	August 2021
	Digital Finance: Handlungsfelder 2022+	SIF	Februar 2022
	Bericht zum Bundesgesetz über die Mobilitätsdateninfrastruktur	BAV	Februar 2022
Digitalpolitik	Bericht Intermediäre und Kommunikationsplattformen	BAKOM	November 2021
	Bericht Digitaler Service Public	BAKOM	Q3 2022
Digitale Infrastruktur	Bedarfsabklärung Swisscloud	ISB	Dezember 2020
KI	Bericht der interdepartementalen Arbeitsgruppe Künstliche Intelligenz	SBFI	Dezember 2019
	Leitlinien Künstliche Intelligenz für die Bundesverwaltung	BAKOM	November 2020
	KI und Völkerrecht	EDA	Q2 2022

Anhang 2: Komponenten eines Datenraums

Die Operationalisierung und die Datennutzung innerhalb eines Datenraums hängt von mehreren Komponenten ab. In einem Datenraum lassen sich verschiedene Akteure identifizieren, die unterschiedliche Rollen übernehmen und verschiedene Datenarten für bestimmte Zwecke nutzen. Des Weiteren liegen Datenräumen unterschiedliche Dateninfrastrukturen und Gouvernanzformen zugrunde. Nachfolgend werden diese Komponenten näher beleuchtet.[92]

1. Akteure und Rollen innerhalb eines Datenraumes

In einem Datenraum lassen sich verschiedene Akteure identifizieren, die unterschiedliche Rollen übernehmen. Die zentralsten Rollen betreffen den Betrieb und die Organisation eines Datenraumes. Die **Betreiber der Infrastruktur** sind zuständig für das Funktionieren der technischen Infrastruktur des Datenraums. Sie können auch Dienstleistungen im Zusammenhang mit dem Datenraum anbieten, wie bspw. die Analyse und Weiterbearbeitung von Datensätzen (→ Datensatz). In vielen Datenräumen besteht eine weitere Rolle in der **Sicherstellung der Gouvernanz**, also der Durchsetzung der Bedingungen und Regeln für die Datennutzung.[93] Sofern dieselbe Organisation sowohl die technische Infrastruktur betreibt als auch für die Sicherstellung der Gouvernanz zuständig ist, spricht man von einer **Datenraumbetreiberin**. Die Gouvernanzformen (d.h. die Spielregeln für den Datenraum) können auch von einer übergeordneten – privaten oder öffentlichen – **Trägerschaft** definiert werden, welche dann auch die Aufgaben der Datenraumbetreiberin bestimmt.

Nebst den Betriebs- und Organisationsrollen können weitere Rollen identifiziert werden, welche sich im Hinblick darauf unterscheiden, ob sie auf der **Datenangebots-** oder **Datennachfrageseite** aktiv sind. Dabei können die gleichen Akteure mehrere der folgenden Rollen einnehmen:

Angebot		**Nachfrage**	
Daten-produzenten	Natürliche oder juristische Personen, welche Daten generieren und erfassen.	**Datennutzer/ Datenbezüger**	Natürliche oder juristische Personen, die Daten von Datenräumen nutzen bzw. beziehen.
Datenanbieter (auch: Daten-lieferant)	Natürliche oder juristische Personen, die Daten über einen Datenraum bereitstellen.		

Diese Rollen sind abhängig von den Zielen und Zwecken der verschiedenen Akteure in einem Datenraum. Ein bestimmter Akteur kann also verschiedene Rollen einnehmen. So kann bspw. ein Spital oder ein Patient durch Untersuchungen, Behandlungen und Operationen gewisse Daten generieren (→ Datenproduzent) und diese dann in einem Datenraum zu Forschungszwecken zur Verfügung stellen (→ Datenanbieter). Gleichzeitig kann das Spital andere Daten aus diesem Datenraum nutzen, um die eigenen Systeme zu verbessern (→ Datennutzer).

[92] Für die grafische Darstellung eines Datenraummodells, siehe Kapitel 3.3.1.
[93] Eine Ausnahme bilden Datengemeinschaften, bei welchen die Gouvernanz kollektiv wahrgenommen wird.

2. Datenarten

Generell lassen sich Datenarten aufgrund verschiedener Kriterien unterscheiden. In diesem Bericht wird insbesondere der gesetzlichen Unterscheidung zwischen **Personen- und Sachdaten** sowie **statischen und dynamischen Daten** (zeitliche Komponente) und **Daten in Bezug auf ihre Zugänglichkeit und Nutzniessung** Beachtung geschenkt.

Eine wichtige Unterscheidung betrifft die Frage, ob Daten einen *Personenbezug* aufweisen und somit dem Datenschutzrecht unterstellt sind. **Personendaten** sind demnach «alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen» (Art. 5 lit. a revDSG). Diese Daten sind durch das Datenschutzgesetz explizit geschützt. Dem gegenüber stehen **nicht-personenbezogene Daten** oder **Sachdaten,** die sich *nicht* auf bestimmte oder bestimmbare natürliche Personen beziehen. Im Gegensatz zu Personendaten sind Sachdaten nicht *per se* reguliert. Es ist wichtig zu erwähnen, dass die Unterscheidung zwischen Personendaten und Sachdaten in der Realität teilweise schwierig zu bewerkstelligen ist.[94] Grund dafür ist, dass die Verbindung von verschiedenen Sachdatenquellen oder Sachdatensätzen oftmals Rückschlüsse auf Personen zulassen. Diese Entwicklung beschleunigt sich mit der ständig wachsenden Verfügbarkeit von Datensätzen. Als Reaktion darauf werden zunehmend auch **Daten in anonymisierter Form** oder **pseudonymisierter Form** (→ Pseudonymisierung) genutzt. Der grosse Vorteil dabei ist, dass unter Umständen zentrale Erkenntnisgewinne möglich sind, ohne dass die Privatsphäre einer Person verletzt wird. Dabei ist zu beachten, dass eine Anonymisierung in Bezug auf eine mögliche Re-Identifikation generell einen besseren Schutz als eine Pseudonymisierung bietet. Ähnliche Ziele verfolgen auch Mechanismen wie *differential privacy*. Dabei werden mittels *Algorithmen* (→ Algorithmus) statistisch relevante Informationen aus einem Datensatz berechnet, ohne dass es möglich wäre zu eruieren, ob die Daten einer bestimmten Person im ursprünglichen Datensatz enthalten waren oder nicht.

Ebenfalls von zunehmender Bedeutung ist die Unterscheidung bezüglich der *zeitlichen Komponente* von Daten. Dabei wird insbesondere zwischen **statischen** und **dynamischen Daten** (→ statische Daten; → dynamische Daten) unterschieden. Statische Daten sind Daten in einem festen Datensatz, d.h. Daten, die nach ihrer Generierung und Erfassung unverändert bleiben. Dynamische Daten sind Datensätze, die sich ändern sobald neue Informationen verfügbar werden. Dies trägt zur Wahrung der Integrität des Datensatzes bei. Es ist jedoch auffallend, dass dynamische Daten, aufgrund ihrer Genauigkeit und der Möglichkeit personalisierte, individualisiert oder sonst den Gegebenheiten angepasste Dienstleistungen zu erbringen, zunehmend bevorzugt werden.

Des Weiteren lassen sich Daten aufgrund ihrer unterschiedlichen Zugänglichkeit unterscheiden. Dabei wird zwischen *closed data*, *shared data* und *open data* unterschieden (→ Closed Data; → Shared Data; → Open Data). **Closed data** sind Sach- und Personendaten, die unter striktem Verschluss und nur einem eingeschränkten Benutzerkreis innerhalb einer Organisation zugänglich sind (bspw. marktrelevante Daten eines Unternehmens). **Shared data** sind Sach- und Personendaten, die unter bestimmten Bedingungen (bspw. gegen Bezahlung, innerhalb eines gewissen Gouvernanzrahmens) mit anderen Akteuren oder Organisationen geteilt werden. Schlussendlich sind **open data** Daten, die keine schützenswerten Informationen enthalten und für die Öffentlichkeit zur freien Nutzung zugänglich gemacht werden. Unter diese Kategorie fallen **open government data** (→ Open Government Data), also Daten der öffentlichen Hand, die frei zugänglich gemacht werden.

[94] Siehe dazu *Purtova N. (2017)*, «The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law»; *Finck M. and Pallas F. (2020)*, «They Who Must Not Be Identified: Distinguishing Personal from Non-Personal Data under GDPR».

Eine weitere Unterscheidung besteht in der Betrachtung der Daten im Hinblick auf eine Nutzniessung. Diese Unterscheidung ist eng an die Frage der Datengouvernanz geknüpft. Hier lässt sich zwischen *data as public good*, *data as infrastructure* und *data as commodity* unterscheiden (→ Data as Public Good; → Data as Infrastructure; → Data as Commodity). **Data as public good** beschreibt Daten, die der Öffentlichkeit als Ganzes zugänglich gemacht werden, da sie als Teil des Gemeinwohls betrachtet werden. Im Bereich der Zugänglichkeit fallen sie damit zwingend unter *open data* und sind in der Regel Sachdaten. Hier lässt sich entsprechend *open government data* als Beispiel anbringen. **Data as infrastructure** sind Daten, die als essentiell betrachtet werden, um das Funktionieren von gesellschaftlich relevanten Systemen (bspw. das Mobilitätssystem in der Schweiz) zu garantieren. Die Unterscheidung zwischen *data as public good* und *data as infrastructure* ist nicht immer trennscharf. So können *data as infrastructure* in gewissen Bereichen auch die Charakteristik von *data as public good* und *open data* haben und öffentlich verfügbar sein. *Data as infrastructure* kann auch als *shared data* nur für einen eingeschränkten Benutzerkreis verfügbar gemacht werden, insbesondere wenn dies sensitive Daten betrifft. Schliesslich beschreibt **data as commodity** Daten, welche zu einem wirtschaftlichen Zweck eingesetzt werden.

Unterscheidung	**Beschreibung**		
Personenbezug	Personendaten	Sachdaten	
Zeitliche Komponente	dynamische Daten	statische Daten	
Zugänglichkeit	open data	shared data	closed data
Nutzniessung	data as public good	data as infrastructure	data as commodity

3. Datenzweck

Daten sind nicht *per se* wertvoll, sondern erhalten ihren Wert erst im Zusammenhang mit der Verfolgung eines bestimmten Zwecks (Primärnutzung). Dieser muss zuerst identifiziert werden und kann bspw. auf die Entwicklung von Lösungen im Gesundheitsbereich oder die Bekämpfung des Klimawandels abzielen als auch zur Verbesserung der Mobilität beitragen. Ein solch gemeinsamer Zweck kann Akteuren innerhalb eines Sektors Anreize für eine gemeinschaftliche Datennutzung geben und neue Möglichkeiten eröffnen.

Neben dieser Primärnutzung von Daten zu einem bestimmten Zweck besteht auch ein grosses Potenzial darin, Daten über ihren ursprünglichen Zweck hinaus zugänglich zu machen. Diese Art der Nutzung wird Sekundärnutzung genannt, welche es verschiedenen Akteuren ermöglicht, in unterschiedlichen Sektoren Daten zeitgleich zu verschiedenen Zwecken zu nutzen. Dies ermöglicht Innovation in Bereichen, die vorher gar nicht in Betracht gezogen wurden. So dient bspw. die Analyse von MRI-Daten einer Person der massgeschneiderten Therapie derselben (Primärnutzung). Aus der Analyse einer Vielzahl von MRI-Daten lassen sich danach wiederum allgemeine und weitergehende Erkenntnisse für den Gesundheitsbereich gewinnen und allenfalls neue Präventions- und Behandlungstherapien entwickeln (Sekundärnutzung).

Am Beispiel der MRI-Daten, der verschiedenen Rollen der Akteure in einem Datenraum und den unterschiedlichen Datenarten lässt sich verdeutlichen, dass Daten einen Datenzyklus durchlaufen (→ Datenzyklus): sie werden generiert, verfügbar und zugänglich gemacht sowie für einen bestimmten Zweck genutzt, gehalten, wiederverwendet und ausgetauscht.

Wo Personendaten bearbeitet werden, ist der datenschutzrechtliche Grundsatz der Zweckbindung zu beachten.[95] Bei der Datenbearbeitung durch Staatsorgane müssen die Bearbeitungszwecke im anwendbaren Recht vorgesehen sein. Bei der Datenbearbeitung durch Private müssen sie vom jeweiligen Rechtfertigungsgrund (Art. 31 revDSG) gedeckt sein, insbesondere von der Einwilligung der betroffenen Person.

4. Dateninfrastruktur

Ein Datenraum benötigt immer auch eine Dateninfrastruktur (→ Dateninfrastruktur). Je nach Verteilstrategie kann diese zentral oder dezentral ausgestaltet sein. Demnach findet der Datenaustausch und die Datenspeicherung (und allenfalls auch die Datenbearbeitung) entweder auf einer speziell geschaffenen, zentralisierten Struktur statt oder wird dezentral direkt zwischen Datenanbieter und Datennutzer bewerkstelligt. Es lassen sich vermehrt auch hybride Formen beobachten, in denen Teile des Datenraumes (bspw. für gewisse Datensätze, die direkt von den Datenanbietern unterhalten werden können oder unterhalten werden müssen) dezentral ausgestaltet sind und andere Elemente (insbesondere Datensets, die weitere Aufbereitung brauchen oder deren Weitergabe bestimmten Kriterien unterliegt) zentral von der Betreiberin verwaltet werden.

5. Gouvernanzformen

Datenräume können unterschiedlich organisiert sein. In der Praxis entstehen deshalb auch die unterschiedlichsten Formen von Datenräumen (siehe Kapitel 5). Jeder Datenraum wird dabei durch bestimmte Rahmenbedingungen und Regeln organisiert. Diese werden über die Gouvernanz des Datenraums festgelegt und anschliessend durchgesetzt. Eine wichtige Unterscheidung ist dabei zwischen Datenräume, die allen offenstehen und Datenräume, die exklusiv zwischen einigen bestimmten Akteuren entstehen (siehe auch weiter oben *open data* und *shared data*) zu machen. Grundsätzlich können aber verschiedene Gouvernanzformen sowohl auf offene als auch exklusive Datenräume angewendet werden. Aufgrund der unterschiedlichen Ausgestaltungen sowie der verschiedenen Verwendung der Begriffe ist eine einheitliche Kategorisierung von Gouvernanzformen schwierig.[96] Grundsätzlich lassen sich aber folgende Ansätze unterscheiden:

Datenkooperative	Organisation mit gleichwertiger Mitsprache und Kontrolle seiner Mitglieder. Rahmenbedingungen, Regeln und deren Durchsetzung werden durch alle Mitglieder festgelegt und deren Einhaltung in transparenter Weise überprüft.
Datenclub	Organisation, in der Mitglieder aufgrund ihrer Rolle und Beteiligung unterschiedlichen Einfluss haben können. Rahmenbedingungen, Regeln und deren Durchsetzung werden den Rollen entsprechend definiert.
Datengemeinschaft	Organisation, in der Daten gegenseitig direkt zur Verfügung gestellt werden, ohne dass eine Betreiberorganisation gebraucht wird. Nutzungsregeln werden gemeinschaftlich festgelegt und durchgesetzt.

[95] Art. 6 Abs. 3 revDSG: «Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist».
[96] *Collovà P. et al.* (*2021)*, «Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung», S. 27.

Neben diesen Gouvernanzformen bestehen auch Datenräume, welche die Kontrolle für Individuen vollständig ins Zentrum stellen und deren Organisation auf die Bedürfnisse des Individuums ausgerichtet sind. Dabei handelt es sich vorwiegend um Datentreuhänder und persönliche Datenspeicher. Als solche können diese Formen auch in grössere Datenräume integriert werden und damit die Gesamtkontrolle stärken.

Datentreuhänder	Organisation, die eine unabhängige und treuhänderische (d.h. unparteiische, umsichtige, transparente und loyale) Verwaltung der Daten im Interesse der betroffenen Person anbietet. Sie setzt die Präferenzen der betroffenen Person stellvertretend direkt bei Dienstleistungsanbietern oder in Datenräumen durch.
Persönliche Datenspeicher	Organisation, die eine unabhängige und sichere Speicherung der Daten einer einzelnen Person anbietet. Dritten wird nur auf direkte Anweisung des Individuums Zugang zu diesen Daten gewährt.

Anhang 3: Empfehlungen zu den Grundprinzipien

Transparenz

Empfehlungen zum Grundprinzip Transparenz

Umfang

- Der Umfang der bereitgestellten Information sollte gewisse Minimalinhalte enthalten (von Sektor definiert).
- Es sollten ausreichend Informationen über das Geschäftsmodell des Datenraumbetreibers sowie über die Datennutzung bereitgestellt werden, damit der Zweck der Datenbearbeitung ersichtlich ist.
- Ebenfalls ist darzulegen, welche Akteure Zugang zu den entsprechenden Daten haben.

Nachvollziehbarkeit

- Die Komplexität der Informationen soll so tief wie möglich gehalten werden und dem jeweiligen Zielpublikum angepasst sein.
- Nutzerinnen und Nutzer verfügen über Prozesse und Mechanismen mittels denen sie die Datenbearbeitung nachvollziehen können.
- Wo möglich sollen weitere Hilfsmittel (bspw. visueller oder audiovisueller Art) verwendet werden, um Informationen niederschwelliger zu vermitteln.
- Auf allfällige Risiken soll in der Kommunikation explizit hingewiesen werden.

Wirksamkeit

- Die zur Verfügung gestellte Information soll proaktiv kommuniziert und einfach aufzufinden sein.
- Kommunikationskanäle und -formen sollen der Situation angepasst sein.

Überprüfung

- Vertrauenswürdige Datenräume sollen öffentlich bekannt sein und ihre Tätigkeiten darlegen.
- Datenräume und deren Betreibern sollen bezüglich ihrer Vertrauenswürdigkeit von Dritten eingeschätzt werden können.

Kontrolle

Empfehlungen zum Grundprinzip Kontrolle

Steuerungsmöglichkeiten

- Nutzerinnen und Nutzer sollen entscheiden können, wem sie wann welche Daten preisgeben.
- Nutzerinnen und Nutzer sollen die Bearbeitung ihrer Daten wo immer möglich (und insbesondere bei sensitiven Daten) einschränken können.
- Die Freigabe von Daten muss reversibel sein.
- Die Einwilligung einer Datennutzung muss zeitlichen und inhaltlichen Beschränkungen unterliegen.

Freiwilligkeit und Wahlfreiheit

- Nutzerinnen und Nutzer sollen ihre Anbieter frei wählen und ohne Hindernisse wechseln können.
- Einem beteiligten Akteur sollen aufgrund einer Entscheidung keinerlei Nachteile oder Schlechterstellungen erwachsen.
- Nutzerinnen und Nutzern soll es auch offenstehen, die Kontrolle und Verwendung der eigenen Daten an Dritte zu delegieren und ihnen die diesbezüglich nötigen Vollmachten zu erteilen.

Schutz vor Kontrollverlust

- Es sollen klare Vorkehrungen und Prozesse bestehen, um Sicherheitsrisiken für den Datenraum und involvierte Akteure zu erkennen, zu steuern und zu mildern.
- Es sollen verbindliche Handlungsanleitungen bestehen, falls die Sicherheit der zur Verfügung gestellten Daten kompromittiert werden sollte.

Fairness

Empfehlungen zum Grundprinzip Fairness

Verhältnismässigkeit

- Die Bearbeitung von Daten ist stets gemäss dem Verhältnismässigkeitsprinzip zu gestalten.

Faire Last- und Nutzenverteilung

- Kosten und Nutzen der Sammlung, Aufbereitung und Speicherung der Daten sollen gerecht verteilt werden.
- Die Teilnahme an vertrauenswürdigen Datenräumen soll einen gezielten Mehrwert für Datenproduzenten und Datennutzer ergeben.

Diskriminierungsfreiheit

- Datenräume sollen diskriminierungsfrei ausgestaltet werden.

Unabhängigkeit

- Der Betrieb eines Datenraumes soll von jeglichen Interessenskonflikten befreit sein.
- Es sollen einfache und transparente Verfahren für die Repräsentation der Interessen von Akteuren mit beschränktem Einfluss und fehlender Marktmacht (insbesondere Einzelpersonen) bestehen.

Verantwortlichkeit

Empfehlungen zum Grundprinzip Verantwortlichkeit

Gouvernanzmechanismen

- Es sollen klare Regeln und Strukturen für Verantwortlichkeiten, Handlungen und Entscheidungsfindungen im Zusammenhang mit dem Betrieb des Datenraumes bestehen.

Durchsetzungsmechanismen

- Es bestehen Mechanismen, welche es bei einer Verletzung erlauben, Ansprüche durchzusetzen.
- Massnahmen innerhalb eines Datenraums sind klar zu begründen.

Effizienz

Empfehlungen zum Grundprinzip Skalierbarkeit

Hohe Datenqualität

- Daten sollen dank einem umfassenden Qualitätsmanagement in ausreichender Qualität vorliegen.

Interoperabilität (eng und breit)

- Die technische Infrastruktur und Datenformate sollen dank klaren und gemeinsamen Standards und Formaten sowie offenen Schnittstellen innerhalb und zwischen Datenräumen kompatibel sein (enge Interoperabilität).
- Grundprinzipien sowie die praktische und normative Ausgestaltung soll mit anderen Datenräumen kompatibel sein (breite Interoperabilität).

Adaptierbarkeit

- Ein Datenraum soll sich verändernden Gegebenheiten flexibel anpassen können, ohne gegen die Grundprinzipien zu verstossen.