Arbeitspapier

Empfehlungen für eine bessere Nutzung personenbezogener Daten in der Schweiz

Stand 18.04.2023

Schweizerische Akademie der Technischen Wissenschaften SATW
St. Annagasse 18 | 8001 Zürich | +41 44 226 50 11 | info@satw.ch | www.satw.ch

Inhaltsverzeichnis

1 Excecutive Summary

Daten werden in der Regel für einen bestimmten Verwendungszweck erhoben, könnten aber darüber hinaus für beliebig viele weitere Zwecke genutzt werden. Um in der Schweiz eine solche Zweitnutzung von Daten zu fördern und das grosse wirtschaftliche und gesellschaftliche Potential[1] besser zu verwerten, braucht es entsprechende Rahmenbedingungen – insbesondere im Bereich Personendaten. Dabei gilt es, die digitale Selbstbestimmung der Schweizer Bürger:innen zu bewahren. Ausserdem sind Forschungsbedürfnisse wie auch wirtschaftliche Interessen zu berücksichtigen und aufeinander abzustimmen.

In Zusammenarbeit mit der Swiss Data Alliance SDA hat die SATW die drei Anwendungsbereiche Mobilität, Gesundheit und Bildung näher untersucht. Sie kommt zum Schluss, dass ein übergeordnetes Rahmengesetz, wie es die Motion 22.3890 «Rahmengesetz für die Sekundärnutzung von Daten» [2] fordert, dringend notwendig ist. Damit liesse sich ein übergeordneter Rahmen für Datenräume in der Schweiz schaffen, die eine gemeinsame Nutzung von Daten durch eine Vielzahl an Akteur:innen ermöglichen.

Datenräume sind in der Regel an Anwendungsbereiche wie Mobilität, Gesundheit oder Bildung gebunden. Diese weisen unterschiedliche Voraussetzungen und spezifische Gesetzgebungen, aber auch Gemeinsamkeiten auf. Ein Rahmengesetz, das übergeordnete Herausforderungen adressiert, könnte laufende Entwicklungen in unterschiedlichen Bereichen beschleunigen. Damit würde der Schweiz der Anschluss an die international laufenden Initiativen gelingen.

Es wird daher empfohlen, dass der Bund einen gesetzlichen Rahmen schafft, um die übergeordneten Herausforderungen bei der Einrichtung von vertrauenswürdigen Datenräumen zu adressieren und dadurch eine bessere Nutzung von Personendaten fördert. Dabei soll die digitale Selbstbestimmung der Bürger:innen berücksichtigt werden. Die Interessen der Forschung wie auch der Wirtschaft sollen angemessen berücksichtigt werden. Durch einen partizipativen Ansatz soll eine gemeinsame Vision erarbeitet werden. Wichtig ist auch, dass eine internationale Interoperabilität insbesondere mit europäischen Datenräumen angestrebt wird.

[1] Beispielhaft illustriert dies eine Studie Europäischen Kommission zu Open Data: The Economic Impact of Open Data; https://data.europa.eu/sites/default/files/the-economic-impact-of-open-data.pdf
[2] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20223890

2 Vorwort

von Matthias Michel, Ständerat (Zug)

Data Sharing Economy: Zusammenwirken aller Kräfte als Vertrauensbasis

Nach genau 30 Jahren hat das erste Schweizer Datenschutzgesetz ausgedient. Es wird ab 1. September 2023 durch eine Totalrevision abgelöst, was die Dynamik der digitalisierten Welt der letzten Jahrzehnte widerspiegelt. Globale Players, die inzwischen weit mehr als nur Kommunikation anbieten, nutzen unsere Daten, die wir ihnen mit jedem Einkauf per Internet oder an der Scan-Kasse freiwillig übermitteln, für die Bewirtschaftung ihrer breiten Angebote. Es kann nicht sein, dass die reine Marktmacht, rechtliche Freiräume und Grauzonen dazu führen, dass nur einige wenige von unseren Daten profitieren. Gerade Gesellschaft und Staat haben ein zentrales Interesse daran, solche Daten zu verwerten, um wichtige Bereiche wie Gesundheit, Verkehr, Energie und Bildung zu steuern und zu gestalten.

Auch private Akteure können ihre Produkte und Dienstleistungen effizienter und damit auch nachhaltiger ausrichten, wenn sie vorhandene Daten nutzen können. Und Individuen sollen erkennen, dass sie Nutzen ziehen von der Bewirtschaftung von Daten, die auch sie selber produzieren. Die Vorteile der Sharing Economy beschränken sich nicht auf Güter, sondern dürften bei Daten sogar noch grösser sein.

Gemeinsame Datenräume statt Einzelsilos sind angesagt. Entsprechend erfrischend ist es, dass der vorliegende Bericht von Verantwortlichen aus Wissenschaft, Wirtschaft, Verwaltung und Gesellschaft erarbeitet und getragen wird. Das ist denn auch das Schweizer Modell, das tragfähig ist und Vertrauen schenkt. Dieses ist schliesslich unabdingbare Basis gerade im Teilen und Nutzen unserer Daten.

3 Einordnung des Berichts

Im Rahmen ihres Schwerpunktthemas Künstliche Intelligenz arbeitet die Schweizerische Akademie der Technischen Wissenschaften SATW seit 2017 daran, den Zugang zu qualitativ hochstehenden Daten zu verbessern. Zusammen mit der *Swiss Data Alliance SDA* organisierte die SATW zahlreiche Workshops mit Fachpersonen zu den Themen Data Sharing und Schweizer Datenräume. Seit 2019 bearbeitet die SATW und die *SDA* mit der *Direktion für Völkerrecht des Eidgenössischen Departements für auswärtige Angelegenheiten EDA* und dem *Bundesamt für Kommunikation BAKOM* das Thema digitale Selbstbestimmung. Gemeinsam lancierten die vier Organisationen das *Netzwerk digitale Selbstbestimmung* (vgl. Kap. 3.1) und führten das Konzept der digitalen Selbstbestimmung in einem Diskussionspapier ein. In einem Bericht zuhanden des Bundesrats zeigten das *BAKOM* und das *EDA* im März 2022 Rahmenbedingungen zur Schaffung vertrauenswürdiger Datenräume auf. Parallel dazu führte die SATW in Zusammenarbeit mit der *SDA* mehrere Roundtables in unterschiedlichen Sektoren durch, um Handlungsbedarfe in konkreten Anwendungsbereichen zu identifizieren.

Der vorliegende Bericht schliesst an die laufenden Anstrengungen mit sektorspezifischen Betrachtungen und einem Fokus auf personenbezogene Daten an. Er basiert auf den Erkenntnissen der erwähnten Roundtables, die durch weitere übergreifende Themen ergänzt werden. Die Publikation ist ein gemeinsames Produkt der SATW, der *SDA* und der *Berner Fachhochschule BFH* unter Mitwirkung zahlreicher Fachpersonen aus unterschiedlichen Bereichen (vgl. Kap. 10).

3.1 Netzwerk digitale Selbstbestimmung

Das *Netzwerk digitale Selbstbestimmung* wurde am 11. Mai 2021 offiziell lanciert[3] und dient der Umsetzung der digitalen Selbstbestimmung in der Schweiz. Deren Grundsätze sind in der bundesrätlichen Strategie Digitale Schweiz sowie der Digitalaussenpolitik festgelegt.

Das Netzwerk fördert den Austausch zu vertrauenswürdigen Datenräumen und digitaler Selbstbestimmung, vernetzt alle Interessierte und dient als Konsultationsforum für öffentliche Entscheidungsträger:innen. Es trägt dazu bei, dass die Gesellschaft das Potenzial der Datenwirtschaft auf Basis unserer demokratischen Werte optimal nutzen kann, indem es die Initiierung und Umsetzung vertrauenswürdiger Datenräume unterstützt.

Das Netzwerk besteht aus Akteur:innen aller Interessengruppen in der Schweiz. Es ist frei zugänglich für alle Interessierte, die die Idee der digitalen Selbstbestimmung teilen und unterstützen möchten. Alle Akteur:innen sollen zusammenarbeiten und zu sicheren und vertrauenswürdigen Datenräumen beitragen, um den entstehenden Mehrwert zum Nutzen aller einzusetzen.

Bericht zur «Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung»

Am 30. März 2022 beschloss der Bundesrat basierend auf dem vom *EDA* und dem *UVEK* erarbeiteten Bericht «Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung» verschiedene Massnahmen, um in der Schweiz und im Ausland solche

[3] https://jahresbericht.satw.ch/de/ereignisse

Datenräume und die digitale Selbstbestimmung zu fördern[4]. Der Bericht legt dar, weshalb das Potenzial der Datennutzung aktuell in der Schweiz nicht voll ausgeschöpft wird. Grosse Akteur:innen konzentrieren Daten heute zunehmend, um sie für eigene Zwecke zu nutzen. Kleineren privaten und öffentlichen Dienstleistungsanbieter:innen fehlen dafür das notwendige Know-how oder die entsprechenden Ressourcen. Ein wachsender Anteil der Bevölkerung befürchtet zudem Missbrauch der eigenen Daten und Verlust der Privatsphäre. Entsprechend fehlt der Anreiz, die Daten für eine weitere Nutzung zur Verfügung zu stellen.

Gemäss Bericht braucht es neue Datennutzungskonzepte, welche die Kontrolle über die eigenen Daten verbessern und dadurch die digitale Selbstbestimmung stärken. Vertrauenswürdige Datenräume sollen auf gemeinsamen Prinzipien basieren und den Datenzugang für Einzelpersonen, Unternehmen und weitere Entitäten verbessern.

Bis Juni 2023 erarbeitet das *EDA* und das *UVEK* unter Einbezug aller relevanten Akteure einen freiwilligen Verhaltenskodex für den Betrieb von vertrauenswürdigen Datenräumen. Der Bundesrat will die Interoperabilität zwischen Datenräumen stärken und klärt ab, ob die Schweiz eine nationale Anlaufstelle für Datenräume benötigt. Auf internationaler Ebene wird die Schweiz die Vision von vertrauenswürdigen Datenräumen fördern und sich – analog zum Verhaltenskodex auf nationaler Ebene – an der Erarbeitung internationaler Richtlinien beteiligen.

Sektorspezifische Roundtables

Die SATW führte in Zusammenarbeit mit der *SDA* und weiteren Organisationen zwischen März 2021 und Juli 2022 drei sektorspezifische Roundtables zu Mobilität, Gesundheit und Bildung durch. Ziel dieser Roundtables war, wichtige Aspekte aus den jeweiligen Bereichen zu identifizieren, die für eine bessere Nutzung von Personendaten und den Aufbau von Datenräumen in den jeweiligen Sektoren zu berücksichtigen sind. Dabei wurden jeweils die Ausgangslage analysiert, ein Wunschbild formuliert und laufende Initiativen sowie zu wenig beachtete Bereiche zusammengetragen. Schliesslich wurden Empfehlungen formuliert, um Personendaten besser zu nutzen und den Aufbau sektorspezifischer Datenräume in der Schweiz zu fördern.

Die Resultate aus diesen Roundtables wurden im Rahmen von Arbeitsgruppen – bestehend aus zahlreichen Fachpersonen (vgl. Kap. 10) – weiter konkretisiert. Die ausformulierten Erkenntnisse dieser drei Gruppen finden sich in den Kapiteln 6 bis 8. Sie bilden den Kern dieses Berichts.

[4] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-87780.html

3.2 Vertrauenswürdige Datenräume

Was sind Daten?

Daten sind Aufzeichnungen von Beobachtungen, Messungen oder anderweitigen Angaben. Sie beschreiben Objekte und Sachverhalte in einem bestimmten Kontext. Digitalisiert als Zahlen können Daten von Rechnern verarbeitet, mittels Übertragungsnetzen verteilt und in Speichern aufbewahrt werden[5]. Daten können anhand unterschiedlicher Merkmale klassifiziert werden (vgl. Abbildung 1[6]).

Daten können grossen wirtschaftlichen und gesellschaftlichen Wert haben. Geschäftsmodelle grosser Technologie-Plattformen basieren auf der Sammlung und Wiederverwendung von Daten. Die Forschung braucht Daten, um wissenschaftliche Erkenntnisse und Forschungsresultate zu generieren.

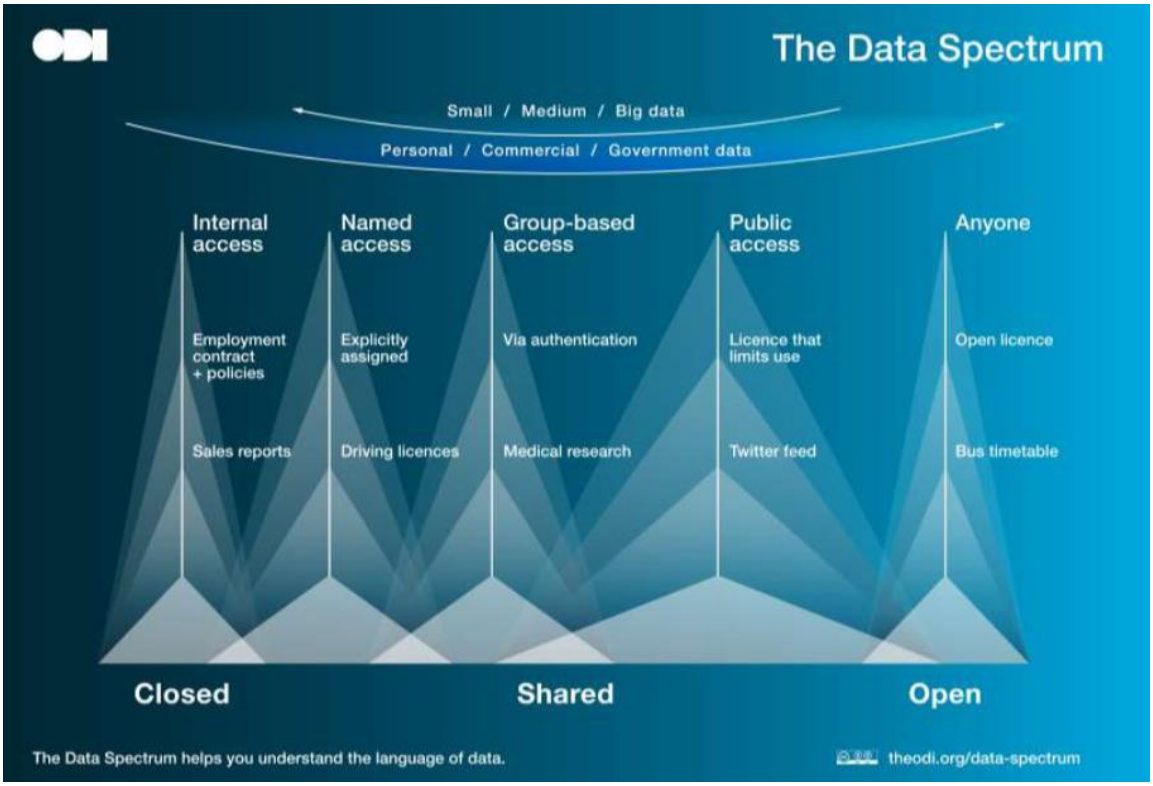


Abbildung 1: Das Datenspektrum.

Nutzung von Personendaten

Personendaten unterliegen rechtlich einem besonderen Schutz. Das Datenschutzgesetz definiert Personendaten als «alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen». Besonders schützenswerte Personendaten sind die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe sowie administrative oder

[5] André Golliez, Juni 2022
[6] https://theodi.org/about-the-odi/the-data-spectrum/

strafrechtliche Verfolgungen und Sanktionen. Mit dem neuen Datenschutzrecht[7], das am 1. September 2023 in Kraft tritt, sollen Personendaten noch besser geschützt werden als bisher. Insbesondere sollen der Datenschutz den technologischen Entwicklungen angepasst, die Selbstbestimmung über die persönlichen Daten gestärkt sowie die Transparenz bei der Beschaffung von Personendaten erhöht werden.

Für Forschung, Planung und Statistik dürfen Personendaten bearbeitet werden, doch müssen sie so rasch wie möglich anonymisiert bzw. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind. Anonymisierte Daten gelten nicht mehr als Personendaten.

Schutz von Personendaten

Personendaten lassen sich durch verschiedene Massnahmen schützen:

1. Pseudonymisierung: Bei pseudonymisierten Daten kann eine bestimmte Person nur noch mithilfe eines eindeutigen Schlüssels identifiziert werden.
2. Anonymisierung: Bei anonymisierten Daten werden primäre Identifikatoren (z. B. der Name) und sekundäre Identifikatoren (z. B. eine AHV-Nummer) aus dem Datensatz entfernt. Dieser Prozess kann im Unterschied zur Pseudonymisierung nicht mehr rückgängig gemacht werden. Ein anderer Ansatz besteht darin, sensible Daten aus einem Datensatz zu entfernen (z. B. Lohn). So bleibt die Privatsphäre einer Person auch dann gewahrt, wenn sie eindeutig identifizierbar ist (differenzielle Privatsphäre).
3. Remote Access: Die Nutzung der Daten geschieht auf eine Weise, die den Zugriff auf die Daten selbst nicht zulässt.

Was ist ein Datenraum?[8]

Ein Datenraum[9,10,11] schafft einen übergeordneten Rahmen, der die gemeinsame Nutzung von Daten durch eine Vielzahl an Akteur:innen ermöglicht. Grundlage dafür ist gegenseitiges Vertrauen und ein verbindliches Regelwerk basierend auf grundlegenden Prinzipien und gemeinsamen Werten. Dabei handelt es sich um rechtliche, organisatorische wie auch technische Vorgaben. Datenräume beziehen sich typischerweise auf einen Anwendungsbereich – z. B. Mobilität, Gesundheit oder Bildung, innerhalb dessen einheitliche Regeln und Richtlinien definierbar sind (vgl. Abbildung 2).

Datenräume sind keine physischen Konstrukte und haben daher keine lokale Begrenzung. Dennoch sind sie über die daran angeschlossenen Dateninfrastrukturen[12] sowie die Regelung des Zugangs geografisch verankert. Die Daten eines Datenraums sind nicht zentral in einer einzelnen Datenbank gespeichert, sondern werden dezentral verwaltet. Weil die Daten von unterschiedlichen Akteur:innen für beliebig viele Dienstleistungen und Anwendungen verwendet werden können, spricht man auch von föderierten Datenökosystemen.

[7] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-90134.html
[8] Angelehnt an André Golliez, *Swiss Data Alliance*
[9] Siehe auch Position-paper-design-principles-for-data-spaces, https://design-principles-for-data-spaces.org/.
[10] Design Principles for Data Spaces
[11] Step 1. Gather Knowledge
[12] Technische Komponenten für Datenpublikation, Datenaufbereitung und Datennutzung.

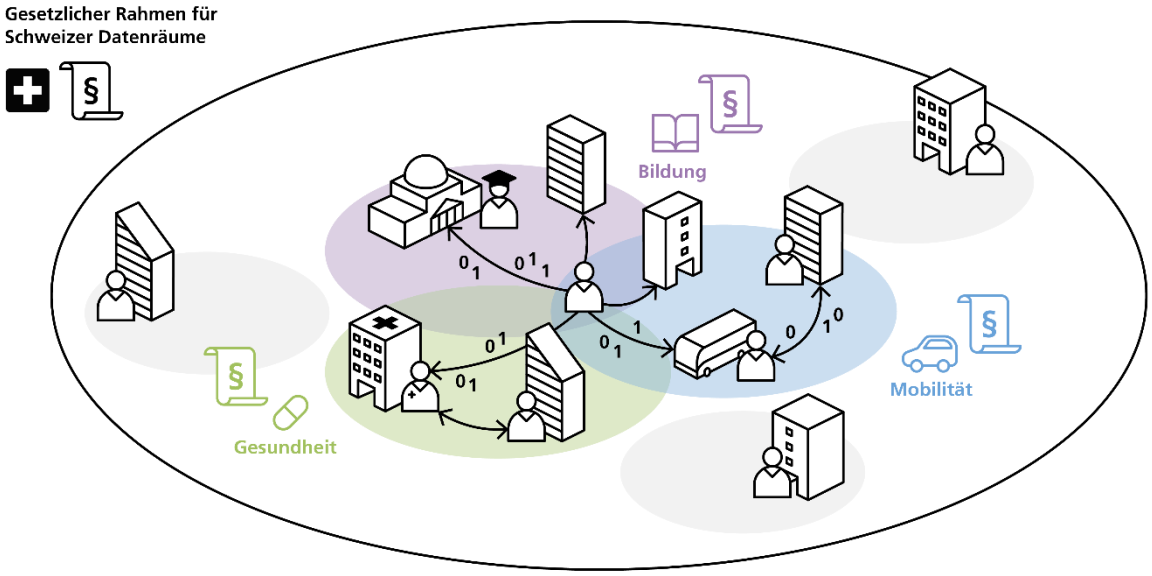


Abbildung 2: In der Schweiz sind Datenräume in unterschiedlichen Anwendungsbereichen am Entstehen. Neben sektoriellen Vorschriften und Normen, braucht es auch einen gesetzlichen Rahmen, der übergeordnete Herausforderungen adressiert und die Nutzung von Personendaten regelt.

Im Rahmen von Datenräumen agieren unterschiedliche Akteur:innen wie Privatpersonen, Unternehmen, öffentliche Verwaltungen oder Forschungsinstitutionen. Diese können – z. T. auch gleichzeitig – verschiedene Rollen wahrnehmen (vgl. Abbildung 3):

- **Datensubjekte** sind natürliche oder juristische Personen, auf die sich bestimmte Daten beziehen wie z. B. Angaben zu Privatpersonen oder Unternehmen.
- **Datenproduzent:innen** erheben Daten und können deren Qualität und Zugänglichkeit steuern.
- **Betreiber:innen von Dateninfrastrukturen** ermöglichen die Datenvermittlung durch technische, organisatorische und rechtliche Massnahmen. Sie stellen dafür z. B. Datenaustausch-Plattformen und weitere Dienste zur Verfügung, welche die Datennutzung erleichtern.
- **Datennutzende** können auf Daten eines Datenraumes zugreifen und diese für datenbasierte Dienstleistungen verwenden.
- **Konsument:innen von datenbasierten Dienstleistungen** sind die Endnutzer:innen der Datenwertschöpfungskette.

Ein Datenraum kann nur dann als föderiertes Datenökosystem fungieren, wenn alle Akteur:innen aktiv daran partizipieren und davon profitieren. Werden Daten von Datensubjekten genutzt, sollten letztere an der Wertschöpfung beteiligt sein. Wer Daten erfasst und deren Qualität sicherstellt oder Dateninfrastrukturen bereitstellt, muss dafür entschädigt werden. Akteur:innen, die Daten eines Datenraums nutzen und damit Erträge generieren oder datenbasierte Dienstleistungen in Anspruch nehmen wiederum, müssen andere Akteur:innen des Datenraums in angemessener Form entschädigen. Ungeachtet dessen braucht es Infrastrukturen, die auf eine Anschubfinanzierung angewiesen sind.

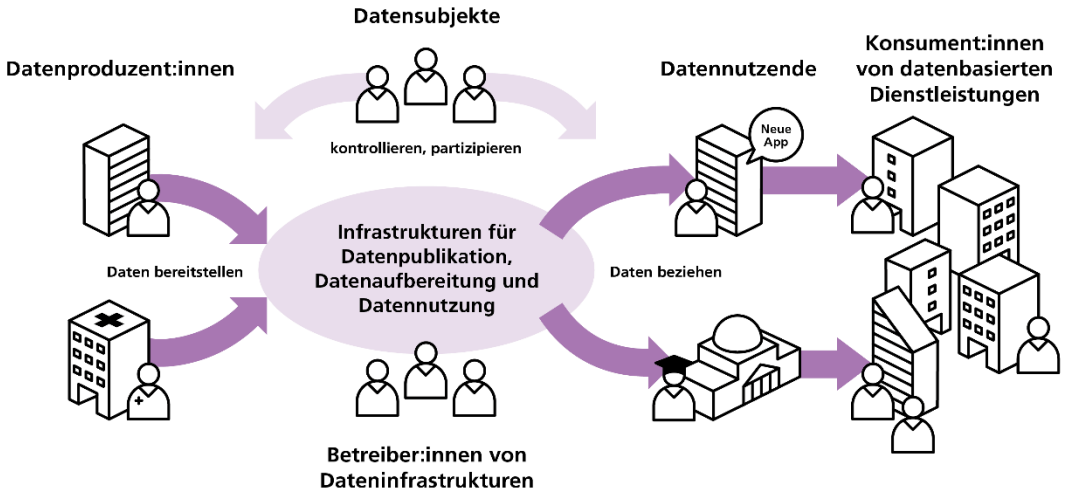


Abbildung 3: Schematische Darstellung der Rollen von unterschiedlichen Akteur:innen in einem Datenraum (nach André Golliez, Zetamind AG).

4 Übergeordnete Rahmenbedingungen und Voraussetzungen

4.1 Datensouveränität

Staaten definieren sich dadurch, dass sie auf einem bezeichneten Territorium die ausschliessliche Hoheitsgewalt und damit Souveränität ausüben[13]. Die digitale Entwicklung wurde in der Vergangenheit weitgehend ohne staatliche Beteiligung und Regulierung primär von privaten Anbieter:innen vorangetrieben. Die Digitalwirtschaft hat rasch übermächtige internationale Grosskonzerne entstehen lassen, die auch in Ländern, in denen sie nicht direkt ansässig sind, wesentlich auf den Alltag einwirken.

Heute besteht ein nicht unerhebliches Risiko für Herstellerabhängigkeiten, sogenannte Vendor Lock-ins. Diese stehen im Gegensatz zur Vision einer digitalen Souveränität, in der nicht nur Individuen, sondern auch Politik und Unternehmen frei über die Ausgestaltung ihrer digitalen Transformation entscheiden können[14,15]. Damit stellt sich die Frage, wie sich die Datenpolitik eines Staats mit Blick darauf positionieren wird und wie Staaten ihre Handlungskompetenz behalten[16].

Der Begriff «digitale Souveränität» hat in der öffentlichen Diskussion der vergangenen Jahre viele Konnotationen erhalten. In Bezug auf Daten kann man von Datensouveränität sprechen. «Datensouveränität formuliert, was im Zusammenhang mit Daten zu tun ist, um den Staat

---

13 «Souveränität und Territorialität sind … eng verknüpft.», Inputpapier zur digitalen Souveränität für die Teilnehmenden des hier angekündigten Beiratstreffen vom 1. November 2022 mit den hier genannten Teilnehmenden.

14 Gees, T., Hürlimann, D., Riedl, R., Stürmer, M. & Wäspi, F. (2022). Digitaler Service Public. Studie im Auftrag des *BAKOM*.

15 Kagermann, H., Streibich, K.-H. & Suder, K. (2021). European Public Sphere. Gestaltung der digitalen Souveränität Europas (acatech IMPULS).

16 Lex Laux: Der wohlmeinende Milliardär, https://www.inside-it.ch/post/lex-laux-der-wohlmeinende-milliardaer-20191029.

souverän sein bzw. werden zu lassen. Datensouveränität ist ein Teilaspekt der digitalen Souveränität und somit von dieser abzugrenzen. Datensouveränität meint die Verengung des Blicks auf Daten, wenn man die Souveränitätsdiskussion führt»[17], hält das Positionspapier Datensouveränität der *SDA* fest.

Die Debatte um Datensouveränität muss die Aufgabe der internationalen Kompetenzabgrenzung lösen. Ein intensiv diskutiertes Beispiel ist Strafverfolgung. Welcher Staat soll das Strafrechtsmonopol haben, wenn die Wirkungen der Tat in einem Staat eintreten (z. B. in den USA), die zur Untersuchung erforderlichen Daten aber auf dem Territorium eines anderen Staats (z. B. in der Schweiz) gespeichert sind? Die Frage ist von verfassungsrechtlicher Bedeutung: Nicht nur das Bestrafen, sondern auch das Untersuchen von Straftaten ist Aufgabe des Staats. Der Staat, auf dessen Gebiet Daten angelegt sind (ausliefernder Staat, hier: die Schweiz), sollte eine Form von Garantieverantwortung für seine Bevölkerung wahrnehmen. Garantieverantwortung heisst z. B., das Strafrechtsmonopol des Staats mit Verfahrensrechten gegen Übermass zu kontrollieren. Was geschieht nun, wenn die USA auf Basis des US-amerikanischen CLOUD Act auf Daten in der Schweiz zugreifen können?[18]

Datensouveränität heisst einerseits, die Gestaltungsfreiheit eines Staats im Rahmen seiner internationalen Zuständigkeiten zu erhalten, um z. B. Datenschutz oder Datennutzungen privater und staatlicher Akteur:innen innerhalb der eigenen Verfassungsordnung zu gestalten. Andererseits auch, um sich gegen Eingriffe anderer Akteur:innen abzugrenzen (Abwehrfähigkeit). Datensouveränität bedeutet somit Garantieverantwortung des Staats für die drei Ziele Kompetenzwahrung, Gestaltungsfreiheit und Abwehrfähigkeit. Garantieverantwortung ist Gestaltungs- und Handlungspflicht. Sie ist verfassungsrechtliche Pflicht nach innen ebenso wie Chance der schweizerischen Diplomatie nach aussen.

4.2 Die europäische Datenwirtschaft[19]

Die *EU* plant mit einer Reihe an regulatorischen Massnahmen, den europäischen Raum zu einer gemeinsamen Datenwirtschaft zu entwickeln. Diese soll das BIP der Region bis 2025 um 528 Milliarden Euro steigern, 5,2 Millionen neue hoch qualifizierte Arbeitsplätze schaffen und die Stellung Europas als eigenständiger Akteur in der globalen Datenwirtschaft entscheidend stärken. Eine Schlüsselkomponente dafür sind Datenräume.

Mit dem *Data Governance Act*[20] hat die *Europäische Union (EU)* ihren Willen bekräftigt, «so viele Daten wie möglich für die gemeinsame Nutzung verfügbar zu machen», auch Personendaten. Sie legte damit die rechtliche Grundlage für Datenaustausch, der im Kontext offener, interoperabler Datenräume geschehen wird, die zu mehr Transparenz und etablierten Standards in der Anonymisierung von Personendaten beitragen sollen. Dateninhaber:innen und Einzelpersonen

---

[17] Positionspapier Datensouveränität der Swiss Data Alliance, https://www.swissdataalliance.ch/publikationen-content/begriffspapier-datensouveraenitaet.

[18] Ein Rechtsgutachten der Kanzlei Laux Lawyers AG hat gezeigt, dass der US CLOUD Act https://www.lauxlawyers.ch/oiz-cloud-gutachten/ keine Rechtswidrigkeit der Cloud-Nutzung begründet, dass aber die Eidgenossenschaft Massnahmen treffen sollte, um ihre Bevölkerung im Sinne der Garantieverantwortung zu schützen.

[19] https://www.swissdataalliance.ch/s/Der-europ-Datenraum-aus-Schweizer-Sicht_-Version-11_Feb-22.pdf, zuletzt abgerufen 23.01.2023

[20] *Europäische Kommission*. (2022a). Verordnung (EU) 2022/868 des *Europäischen Parlaments* und des *Rates*.

sollen Zugriff auf die nötigen Mechanismen haben, um selbstbestimmt die Kontrolle über die sie betreffenden Daten auszuüben.

Mit dem *Data Act*[21] definierte die *EU* die Nutzungs- und Zugriffsrechte. Insbesondere sollen Personen Zugang zu allen Daten haben, die über sie gewonnen werden. Der *Digital Markets Act* sowie der *Digital Services Act* enthalten spezifische Auflagen für Plattformanbieter mit besonderer Marktmacht.

4.3 Gaia-X und internationale Data Hubs

Gaia-X ist ein industriepolitischer Vorstoss und liefert ein Rahmenwerk, das eine dezentrale Dateninfrastruktur in Europa fördern soll[22]. Die einheitliche Architektur ermöglicht es neuen und bestehenden Cloud-Anbietern, einen eigenen Knoten in diesem Netzwerk aufzubauen[23,24]. Zentrale Merkmale von *Gaia-X* sind Datensouveränität, offene Technologien und Interoperabilität. Ein wichtiger Bestandteil von *Gaia-X* sind nationale Datenhubs, die als Anlaufstelle im jeweiligen Land fungieren. Gemäss einer Umfrage[25] sind die Akteur:innen der Schweizer ICT- und Online-Branche gegen die Schaffung eines Schweizer Hub von *Gaia-X*. Sie bevorzugen einen koordinierten Selbstregulierungsansatz, der Massnahmen ermöglicht, ohne die Innovation einzuschränken. Der Bund hingegen empfiehlt die Schaffung eines Swiss Data Hub, um die Verbindung zu *Gaia-X* und anderen Datenraumprojekten sicherzustellen[26].

Mit elf Leuchtturmprojekten befindet sich *Gaia-X* seit Anfang 2022 nach eigenen Angaben in der Umsetzungsphase[27]. Die Projekte können als Kampfansage an die aussereuropäische Konkurrenz betrachtet werden. So entwickelt das Projekt *OpenGPTX* beispielsweise *Gaia-X*-kompatible und offen zugängliche KI-Sprachmodelle, wie sie bisher fast ausschliesslich von US-amerikanischen und chinesischen Unternehmen hergestellt werden. Ein weiteres Förderprojekt, *POSSIBLE*, nutzt eine Open-Source-Alternative zu proprietären Cloud-Lösungen, um Einzelpersonen Zugriff auf die über sie gewonnen Daten zu ermöglichen. Unter den geförderten Projekten finden sich auch Vorhaben aus der Industrie, namentlich der Autobranche, der Luft- und Raumfahrt sowie der Bauwirtschaft.

4.4 Die digitale Identität als Katalysator für vertrauenswürdige Datenökosysteme

Traditionell steht bei Identitätsbeweisen das Vertrauen in die Herausgeber:innen im Vordergrund. Es wird durch Sicherheitsmerkmale in physischen Ausweisen gewährleistet. Das Konzept

---

[21] *Europäische Kommission*. (2022b). Datengesetz: Kommission schlägt Maßnahmen für eine faire und innovative Datenwirtschaft vor. https://ec.europa.eu/commission/presscorner/detail/de/ip_22_1113, abgerufen am 27.9.22.
[22] Reiberg, A., Niebel, C. & Kraemer, P. (2022). Was ist ein Datenraum? Definition des Konzeptes Datenraum. Gaia-X Hub Germany, White Paper.
[23] Gaia-X. (2022c). Join the new Federated Data Infrastructure Ecosystem. Gaia-X Factsheet. https://gaia-x.eu/wp-content/uploads/files/2021-10/Gaia-X%20Factsheet.pdf, abgerufen am 2.11.22.
[24] Gaia-X. (2022b). Members Directory. https://gaia-x.eu/membership/members-directory, abgerufen am 26.9.22.
[25] Swico. (2022). Gaia-X. https://www.swico.ch/de/wissen/politik-positionen/gaia-x, abgerufen am 21.9.22.
[26] *UVEK* und *EDA*. (2022). Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung. Bericht des *UVEK* und des *EDA* an den Bundesrat.
[27] Gaia-X. (2022a). Mit Gaia-X zur digitalen Souveränität. Leuchtturmprojekte aus dem Förderwettbewerb.

funktioniert, weil die prüfende Partei (z. B. der Zoll oder Händler:innen) der herausgebenden Partei (z. B. die Gemeinde für die ID oder die Bank für Bankkarten) vertraut.

Die digitale Welt kennt nur die Identitäten von Systemen, sogenannte IP-Adressen. Identitäten von Nutzer:innen wurden im Konzept des Internetprotokolls nie integriert. Deshalb haben sich pro Anwendung oder Service eigene Identitäten und Log-ins entwickelt. Jeder Service vergibt eigene Passwörter und prüft die Identität anders bzw. neu. Daraus haben sich Silos entwickelt.

Aufgrund des fehlenden digitalen Identitätsnachweises und dem so entstandenen Passwort-Chaos haben sich Intermediäre, sogenannte Identity Providers (IDP) gebildet. Oft sind es mächtige Internetfirmen, die diesen Service anbieten. Das Problem: Die Identitätsdaten liegen bei den IDP. Diese können alle Aktionen der Benutzer:innen nachvollziehen, den Zugang verweigern oder Benutzer:innen ausschliessen und die Informationen zu eigenen Zwecken nutzen (z. B. personalisierter Werbung).

Die Schweizer Stimmbevölkerung lehnte die Vorlage zur Einführung einer digitalen Identität im Jahr 2021 ab. Ausschlaggebend dafür war u. a. das mangelnde Vertrauen der Schweizer Bevölkerung in die privaten Unternehmen, die als Identitätsanbieter hätten agieren sollen. Aktuell ist ein Gesetz für eine neue staatliche E-ID in der Vernehmlassung.

Die selbstbestimmte, digitale Identität (Self-Sovereign Identity, SSI[28]) bringt die Kontrolle über die Identitäts- und Datennutzung im digitalen Raum zu den Benutzer:innen. Sie können selbst sogenannte Decentralized Identifier (DID) generieren. Eine DID ist eine Adresse, die als Anker für verschiedenste (Identitäts-)Attribute dient. Ein Aussteller kann Attribute an diesen Anker anbinden und Verifikatoren können deren Authentizität ohne direkte Verbindung zum Aussteller überprüfen. Ein ID-Attribut in einem SSI-Ökosystem funktioniert somit ähnlich wie die physische Identität: Die Identitätsdaten bleiben in einer kryptografisch geschützten Wallet (analog zur ID im Portemonnaie). Entsprechende Daten können – analog einer Beglaubigung – durch eine herausgebende Partei kryptografisch verifiziert werden. Die prüfende Partei vertraut der herausgebenden Partei und der im Ökosystem digital verankerten Gouvernanz. Distributed Ledger Technology (DLT) kann als Speicher oder Register für die Beglaubigungen genutzt werden, muss aber nicht.

Mit SSI ergeben sich u. a. folgende Chancen:

- Privacy by Design bzw. Privacy by Default an der Quelle personenbezogener Daten
- Identität und Vertrauen in Datenräumen für vertrauenswürdige und friktionslose Dienste
- Attribut-basierter Zugriff zu Datenräumen
- Verankerung semantischer Systeme von Katalogen mit verifizierbaren Attributen und damit Sicherstellung der Provenienz der Beschreibungen, Attestierungen und der Daten selbst
- Dezentrale Datenspeicherung unter nachhaltig souveräner Kontrolle durch Benutzer:innen und Teilen der Datenpakete mit vertrauenswürdigen Parteien

[28] Die wichtigsten Aspekte von SSI in Kontext mit Datenräumen können z. B., im folgenden Gaia-X Whitepaper detaillierter nachvollzogen werden: https://www.gxfs.eu/ssi-whitepaper/

Selbstbestimmte digitale Identitäten und verifizierbare Attribute helfen dabei, Vertrauen im digitalen Raum und somit auch in Datenräumen zu etablieren. Im Zentrum dieser Modelle steht die digitale Mündigkeit der Benutzer:innen. Das birgt auch Risiken. Es ist wichtig, nachhaltig prinzipienbasiert und innerhalb eines wirkungsvollen, jedoch anpassungsfähigen Rechtsrahmens vorzugehen und alle Stakeholder:innen miteinzubeziehen.

5 Nutzung personenbezogener Daten in der Mobilität

5.1 Ausgangslage und Wunschbild

Bewegungsfreiheit ist ein Menschenrecht und Mobilität ein Grundbedürfnis. Reisen ermöglichen Begegnungen und erweitern den Horizont. Sie können auch unabdingbar sein, z. B. aufgrund eines Anstellungsverhältnisses. Zunehmende Mobilität durch die stetig wachsende Weltbevölkerung bringt aber negative Begleiterscheinungen mit sich. Die Mobilitätsinfrastruktur muss ständig ausgebaut, verdichtet und unterhalten werden, was hohe Kosten verursacht und den Lebensraum von Tieren und Pflanzen verknappt. Das Betreiben privater motorisierter Transportmittel und des öffentlichen Verkehrs benötigt viel Energie und führt zu für Mensch und Umwelt schädlichen Emissionen. Es ist daher angezeigt, das Gesamtmobilitätssystem möglichst effizient zu gestalten.

Daten zum persönlichen Mobilitätsverhalten könnten dabei helfen, Menschen zu sensibilisieren, nachhaltiger unterwegs zu sein. Hätten Mobilitätsanbieter besseren Zugriff auf Daten zu vergangenen, aktuellen und geplanten Reisen, könnten sie ihre Angebote optimieren, effizienter weiterentwickeln oder gar individualisieren. Der Bund könnte Verkehrsinfrastrukturen effektiver planen und das Gesamtmobilitätssystems besser orchestrieren.

Personenbezogene Mobilitätsdaten sind sensibel und schützenswert. Sie können nicht nur preisgeben, wo wir uns aufhalten, sondern auch, in welchen Kreisen wir verkehren, welche Vorlieben wir haben oder was unser aktueller Gesundheitszustand ist. Nutzer:innen sollten die Kontrolle über ihre Bewegungsdaten haben. Dafür bedarf es rechtlicher Rahmenbedingungen. Für gut informierte und selbstbestimmte Entscheidungen brauchen wir eine möglichst vollständige und aktuelle Übersicht über alle zugänglichen Alternativen. Eine solche technische Hilfe kann das benötigte Umdenken unterstützen, das z. B. Peak-Zeiten und Staus zu vermindern hilft.

Wenn Nutzer:innen persönliche Mobilitätsdaten über den ursprünglichen Erhebungszweck mit anderen Parteien teilen, sollten sie einen Nutzen davon haben. Das können direkte Vergütungen, Zusatzdienstleistungen oder bessere, individualisierte Angebote sein – oder einfach das gute Gefühl, zu einer nachhaltigeren Mobilität beizutragen. Anreize dürfen aber keinesfalls zu einem indirekten Zwang führen oder dazu, dass Dienste unbegründet verweigert werden.

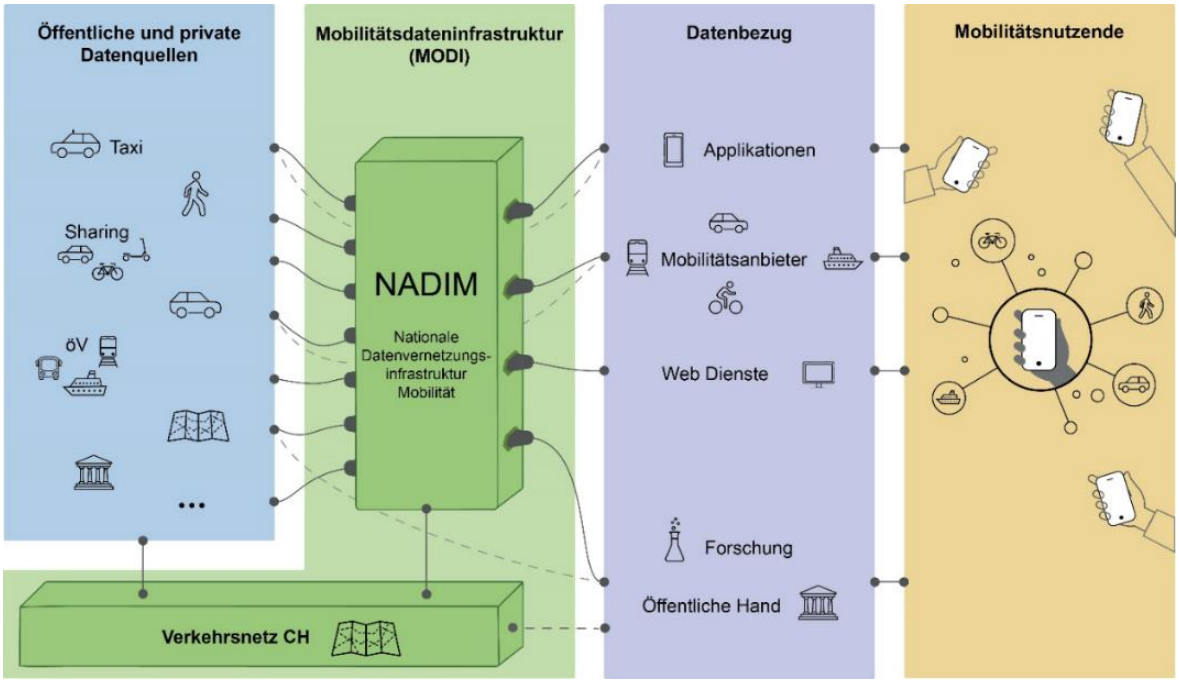
Wunschbild Mobilitätsdatenraum

Bürger:innen können sich mittels eines persönlichen Portals eine Übersicht über sämtliche für sie relevante, digital verfügbare Mobilitätsdaten verschaffen. Dort sehen sie, wer welche Daten über sie erfasst hat und können bei Bedarf weitere hinterlegen. Von Mobilitätsanbieter.innen erfasste Daten stehen automatisiert austauschbar zur Verfügung. Die Übersicht sensibilisiert Bürger:innen hinsichtlich ihres Mobilitätsverhaltens und motiviert sie, ihre Mobilität möglichst nachhaltig zu gestalten. Sie tragen vermehrt zur Entlastung des Gesamtmobilitätsystems sowie zur Schonung der

Umwelt und der Verkehrsinfrastruktur bei. Die Bürger:innen sind befähigt, ihre Daten über den ursprünglichen Erhebungszweck hinaus zusätzlichen Parteien wie Forschungsunternehmen, Staatsebenen und Dienstleister.innen zur Verfügung zu stellen. Sie kontrollieren, wer in welchem Umfang und zu welchem Zweck welche Daten verwenden darf. Basierend auf den geteilten Daten entwickeln Unternehmen neue innovative und individualisierte On-Demand-Dienstleistungen und Angebote. Bürger:innen können diese und weitere Mobilitätsangebote über einen persönlichen Zugang buchen und bezahlen.

5.2 Laufende Initiativen

Treibende Entwicklungen in der Mobilität sind die Automatisierung des Fahrens, die Mobilitätssteuerung sowie die Vernetzung der Mobilitätsangebote (intermodale Mobilität). Um die dafür benötigten Informationen harmonisiert verfügbar zu machen, will der Bundesrat eine staatliche Mobilitätsdateninfrastruktur (MODI) aufbauen. Das Bundesgesetz über die Mobilitätsdateninfrastruktur (MODIG)[29] soll dafür optimale Grundlagen schaffen. Der Entwurf des *UVEK* unter Federführung des *Bundesamts für Verkehr (BAV)* ist aktuell in der Vernehmlassung. Die MODI besteht in der ersten Ausbaustufe aus zwei Hauptelementen: Das Verkehrsnetz CH und die Nationale Datenvernetzungsinfrastruktur (NADIM).



Das Verkehrsnetz CH bildet geographische Karten digital ab und stellt verkehrsträgerübergreifend eine routingfähige geografische Datenbasis zur Verfügung. Die NADIM verbindet Mobilitätsanbieter:innen mit Vermittler:innen von Mobilitätsangeboten.

Für die Ausgestaltung der Funktionen, der Datenflüsse und -speicherung auf der NADIM ist die digitale Selbstbestimmung ein zentraler Aspekt. Die relevanten Use Cases aus Sicht der Nutzer:innen der Mobilität müssen daher bei der Entwicklung der NADIM zwingend beachtet werden.

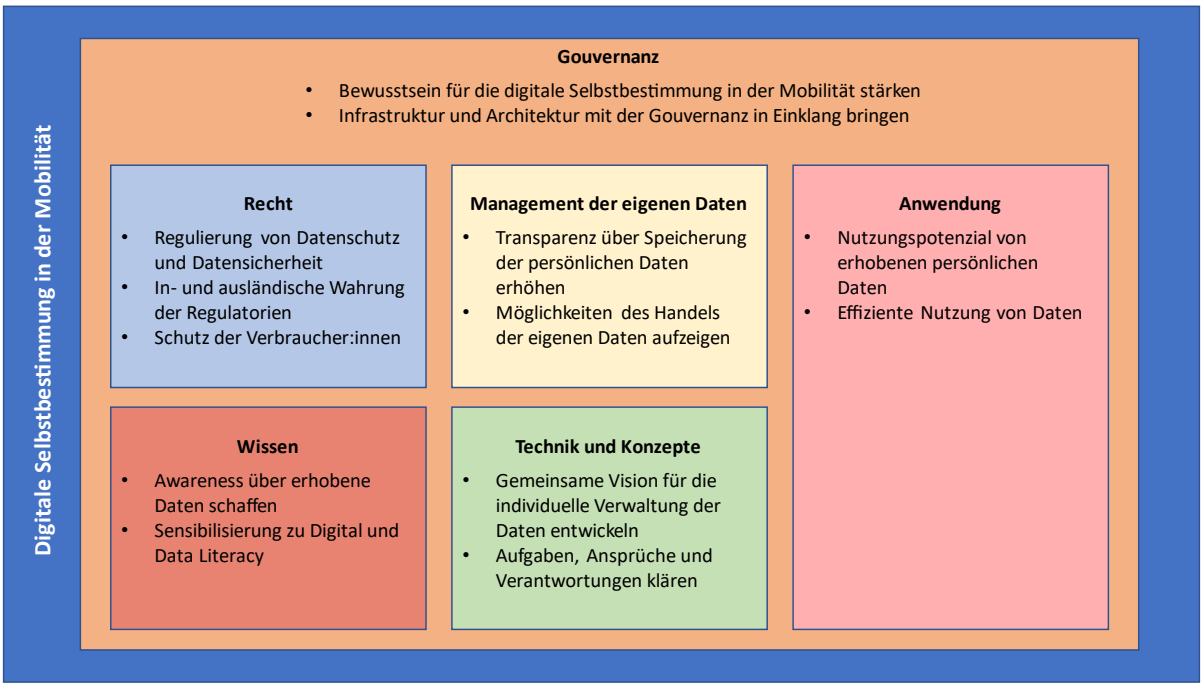
[29] https://www.bav.admin.ch/bav/de/home/allgemeine-themen/mmm.html

Im Forschungsprogramm des *Bundesamts für Strassen (ASTRA)* wird ein Vorgehen zur Erstellung von Datengouvernanz-Modellen für Smart-Mobility-Anwendungen entwickelt. Diese regeln die Datengouvernanz auf organisatorischer, rechtlicher und technologischer Ebene. Die strukturierte Methodik erlaubt die Identifikation anfallender Datenflüsse zwischen den involvierten Akteur:innen und eine Zuteilung der Datenflüsse zu generischen Datentypen. Im Weiteren können mit den entwickelten juristischen Instrumenten die Daten zugeordnet werden. Damit lässt sich feststellen, ob Daten anhand des Urheberrechts, über den strafrechtlichen/wettbewerblichen Schutz von Fabrikations- oder Geschäftsgeheimnissen, dem wettbewerbsrechtlichen Schutz von fremden Arbeitsergebnissen, oder für personenbezogene Daten über das Datenschutzgesetz geschützt werden. Die Daten lassen sich dank privatsphäreschützender Technologien dennoch verwenden. Im Projekt wurden diese Instrumente für zwei verschiedene Gouvernanz-Modelle verwendet, eines für Mobility-as-a-Service (MaaS) und eines für Mobility Pricing. Es zeigten sich grosse Unterschiede, ob die Teilnahme von Nutzer:innen auf einer freiwilligen (MaaS) oder verpflichtenden (Mobility Pricing) Basis ist. Bei letzterem muss der gesetzliche Datenschutz für die Verwendung personenbezogener Daten, z. B. für Bewegungsprofile, zusätzlich mittels privatsphäreschützender Technologien[30] garantiert werden (Privacy by Design). Andererseits dürfte wohl das Vertrauen fehlen. Trusted Execution Environments bieten dazu die Möglichkeit, innerhalb dieser geschützten digitalen Räume personenbezogene Daten in irreversibel anonymisierter Form zu platzieren und für Analysen zur Verfügung zu stellen. Innerhalb dieser geschützten Räume ist es nur möglich, Algorithmen mit entsprechender Zertifizierung rechnen zu lassen. Eine Haupterkenntnis des Projekts ist, dass Daten vertrauenswürdiger Institutionen über zertifizierte Prozesse behandelt werden müssen, unabhängig ob freiwillige oder verpflichtende Teilnahme.

[30] Hier kann z. B. das neue E-ID Gesetz einen Beitrag leisten.

5.3 Ungenügend adressierte Bereiche

4Digitale Selbstbestimmung in der Mobilität adressiert Themenfelder wie Recht, Wissen, Management der eigenen Daten, Technik und Konzepte sowie die Umsetzung, in der Regel in IT-Systemen. Übergeordnet muss eine verbindliche Gouvernanz die unterschiedlichen Interessen adressieren. Aktuell fehlt das Verständnis für alle diese Themenfelder, die deshalb weiter untersucht werden müssen. Aktuelle Datengouvernanzen und -Frameworks adressieren das Thema digitale Selbstbestimmung nicht, sind zu wenig transparent und flexibel.



Datenräume in der Mobilität sind erst in Entwicklung. Auch das Verständnis muss entwickelt und der Konsens zu offenen Fragen gefunden werden. Die Schwierigkeit besteht darin, die geeignete Policy zur Weiterentwicklung der hybriden, digitalen und physischen Ausgestaltung der Datenräume in der Mobilität zu definieren. Bisher rein unter dem Gesichtspunkt der digitalen Welt entwickelte Dateninfrastrukturen müssen neu gedacht werden.

Recht: Es müssen Grundlagen für die Regulierung der Datensicherheit sowie des Daten- und Verbraucherschutzes geschaffen werden. Diese müssen mit der Entwicklung im Ausland, insbesondere den Nachbarländern, abgestimmt sein. In einer sich rasch verändernden und zunehmend digitalen Welt muss eine hohe Wandlungs- und Anpassungsfähigkeit in der Gestaltung der Gesetzesgrundlage berücksichtigt werden.

Wissen: Es muss eine Transparenz geschaffen werden, die es ermöglicht, nachvollzuziehen, welche Daten erhoben werden und was mit diesen Daten erreicht wird. Ein Beispiel hierfür ist die Kampagne Data Literacy[31], welche die Probleme der fehlenden Datenkompetenz in vielen Bereichen der Politik adressiert.

Technik und Konzepte: Es besteht noch keine gemeinsame Vorstellung für die individuelle Verwaltung von Daten sowie für damit verbundene Aufgaben, Ansprüche und Verantwortung.

[31] https://www.data-literacy.ch/kampagne

Neben der pauschalen Forderung «Weniger ist mehr» stehen die Fragen von Garantien und Hoheit in der geplanten oder ungeplanten Nutzung sowie notwendigen Integrität im Raum. Werden diese nicht beantwortet, braucht es alternative Möglichkeiten zum Schutz der digitalen Selbstbestimmung. Die Konzepte und Mechanismen dazu sind erst in der Entstehung.

Management der eigenen Daten: Datensubjekte haben wenig Überblick darüber, wo welche persönlichen Daten gespeichert und wie diese weiter genutzt werden. Selbst grundlegende Elemente wie die dauerhafte Kontrolle über abgeschlossene Verträge und die Konsequenzen daraus, z. B. aus den AGB, fehlen heute. Es mangelt an Werkzeugen, Beratungs- oder gar Vermarktungsmöglichkeiten für die eigenen Mobilitätsdaten.

5.4 Empfehlungen

In der Mobilität hat Technologie in den letzten Jahren im Umgang mit Daten vielfältige neue Möglichkeiten geschaffen. Allerdings wird Mobilität heute immer noch in getrennten Silos geplant und betrieben, insbesondere von traditionellen Akteur:innen. Diese finden oft keinen Business Case in der Nutzung der ihnen zugänglichen Daten. Neue Akteur:innen, insbesondere aus anderen Sektoren, nutzen die Möglichkeiten; sie konzentrieren die entscheidende Expertise.

Bei Reisenden ist das Wissen über die technischen und rechtlichen Gegebenheiten sehr schwach ausgeprägt. Es hat sich kaum ein Bewusstsein zur digitalen Selbstbestimmung entwickelt. Dabei ist diese weniger ein technisches Problem als eines des mangelnden gemeinsamen Verständnisses.

Es braucht die richtige Balance zwischen Schutz der Souveränität und flexibler Nutzung. Dazu müssen Nutzer:innen befähigt und eine ausgewogene Regulierung und Gouvernanz definiert werden. Der Gesetzgebungsprozess ist viel langsamer als die Entwicklung der (technischen) Möglichkeiten. Dies soll nicht zu restriktiven Regelungen führen, die sinnvolle Entwicklungen verhindern. Der Aufbau von Vertrauen und überprüfbare Prozesse zwischen den Akteur:innen auf verschiedenen Ebenen ist entscheidend:

- technisch durch passende Entwicklungsmethoden (Security by Design, Trusted Execution Environments) und der Überprüfung der Einhaltung (z. B. durch Zertifizierung)
- Beurteilungsfähigkeit aller Akteur:innen (z. B. amtliche Registrierungspflicht)
- Schaffung von Transparenz über die Flüsse der Daten und ihrer Bearbeitung, insbesondere der Möglichkeiten der Aggregation und der Nutzung der daraus gewonnenen Erkenntnisse
- Entwicklung einer griffigen und ausgewogenen prinzipienbasierten Regulation

Zwei Pfade sind grundsätzlich möglich:

1. Der Ansatz der Datensparsamkeit fokussiert auf den Schutzaspekt, mindert aber die Chancen, die sich durch die Verknüpfung von Daten aus unterschiedlichen Bereichen ergeben.
2. Die souveräne Entscheidung über die Erfassung, Verarbeitung und Löschung der Daten sowie deren Verknüpfungen über einen zentralen Weg für die Kontrolle (z. B. über ein persönliches Portal) und einen dezentralen für die ökonomische Nutzung. Die gemeinsame Verantwortung der Beteiligten für ein abgestimmtes Vorgehen ermöglicht eine Balance in der dualen Befähigung, Ermächtigung und Innovation sowie Forschung zur digitalen Souveränität.

Welcher Pfad verfolgt wird, sollte über ein nationales behördenverbindliches Instrument transparent geprüft, geregelt und die Entscheidungsprozesse kommuniziert werden. Der notwendige Diskurs wäre über die parlamentarischen Instrumente hingegen besser abgestützt.

Dies führt zu folgenden Empfehlungen:

1. Entwicklung einer Awareness-Kampagne für die Bevölkerung zur digitalen Selbstbestimmung in der Mobilität. Der Auftrag dazu soll aus dem *UVEK* in Abstimmung mit dem *EJPD* kommen. Für die Umsetzung müssen verschiedene Kompetenzen u. a. zu Daten, Recht und Mobilität gebündelt werden. Schulen und generell Ausbildungsstätte sollen eine Vermittlerrolle übernehmen. Dies kann schrittweise erfolgen, beginnend mit der Vermittlung von Basiswissen.
2. Staatliche Aktivitäten, insbesondere im Kontext der Entwicklung der Mobilitätsdateninfrastrukturen, berücksichtigen die digitale Selbstbestimmung als zentrales Element. Die Betreiber:innen dieser Dateninfrastrukturen stellen diese nicht nur auf der eigenen Infrastruktur sicher, sondern auch für die daran angeschlossenen Akteur:innen.
3. Die Gesetzgeber:innen sollen die digitale Selbstbestimmung in allen betroffenen Gesetzen verankern. Eine Analyse der bestehenden Gesetze und des Handlungsbedarfs sollte vom *EJPD* beauftragt werden. Es überprüft zudem die Möglichkeit einer Zertifizierung.
4. Die Wirtschaftsverbände der Mobilität und des ICT-Sektors stellen ihren Mitgliedern Best Practices zur Verfügung. Der vom Bundesrat beauftragte Verhaltenskodex wird unterstützt.

6 Digitale Selbstbestimmung im Gesundheitsdatenraum

6.1 Ausgangslage und Wunschbild

Die Sekundärnutzung von Gesundheitsdaten ist für die Schweiz von grosser Bedeutung[32]. Das ist spätestens seit der Covid-Pandemie unter den Akteur:innen der Gesundheitsversorgung und der Forschung breit akzeptiert. Dank einer besseren Sekundärnutzung von Gesundheitsdaten liesse sich das Krankheitsgeschehen in der Bevölkerung und die Nutzung des Gesundheitssystems besser und zeitnah überwachen; digitale Gesundheitsanwendungen könnten mit hoher Qualität entwickelt werden; die Forschung könnte gestützt auf diese Daten neue Erkenntnisse gewinnen und neue Ansätze für Prävention, Diagnostik und Therapie entwickeln.

Gesundheitsdaten sind besonders komplex und sensibel: Gemäss schweizerischem Datenschutzgesetz (DSG) gelten (nicht anonymisierte) Gesundheitsdaten als besonders schützenswerte Personendaten. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten. Anonymisierung wird aber gerade durch die sich entwickelnden Möglichkeiten der Datenaggregation und Analytik zunehmend hinfällig. Re-Identifikationen sind verhältnismässig einfach durchzuführen. Zudem ist die Anonymisierung für gewisse Klassen von Gesundheitsdaten kaum praktikabel (z. B. Genomdaten).

Der Nutzen einer besseren Sekundärnutzung der Daten liegt einerseits in einer besseren Qualität der Versorgung und andererseits in effizienteren Prozessen. Dieser Nutzen ist aber schwierig zu vermitteln, da die Zufriedenheit der Bevölkerung mit der bestehenden Gesundheitsversorgung trotz steigender Krankenversicherungsprämien sehr hoch ist.

Im Zusammenhang mit der digitalen Selbstbestimmung der Bürger:innen stellt das Datenmanagement und die Gouvernanz der Sekundärnutzung von Daten nicht nur aufgrund des hohen Schutzniveaus eine grosse Herausforderung dar:

- Die besondere Sensibilität von Gesundheitsdaten sowie ihre Erzeugung in einem hoch regulierten Umfeld hat dazu geführt, dass Gesundheitsdaten in schwer vernetzbaren Datensilos der Leistungserbringer:innen (Spitäler, Praxen, Apotheken etc.) gehalten werden. Für eine sinnvolle Nutzung ist aber das Aufbrechen dieser Silos eine wesentliche Voraussetzung.
- Noch immer wird ein grosser Teil der Daten nicht digital erfasst und die Datenerfassung ist nicht standardisiert; sie werden uneinheitlich und mit unterschiedlicher Qualität erhoben. Die Interoperabilität ist nicht sichergestellt.
- Die Akteur:innen haben die Sekundärnutzung von Daten bisher kaum diskutiert. Die Vorstellungen über die Gouvernanz und die Finanzierung einer Gesundheitsdateninfrastruktur gehen weit auseinander und die Diskussionen darüber stehen noch am Anfang.
- Die öffentliche Debatte über die Sekundärnutzung der Gesundheitsdaten ist kaum existent. Die Erfahrungen mit dem Generalkonsent für die Nutzung von Gesundheitsdaten zu Forschungszwecken zeigen, dass die Patient:innen eine hohe Bereitschaft zeigen, ihre Daten dafür zur Verfügung zu stellen. Eine neue Befragung zeigt zudem, dass 71 Prozent der

[32] https://lsr.recht.ch/de/artikel/01lsr0322bra/gesundheitsdatenraum-schweiz

(gesunden) Bevölkerung bereit ist, ihre Gesundheitsdaten zu teilen, sich eine Mehrheit aber auch mehr Transparenz und Informationen zu diesem Thema wünscht[33].

Wunschbild Gesundheitsdatenraum

Analog zum Schweizer Eisenbahnnetz entsteht eine nationale Dateninfrastruktur für Gesundheitsdaten (NaDiG), die als kritische nationale Infrastruktur und damit auch als öffentliches Gut gilt[34]. Die NaDiG stösst auf breite Akzeptanz bei der Bevölkerung. Die Nutzung der Dateninfrastruktur ist transparent und fair geregelt und setzt wirksame Anreize für Datennutzer:innen und für die Datenproduzent:innen. Für den Aufbau einer Basisinfrastruktur stehen finanzielle Mittel der öffentlichen Hand zur Verfügung.

6.2 Laufende Initiativen

Zahlreiche Initiativen haben sich in den letzten Jahren der Thematik auf unterschiedlichen Ebenen angenommen. Die untenstehende Auflistung ist unvollständig:

Forschung

Das Swiss Personalized Health Network (SPHN) wird im Rahmen der BFI-Botschaft des Bundes über einen Zeitraum von acht Jahren gefördert (2017–2024). Im Zentrum des SPHN steht der Aufbau eines skalierbaren Netzwerks verschiedener Datenproduzenten, das die Sekundärnutzung der Daten primär für die Forschung erlaubt. Mit SPHN verbunden ist die ETH-Initiative Personalized Health and Related Technologies (PHRT) sowie die Datenaustausch-Infrastruktur (BioMedIT)

Einen menschenzentrierten Ansatz zur Sekundärnutzung von Gesundheitsdaten setzt die *MIDATA-Genossenschaft* um. Die Inhaber:innen eines Gesundheitsdaten-Kontos haben die volle Kontrolle über die Sekundärnutzung der Daten. Die MIDATA-Plattform wird derzeit vor allem im Rahmen von Forschungsprojekten, etwa innerhalb von SPHN und PHRT, von Horizon-Projekten und im Bereich Prävention in der Gesundheitsversorgung eingesetzt.

Ein bundesrätlicher Bericht zur besseren Nutzung von Gesundheitsdaten[35] kam 2022 zum Schluss, dass ein «Nationales System zur Weiterverwendung und Verknüpfung von Gesundheitsdaten» geschaffen werden sollte, damit die Datenakteure über akzeptable und attraktive Rahmenbedingungen für die mehrfache Nutzung von Gesundheitsdaten zu Forschungszwecken verfügen. Das im Bericht skizzierte System soll mithilfe eines rechtlichen Rahmenwerks gesteuert

[33] Pletscher F, Mändli Lerch K, Glinz D. Willingness to share anonymised routinely collected clinical health data in Switzerland: a cross-sectional survey. Swiss Med Wkly. 2022 Jun 16;152:w30182. doi: 10.4414/smw.2022.w30182. PMID: 35752970.

[34] In einer Gesundheitsdateninfrastruktur werden Daten aus unterschiedlichen Quellen und von unterschiedlichen Lieferanten sichtbar gemacht und nach definierten Regeln unter verschiedenen Akteur:innen miteinander geteilt und gemeinsam genutzt. Solche Infrastrukturen bestehen aus drei Elementen: 1. einer Technologie, die eine sichere und transparente Datennutzung nach den Regeln der Infrastruktur ermöglicht, 2. einer Organisation, welche die Datennutzung verwaltet, überwacht und die technische Infrastruktur betreibt, 3. einer Regulierung, welche die Regeln der Datennutzung in der Dateninfrastruktur festlegt.

[35] Bessere Nutzung von Gesundheitsdaten zu Forschungszwecken
Bericht des Bundesrats in Erfüllung des Postulates 15.4225 Humbel (PDF, 4 MB, 04.05.2022)

werden. Eine Nationale Datenkoordinationsstelle würde sicherstellen, dass der Datenaustausch und die damit verbundene Datenbearbeitung rechtskonform und sicher erfolgen.» Ein weiterer Bericht aus dem Jahr 2022 fokussiert zudem auf das Datenmanagement, das im Nachgang zur Covid-Pandemie verbessert werden soll[36].

Gesundheitsversorgung

Mit dem elektronischen Patientendossier (EPD) wird seit Jahren eine Infrastruktur aufgebaut, die es Patient:innen erlaubt, ihre Gesundheitsinformationen zu sammeln und mit Leistungserbringer:innen zu teilen. Die Sekundärnutzung der Gesundheitsdaten für Forschungszwecke oder personalisierte Medizin wird bislang ausgeklammert. Sie wird als Teil der Revision des Gesetzes über das EPD (EPDG)[37] geprüft[38].

Zahlreiche Daten werden in krankheitsbezogenen Registern erfasst und ausgewertet, z. B. den Krebsregistern[39]. Diese werden für die epidemische Forschung sowie zur Versorgungsforschung genutzt. Darüber hinaus verfügen das *Bundesamt für Statistik*[40] und die Leistungserbringer:innen über Datenbanken zur Epidemie, Versorgung und Versorgungsqualität[41].

Derzeit entstehen zwei nationale, digitale Gesundheitsökosysteme (*Compassana*, *Well*)[42], die ebenfalls Daten erfassen und in ihrem Geschäftsmodell nutzen. Eine Initiative der *Handelskammer beider Basel* strebt ausserdem an, in der Nordwestschweiz ein regionales Gesundheitsdatenökosystem für die Forschung und die Gesundheitsversorgung aufzubauen.

Die *Allianz digitale Transformation im Gesundheitswesen* bündelt seit 2021 die Interessen einzelner Akteur:innen[43] und führt auch eine Arbeitsgruppe zu Gesundheitsdatenökosystemen.

Öffentliche Hand

Mit dem Programm *Nationale Datenbewirtschaftung (NaDB)* des *BFS* soll die Datenbewirtschaftung der öffentlichen Hand durch die Mehrfachnutzung von Daten einfacher und effizienter werden. Übergeordnetes Ziel ist, dass Personen und Unternehmen den Behörden bestimmte Angaben nur noch einmal melden müssen (Once-Only-Prinzip). Im Rahmen des *NaDB* werden Gesundheitsdaten gesondert behandelt[44].

---

[36] Verbesserung des Datenmanagements im Gesundheitsbereich
Bericht zur Verbesserung des Datenmanagements im Gesundheitsbereich vom 12.01.2022 (PDF, 1 MB, 12.01.2022)

[37] https://www.bag.admin.ch/bag/de/home/strategie-und-politik/nationale-gesundheitsstrategien/strategie-ehealth-schweiz/umsetzung-vollzug/weiterentwicklung-epd.html

[38] Der Bundesrat will das elektronische Patientendossier weiterentwickeln, Medienmitteilung (27.04.2022)

[39] https://www.nkrs.ch/

[40] https://www.bfs.admin.ch/bfs/de/home/statistiken/gesundheit.html

[41] https://www.fmh.ch/themen/qualitaet-saqm/register/medizinische-register.cfm

[42] https://www.compassana.ch/de, https://www.well.ch/

[43] https://www.ig-ehealth.ch/allianz/

[44] https://www.bfs.admin.ch/bfs/de/home/nadb/nadb.html

Regulierung

Hinsichtlich der regulatorischen Rahmenbedingungen dürften die für 2023 angekündigte Revision des EPDG sowie ein allfälliges Rahmengesetz über die Sekundärnutzung von Daten[45] in der Schweiz wichtige Impulse geben. Ausserdem spricht auch der bundesrätliche Bericht über das bessere Datenmanagement von entsprechenden rechtlichen Anpassungen. Darüber hinaus hat das *Bundesamt für Gesundheit* die Fachgruppe Datenmanagement installiert[46]. Sie setzt einen Schwerpunkt bei der semantischen und der technischen Interoperabilität und kann von den politischen Gremien Massnahmen z. B. zur Rechtsetzung beantragen.

6.3 Ungenügend adressierte Bereiche

Es fällt auf, dass die zahlreichen Initiativen und Ansätze nicht miteinander koordiniert sind. Dadurch besteht die Gefahr, dass Synergien nicht genutzt werden. Letztlich fehlt eine von den Akteur:innen gemeinsam getragene Vision über die Sekundärnutzung von Gesundheitsdaten. Bestehende Fehlanreize im Gesundheitssystem behindern eine sinnvolle Digitalisierung und Datenerfassung. Diese betreffen etwa die Tarifierung der ärztlichen Leistung, die Kosten der Erfassung der Daten oder die Transparenz über die Qualität und den Erfolg medizinischer Leistungen.

Die Stimme der Bürger:innen als Datensubjekte kommt zudem kaum zum Tragen. Ihr Vertrauen in die Sekundärnutzung von Daten ist im Zusammenhang mit der digitalen Selbstbestimmung zentral. Die Sekundärnutzung von Daten wird derzeit aber kaum diskutiert. In staatlich finanzierten Gesundheitswesen (wie etwa in Skandinavien) besteht ein gesellschaftlicher Konsens, dass die Gesundheitsdaten zum System und dem Staat zur Verfügung gestellt werden. Dieser Konsens fehlt in der Schweiz.

Darüber hinaus besteht eine grosse Heterogenität hinsichtlich der Form und der Qualität der Datenerfassung bei den Datenproduzent:innen (Spitäler, Arztpraxen, Apotheken etc.). Um hier semantische und technische Interoperabilität herzustellen, bedarf es grosser Anstrengungen.

Der Aufbau einer Gesundheitsdateninfrastruktur in einem Datenraum ist ein langjähriges Vorhaben, das eine Finanzierung erfordert. Diese sicherzustellen ist noch in weiter Ferne. Allerdings hat der Bundesrat angekündigt, dem Parlament bis Ende 2023 ein Programm zur «Förderung der digitalen Transformation im Gesundheitswesen» inklusive eines Verpflichtungskredites zu unterbreiten, sodass ab 2025 mit der Umsetzung gestartet werden kann.

6.4 Empfehlungen

1. Die Einwilligung der Bürger:innen in die Sekundärnutzung von Daten muss vom Gesetzgeber prioritär behandelt werden. Ein Widerspruchsrecht analog dem Transplantationsgesetz ist anzustreben.
2. Um dieses Widerspruchsrecht zu legitimieren, ist durch alle Beteiligte das Vertrauen der Bevölkerung in eine sinnvolle und wertstiftende Datennutzung zu gewinnen und zu erhalten. Dafür ist nebst einer hohen Datensicherheit die Transparenz eine wesentliche Voraussetzung. D. h. es muss dem Datensubjekt jederzeit möglich sein zu erfahren, welche Daten erfasst sind

[45] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20223890
[46] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-90422.html

und durch wen bzw. zu welchem Zweck diese Daten sekundär genutzt werden. Patient:innen sollten zudem die Möglichkeit haben, fehlerhafte Einträge zu korrigieren. Eine künftige Gesundheitsdateninfrastruktur sollte Datensubjekten jederzeit erlauben, die Nutzung ganz oder teilweise auszuschliessen (Opt-out-Lösung).

3. In diesem Zusammenhang muss die Datenkompetenz (Data Literacy)[47] der Bürger:innen wie auch der Leistungserbringer:innen berücksichtigt werden. Das Interface einer Gesundheitsdateninfrastruktur muss durch die Anbieter digitaler Lösungen so einfach und anwendungsorientiert wie möglich sein, um den Teilnehmenden einen möglichst niederschwelligen Zugang zu gewähren. Die Datenkompetenz der Leistungserbringer:innen muss zudem durch Fachorganisationen und Bildungsinstitutionen aktiv gefördert werden.
4. Um Gesundheitsdaten aus bestehenden und künftigen Datenbanken miteinander zu verbinden, muss der Gesetzgeber eine **einheitliche Identifikation für Patient:innen** (z. B. E-ID) realisieren. Eine solche würde es ermöglichen, pseudonymisierte Datensätze aus unterschiedlichen Datenbanken zu aggregieren und in der Folge zu nutzen.
5. In Hinblick auf eine strukturierte und interoperable Datenerfassung sollten Gesundheitsdaten für die Gesundheitsdateninfrastruktur durch die Leistungserbringer:innen prospektiv erfasst werden. Die Digitalisierung und die Kuration historischer Aufzeichnungen sind ineffizient. Zudem sind getrennte Systeme für die Speicherung der Daten und deren Darstellung zu entwickeln.
6. Die Finanzierung einer Gesundheitsdateninfrastruktur als öffentliches Gut benötigt Investitionen der öffentlichen Hand. Dabei ist ein stufenweises und iteratives Vorgehen zu wählen, welches mit den technischen, nationalen und internationalen Entwicklungen Schritt hält. Um neben den Investitionen der öffentlichen Hand private Investitionen zu ermöglichen, ist die Gouvernanz der Gesundheitsdateninfrastruktur durch den Gesetzgeber so auszugestalten, dass ihre Nutzung den Betrieb von Geschäftsmodellen erlaubt.
7. Das Gesundheitsversorgungssystem muss durch den Gesetzgeber digitalfreundlicher gestaltet werden: Es gilt Anreize zu setzen, um die Datenerfassung und die Datennutzung durch die Leistungserbringer:innen aktiv zu fördern.

[47] https://www.data-literacy.ch/

7 Nutzung personenbezogener Daten im Bildungsbereich

7.1 Ausgangslage und Wunschbild

Für die Nutzung personenbezogener Daten im Bildungsbereich werden vier Wunschszenarien skizziert: Verbesserte Lernumgebung, Steigerung der Kompetenzen, Schaffung organisatorischer und technischer Aspekte sowie Klärung übergeordneter Aspekte.

Verbesserte Lernumgebung

Verbesserte Lernumgebungen gliedern sich in die Flexibilisierung und Individualisierung des Lehrens und Lernens ein. Das Wunschbild der weiteren Digitalisierung zur Nutzung personenbezogener Bildungsdaten ist die verbesserte digitale und / oder hybride Pädagogik und Andragogik für Lehrpersonen, Schüler:innen, Lernende und Studierende, die ihr eigenes Lernen selbstbestimmt und aufbauend auf Daten nutzen möchten. Digitalisierung und Vernetzung der Lehre werden weiter voranschreiten. Zeit, Ort, Lerntempo und Lerninhalte werden vermehrt von Studierenden nach eigenen Kompetenzentwicklungen selbst festgelegt. Hierbei sollen mit Bildungsdaten Wege verbessert oder geschaffen werden, um aufbauend auf datenbasierten Vorschlägen persönliche Talente, einen genderneutralen Unterricht in der Schule (d. h. vorurteilsfreie Förderung von z. B. Mathematik- oder Sprachkompetenzen) sowie bedürfnisgerechte individuelle Lernsettings(z. B. auch in der Eltern- oder Erwachsenenbildung) zu fördern. Der individualisierte Unterricht und das personalisierte, kollaborative Lernen sollen dies befähigen.

Kompetenzen steigern

Die digitalen Kompetenzen aller beteiligten Akteur:innen (d. h. Schüler:innen, Studierende, Lernende, Lehrende, Eltern, Politik usw.) müssen gefördert werden. Zunächst sind in Zukunft relevante digitale Kompetenzen zu identifizieren, priorisieren und zielorientiert zu adressieren. Die Nutzenden von Lösungen, basierend auf personenbezogenen Bildungsdaten, müssen nicht die zugrundeliegende Technologie verstehen, sondern was mit ihren Daten passiert und wie ein Nutzen daraus entstehen kann. Die Mündigkeit der Nutzenden soll erhöht werden. Hierfür ist eine Sensibilisierung auf allen Ebenen erforderlich. Allgemein ist zur Data Literacy ein breiter Diskurs in der Gesellschaft erwünscht, insbesondere bei Lehrpersonen.

Organisatorische und technische Strukturen schaffen

Es bedarf gewisser organisatorischer und technischer Voraussetzungen, um Mehrwerte durch die Nutzung personenbezogener Bildungsdaten zu schaffen:

- Datengouvernanz und -management: Eine übergeordnete Organisation stellt die Vertrauenswürdigkeit verschiedener Akteur:innen sicher. Diese Vertrauensorganisation könnte relevante Leitplanken zur Orientierung festlegen, ethische Fragen klären, Nutzungsmöglichkeiten aufzeigen und generell das Ziel haben, Transparenz zur Datennutzung zwischen den Akteur:innen zu schaffen.
- Data-Space-Infrastruktur: Es gilt, eine vertrauenswürdige Infrastruktur mit Clearingstellen (d. h. Regeln, Entscheidungen, Kompetenzen, Kontrolle) zu schaffen. Diese stellt in den Bereichen Bildungscontent und Interaktionsdaten (von Tools und Services) Datenstandards

und Interoperabilität für Kontrolle und Personalisierung sicher. Die Nutzungsmöglichkeiten umfassen Datenerhebung, Prüfung der Validität von Daten, Steigerung der Datenqualität, Nachvollziehbarkeit der Nutzung und Schaffung eines verbesserten Zugangs zu Wissensressourcen. Alle Akteur:innen sollten Werkzeuge erhalten, um die Sekundärnutzung zu steigern. Einfache Bedienungsoberflächen vereinfachen dies.

Übergeordnete Aspekte klären

Die Souveränität zu personenbezogenen Bildungsdaten wird sowohl dem Individuum als auch dem Kollektiv zugeschrieben – Bildungsdaten als Gut der Gesellschaft. Der Personenbezug kann bei der Nutzung durch das Kollektiv, z. B. durch Pseudonymisierung, aufgehoben werden. Einfache und verständliche Use Cases für die Nutzung von Bildungsdaten ermöglichen die Entwicklung Problem-orientierter pragmatischer Lösungen. Dafür müssen Bildungsdaten zugänglich und nutzbar sein. Lösungen sollten so offen wie möglich gestaltet werden, wobei Akteur:innen dennoch die entsprechende Verantwortung dafür tragen müssen.

7.2 Laufende Initiativen

Zahlreiche Initiativen sind im Bereich Nutzung personenbezogener Bildungsdaten aktiv. Neben der Vernetzung von Stakeholder:innen und Expertise adressieren diese Anpassungen im Datenschutz, Harmonisierungen von Regeln und Prozessen, Verbesserung der Kompetenzen von Nutzenden, die Erstellung von themenbezogenen Wissensspeichern und die Konzeptionierung von Infrastrukturen zur sicheren Nutzung von Daten. Ziel ist eine Entwicklung weg von einem Datenschutz, der blockiert und Unsicherheit schafft, hin zu einer sicheren und transparenten Datennutzung. Infrastrukturen bieten die Chance, eine sichere Umgebung für die Nutzung von Daten zu bieten.

Educa, als Fachagentur im Auftrag von Bund und Kantonen, koordiniert Entwicklungen und führt Stakeholder:innen zusammen. Gleichzeitig bestehen verschiedene Initiativen zur Digitalisierung und zum Umgang mit dieser, z. B. durch pädagogische Hochschulen. Bildungsverlage schaffen durch die Digitalisierung ihrer Angebote mehr digitale Daten. Gleichzeitig entwickeln sie Analyseformen und personalisiertes Lernen auf Basis dieser Daten.

Data Use Cases

Die Use Cases für die Nutzung personenbezogener Bildungsdaten sind u. a. in den Bereichen Lifelong-Learning, Learning Analytics und Personalised Learning angesiedelt. Im Lifelong-Learning steht das Wissen im Zentrum, z. B. Nutzungsmöglichkeiten wie ein «Book of Knowledge» als Sammlung von allem je Gelernten. Bei Learning Analytics geht es v. a. um die Verbesserung der Lehrmethoden, aber auch um die Messbarkeit der Lehrpersonen in Bezug auf die Effizienz der Lernmaterialien. Personalised Learning beinhaltet Anwendungsfälle im Learning ohne Schul- und Altersgrenzen, datengetriebener Förderung des Individuums und personalisierte Gestaltung des Lehrangebots (z. B. auch für die Sekundarstufe 2).

Offen sind Fragen, wie man durch individualisierten Unterricht individuelle Talente stärken kann. Grundvoraussetzung für solche Use Cases ist eine breite Data Literacy – im Sinne des Verständnisses und der Verantwortung über eigene Daten. Nur ein Paradigmenwechsel hin zu einer nutzenorientierten Verwendung von Daten – unter Einhaltung von Datenschutz und Datensicherheit – kann diese datenbasierten Anwendungen ermöglichen.

Aus technischer Perspektive geht es bei der Nutzung personenbezogener Bildungsdaten um die Evaluierung, Beschreibung und Umsetzung sicherer Datenspeicherung, harmonisierter Schnittstellen und Datenformate sowie von Analysen unter Beachtung des Datenschutzes. Datenflüsse von Bildungsdaten von ihrer digitalen Erstellung bis hin zu ihrer Nutzung bzw. Löschung sind transparent zu beschreiben und nach geltenden Standards zu sichern.

7.3 Ungenügend adressierte Bereiche

Damit die Digitalisierung nicht beängstigend auf Individuen wirkt, sind Vertrauen und eine Art Positivismus in Bezug auf Tools, digital gespeicherte Daten, deren Vernetzung und Sekundärnutzung notwendig. All diese Aspekte müssen zu einem normalen und akzeptierten Teil des täglichen Lebens und insbesondere von Bildung, Lernen und Lehren werden.

Rechtliche Aspekte sind noch ungenügend geklärt und ein Blickwinkelwechsel hin zu Datennutzung ausstehend. Harmonisierung zwischen Bund und Kantonen sowie in Bezug auf rechtliche Konsequenzen von Erhebungszweck und Nutzungsinteresse ist sinnvoll. Unabhängig davon sollte zumindest eine klare und widerspruchsfreie Dokumentation der rechtlichen Situation, am besten anhand von Use Cases, bereitgestellt werden. Ein Fokus auf die Nutzung und den Nutzen von Daten im Bildungsbereich kann zu einer grundsätzlichen Veränderung der Situation führen. Es ist eine breite und nachhaltige gesellschaftliche Diskussion anzustossen. Hierzu gehören dann auch Weiterentwicklungen im Bereich Datengouvernanz und -management mit direktem Einbezug der Öffentlichkeit.

Bewährte, traditionelle Lernansätze sind noch wenig mit den Möglichkeiten der Digitalisierung angereichert, um verbesserte Lernumgebungen zu schaffen. Die Beteiligten sehen noch keinen klaren Mehrwert von Daten und digitalen Werkzeugen. Noch fehlen gute Konzepte, (Test-)Implementierungen und Innovationsprojekte sowie die entsprechenden notwendigen Ressourcen.

Kompetenzen in Bezug auf Digitalisierung und die Nutzung von Daten sind auf verschiedenen Ebenen nicht vorhanden. Es fehlt ein grundsätzliches Verständnis von Prozessen, Möglichkeiten und Konsequenzen der Datennutzung.

Ein digitales Bildungssystem kann nicht ohne IT-Infrastrukturen funktionieren. Aktuell gibt es keine Organisation, die für deren Betrieb und Weiterentwicklung zuständig wäre. Zudem fehlen Konzepte, offene Prozesse und Organisationen, die das Management und Controlling einer sicheren, zielführenden Datennutzung sicherstellen. Technisch braucht es die breite Unterstützung standardisierter Dateiformaten und Schnittstellen wie auch Lösungen für sichere Speicherung und die Nachvollziehbarkeit von Prozessen.

7.4 Empfehlungen

Politische und rechtliche Rahmenbedingungen klären

- Rechtliche Rahmenbedingungen von Bildungsdaten (Zugänglichkeit und Verfügbarkeit) sollten geklärt werden
- Bund und Kantone sollten die Entwicklung einer kohärenten Datennutzungspolitik für den Bildungsraum durch *educa* weiter befähigen. Hierbei sollten klare Regelungen von Bund

und Kantonen für alle Akteur:innen wie z. B. Lehrpersonen, Schulleitungen, Erziehungsberechtigte, Verwaltungen und Anbieter:innen von Lösungen entstehen und in der Breite verteilt werden wie auch eine gesellschaftliche Beteiligung gewährleistet sein.

Koordination und Zusammenarbeit stärken

- Eine zivilgesellschaftliche, unabhängige Organisation sollte den Austausch zwischen relevanten Akteur:innen im Themenfeld auf nationaler Ebene herstellen und dabei verschiedene Projekte (z. B. von kantonaler Stufe) und Initiativen zusammenbringen. Im Fokus sollte die Förderung des lebenslangen Lernens, die Aus- und Weiterbildung von Lehrpersonen und die Mündigkeit und Chancengerechtigkeit der Bürger:innen sein. Mitglieder aus diversen Bereichen wären hierbei wünschenswert.
- Ein regelmässiger, breiter Diskurs zwischen Akteur:innen aus der Bildung zum Wert und der sicheren Nutzung von personenbezogenen Bildungsdaten sollte durch die o. g. neue Organisation hergestellt werden. Hierbei geht es v. a. um den Austausch von Best Practices und die Herstellung gemeinsamer Projekte.
- Die Möglichkeiten zur Nutzung personenbezogener Bildungsdaten sollten bekannt sein. Lehrpersonen und Schüler:innen sollen Anwendungen spielerisch kennenlernen und implementieren können. Die o. g. Organisation könnte hierfür als Katalysator dienen.

Awareness und Data Literacy fördern

- Bildungsanbietende Organisationen und deren Koordinationsgremien sollten eine breite Awareness zu Mehrwerten bei der Nutzung personenbezogener Bildungsdaten unter Verwendung von Beispielen schaffen.
- Data Literacy, Datennutzung und der Datenschutz (Schutz vs. Nutzen) sollten Bestandteil von Ausbildungen und der fächerübergreifenden Lehre sein (inkl. Schulleitungen). Hierfür braucht es Rollen und Verantwortlichkeiten bei den verschiedenen Akteur:innen. Datenschützer:innen für Bildungsdaten sind erwünscht.

Organisatorische und technische Voraussetzungen schaffen

- Schaffung legitimierter, vertrauensvoller und nachhaltig finanzierter Träger und Bindeglieder für sichere Infrastrukturen, Tools, Services und den nötigen Daten-Gouvernanz und rechtlichen Rahmenbedingungen zur Nutzung (sensitiver) personenbezogener Bildungsdaten als grundlegendes Element zur Befähigung und breiten Nutzung.
- Herstellung eines Überblickes, welche Daten zur Sekundärnutzung vorhanden sind.

Nachhaltige Finanzierung sicherstellen

- Herstellung von verlässlichen, nachhaltigen Finanzierungsstrukturen zur Umsetzung auf verschiedenen Ebenen (Infrastrukturen und Use Cases, Organisationsstrukturen zur Befähigung und Dissemination, Bildung von Awareness sowie Moderation eines gesellschaftlichen Diskurses).

8 Gemeinsame Herausforderungen und übergeordnete Aspekte

Wie die Kapitel 5 bis 7 zeigen, ergeben sich in den drei Anwendungsbereichen sehr ähnliche Herausforderungen und Handlungsbedarfe.

8.1 Mangelnder Austausch und fehlender übergeordneter Rahmen

Das Verständnis rund um Personendaten im Zusammenhang mit digitaler Selbstbestimmung und vertrauenswürdigen Datenräume ist uneinheitlich. Aufgrund ihrer Sensibilität und fehlender Sensibilisierung für deren Nutzung, werden Personendaten teilweise sogar ausgeklammert. Es mangelt generell an Kenntnis der Thematik sowie an einer Übersicht über die aktuellen Entwicklungen. Nicht immer ist klar, wer den Aufbau vertrauenswürdiger Datenräume in der Schweiz vorantreiben soll. Viele Initiativen laufen auf unterschiedlichen Ebenen. Prinzipien-basierte übergeordnete Auslegeordnungen lassen sich allerdings oft nur schwer in die Praxis überführen und auf konkrete Use Cases runterbrechen. Es fehlt ein Abgleich zwischen laufenden Aktivitäten und ein übergeordneter Rahmen mit einer gemeinsamen Zielsetzung, um Personendaten in der Schweiz besser nutzen können.

Zudem besteht ein Spannungsfeld zwischen der Datennutzung und dem Datenschutz. Oftmals überwiegt die Diskussion um Risiken. In konkreten Use Cases ist der Mehrwert für das Teilen von Personendaten meist ersichtlich. Hingegen bestehen nachvollziehbare Vorbehalte gegenüber der Bereitschaft, Personendaten in grossem Stil zu sammeln und eine Sekundärnutzung über deren eigentlichen Verwendungszweck zu ermöglichen. Entsprechend gering ist die Motivation der betroffenen Akteur:innen, in die Datensammlung und -bereitstellung sowie den Aufbau entsprechender Strukturen zu investieren. Teils bestehen gar Fehlanreize, um Daten zu teilen: Ist deren Qualität beispielsweise unzureichend, kann dies zu einem Reputationsschaden für das erhebende Unternehmen führen. Oder es kann bestehende Geschäftsmodelle gefährden, die darauf basieren, Dienstleistungen mehrmals durchzuführen z. B. im Gesundheitswesen.

8.2 Globalisierung und Plattformökonomie

Sobald Plattformen eine gewisse Grösse erreichen, schaffen sie Abhängigkeiten zu ihren Ökosystemen und nehmen eine monopolartige Stellung ein. Für Kund:innen kann das von Vorteil sein: Sie profitieren oft von umfangreichen und kostenlosen Dienstleistungen. Wollen sie hingegen die Plattform wechseln, lassen sich z. B. persönliche Daten oder erworbene Dienstleistungen in der Regel kaum oder nur mit grossem Aufwand transferieren. Zudem gibt es meist keine Möglichkeit, die persönlichen Daten für Zwecke ausserhalb der Angebote des jeweiligen Ökosystems zur Verfügung zu stellen. Die Daten der Einwohner:innen der Schweiz werden daher zu einem grossen Teil im Ausland monetarisiert.

Grosse ausländische Akteur:innen erobern so immer mehr Bereiche. Wird die Schweiz in strategisch wichtigen Bereichen wie Mobilität, Gesundheit und Bildung nicht aktiv, werden andere es tun. Noch ist jedoch unklar, wie Datenräume in der Schweiz ausgestaltet sein sollen: Welche Akteur:innen übernehmen darin welche Rollen, wie wird der Zugang dazu gestaltet und wie deren Aufbau finanziert? Würden in der Schweiz öffentliche Gelder für den Aufbau von Datenräumen investiert und Personendaten zur Verfügung gestellt, dürfte dies jedenfalls nicht dazu führen, dass nur die Unternehmen mit den meisten Ressourcen davon profitieren.

9 Konkrete Empfehlungen für die bessere Nutzung von Personendaten in der Schweiz

9.1 Personendaten und individuelle Kontrolle mitdenken

Personendaten sollten beim Aufbau vertrauenswürdiger Datenräume immer mitgedacht werden. Bei der Nutzung von Personendaten stehen – im Sinne einer menschenzentrierten digitalen Transformation – die Individuen, deren Zugang zu und Kontrolle über die eigenen Daten im Zentrum. Bei Initiativen, bei denen dies noch nicht der Fall ist, sollten dies die Beteiligten schnellstmöglich nachholen. Zu beachten gilt, dass Bürger:innen bevorzugt eine Dateninfrastruktur nutzen, worüber sie Berechtigungen auf ihre Daten erteilen können.

Allfällige Hemmnisse sollten durch Umfragen bei Bürger:innen genauer untersucht werden. Beispielhaft ist hier das Paradoxon der Privatsphäre genannt: Einerseits sind Individuen sehr zurückhaltend, persönliche Daten kontrolliert zu teilen. Andererseits geben sie in sozialen Medien sehr intime Informationen über sich preis. Auf übergeordneter Ebene sollte in diesem Bereich der Bund die Kontrolle übernehmen, beispielsweise im Rahmen der «Strategie Digitale Schweiz». Sektorspezifisch sollten die treibenden Interessensgruppen aktiv werden.

9.2 Sensibilisierungs- und Data-Literacy-Aktivitäten ausbauen

Um bestehende Vorbehalte abzubauen, sind gesellschaftliche Voraussetzungen zu schaffen, d. h. eine Datennutzungskultur zu fördern und damit die Bereitschaft der Bevölkerung, personenbezogene Daten zu teilen, zu erhöhen.

Dafür gilt es, die richtigen Fragen zu stellen[48]. Organisationen, aber auch Bürger:innen sollten sich fragen, über welche Daten sie verfügen und welche Daten ihnen einen Mehrwert bieten. Darauf aufbauend sollten die jeweiligen Akteur:innen evaluieren, welche Rolle sie in einem Datenraum einnehmen möchten und unter welchen Bedingungen sie bereit sind, persönliche Daten zu teilen. Alle Akteur:innen sollten sich bewusst werden, welche Anreize sie haben, um Daten zu teilen. Es braucht ein breiteres Bild, eine gemeinsame Vision und ein besseres Verständnis darüber, welche Fragen sich mit Personendaten beantworten lassen und wofür man welche Daten erheben und verwenden möchte.

Darüber hinaus ist ein geeignetes Gefäss erforderlich, das einen regelmässigen Austausch erlaubt. Datenkooperationen und bedeutende Use Cases kommen dann zustande, wenn genügend Wertschöpfung daraus entstehen kann. Dieses Konzept gilt es zu verallgemeinern.

Der Bund sollte im Rahmen der «Strategie Digitale Schweiz» eine fortwährende Diskussion anstossen mit dem Ziel, eine Datennutzungskultur zu etablieren. Bei einem entsprechenden Mandat könnte dies das *Netzwerk Digitale Selbstbestimmung* in Zusammenarbeit mit sektoriellen Akteur:innen und weiteren bestehenden Netzwerken leisten.

[48] Eine wertvolle Sammlung guter Fragen findet sich hier: https://the100questions.org/

9.3 Einen übergeordneten Rahmen für vertrauenswürdige Datenräume schaffen

Um ihre digitale Souveränität zu wahren und zu verhindern, dass sie in Bereichen von nationaler Bedeutung – wie Mobilität, Gesundheit und Bildung – in die Abhängigkeit ausländischer Unternehmen gerät, muss die Schweiz geeignete Rahmenbedingungen schaffen. Es braucht rechtsverbindliche Bestimmungen für vertrauenswürdige Datenräume, Dateninfrastrukturen und Plattformen, die Missbrauch vorbeugen.

Dafür braucht es auch das entsprechende Wissen (Data Literacy) sowie ein gleichzeitiges Vorgehen auf verschiedenen Ebenen – Prinzipien-basiert top-down und Use-Case-getrieben bottom-up. Insbesondere aber ist die Koordination der laufenden Aktivitäten und damit einhergehend ein entsprechender Wissensaustausch sicherzustellen. Das *Netzwerk Digitale Selbstbestimmung* könnte bei einem entsprechenden Mandat einen regelmässigen Austausch mit sektoriellen Arbeitsgruppen und weiteren Initiativen moderieren.

Als Basis für dieses Vorgehen gilt es, einen übergeordneten und verbindlichen Rahmen für Schweizer Datenräume bereitzustellen. Das geplante Gesetz für die Sekundärnutzung von Daten sollte zusammen mit dem Verhaltenskodex einen solchen Referenzrahmen für Schweizer Datenräume aufspannen und die vermeintliche Unvereinbarkeit zwischen Datenschutz und Nutzung von Personendaten auflösen.

Der Verhaltenskodex für den Betrieb vertrauenswürdiger Datenräume basierend auf der digitalen Selbstbestimmung sollte breit angenommen werden. Um die Vertrauenswürdigkeit eines Datenraums sicherzustellen, braucht es aber mehr als einen auf Freiwilligkeit basierenden Verhaltenskodex, der auf dem Prinzip der Selbstregulation beruht. Der Verhaltenskodex sollte kontinuierlich hin zu einer übergeordneten und verbindlichen Gouvernanz weiterentwickelt werden. Zu prüfen ist auch die Einführung eines Labels für vertrauenswürdige Schweizer Datenräume.

Das Gesetz für die Sekundärnutzung von Daten sollte einheitliche Begrifflichkeiten definieren und einen gemeinsamen Referenzrahmen für vertrauenswürdige Schweizer Datenräume festlegen, um eine sekundäre Datennutzung unter Berücksichtigung des Datenschutzes zu fördern. Es sollte klare Zuständigkeiten für die Koordination von Aktivitäten zum Aufbau von Datenräumen festlegen. Es sollte die benötigte Finanzierung mittels öffentlicher Förderung durch Bund und Kantone als auch privater Investitionen regeln.

Weiter sollte das Gesetz für die Sekundärnutzung von Daten übergeordnete Regeln einführen, welche die Möglichkeiten von Akteur:innen berücksichtigen, aus Datenräumen Profit zu generieren und einer unangemessenen Bereicherung vorzubeugen. Der Bezug von Daten wird in irgendeiner Form mit Gebühren einhergehen müssen. Auch sind die anfallenden Kosten zu berücksichtigen, qualitativ hochwertige Daten zu erzeugen. Ansonsten besteht kein Anreiz, die Daten zur Verfügung zu stellen. Um Missbrauch zu vermeiden, braucht es eine Aufsicht, die national einheitlich sanktionieren kann.

Um einen Rückfluss für bezogene Daten sicherzustellen, könnten lokale Anbieter:innen Daten gratis beziehen, während grosse ausländische Unternehmen dafür bezahlen oder aber im Gegenzug wiederum Daten zur Verfügung stellen müssten. Ein weiteres Modell ist eine progressive Preiskurve, beginnend bei einer Gratisnutzung. Dies mindert die Motivation von Unternehmen,

übermässig zu konsumieren. Grundsätzlich nicht eingeschränkt wird der Zugriff auf Open Data. Das heisst aber nicht, dass sie auch kostenlos zur Verfügung gestellt werden. Bestehende Lizenzmodelle[49] könnten auch auf der Anbieterseite eingeführt werden.

Die Interoperabilität zwischen verschiedenen Schweizer Datenräumen wie auch auf internationaler Ebene ist zentral und zwingend sicherzustellen. Der Verhaltenskodex sowie ein allfälliges Gesetz für die Sekundärnutzung von Daten sollten hierzu wichtige Richtlinien liefern. Zudem sollten das *EDA* und das *BAKOM* wie auch sektorspezifische Akteur:innen den Austausch mit europäischen und weiteren ausländischen Initiativen aktiv verfolgen.

9.4 Anforderungen für Datenräume formulieren

Um den Aufbau sektorspezifischer Datenräume voranzutreiben, legen in dem Bereich aktive Organisationen gemeinsam fest, wer was in welcher Form und zu welchen Bedingungen zugänglich macht. Oder es besteht ein gewisser Zwang, indem der Regulator vorschreibt, welches Mindestmass an Daten geliefert werden muss. Darüber hinaus sollten Daten freiwillig geteilt werden können – mit erweiterten Spielregeln basierend auf gemeinsamem Nutzen.

Um Datenräume in unterschiedlichen Anwendungsbereichen aufzubauen sind bereichspezifische Bestimmungen und Standards erforderlich. Bei deren Ausgestaltung sind die Bedürfnisse aller Akteur:innen in den jeweiligen Rollen zu berücksichtigen. Wo noch nicht vorhanden, sollten sich die wesentlichen Akteur:innen in einem bestimmten Anwendungsbereich zu sektoriellen Communitys zusammenfinden, um ein gemeinsames Verständnis ihres jeweiligen Datenraums zu entwickeln. Auf Basis des oben dargelegten Referenzrahmens sollten sie detailliertere Gouvernanzmodelle formulieren. Ausserdem braucht es eine gemeinsame Semantik, Datenmodelle und sektorielle Standards sowie weitere Anforderungen an Daten und deren Austausch in Form von Regelungen und Reglementen.

Um solche Communitys zu formieren, sollten bestehende übergeordnete Branchenorganisationen und Initiativen den Lead übernehmen. Wo dies nicht besteht, sollte der Bund in Form des zuständigen Bundesamts sich darum bemühen, solche Gruppierungen zusammenzubringen. Um die Spielregeln eines Datenraumes zu definieren, sollten alle relevanten Interessensgruppen miteinbezogen werden. Dominante Akteur:innen sollten kein unverhältnismässiges Gewicht erhalten. Bestehende sektorielle Initiativen sollten unterstützt und eingebunden sowie ein regelmässiger Austausch zwischen entsprechenden Aktivitäten sichergestellt werden. Darüber hinaus sollten experimentelle Use Cases forciert werden, u. a. um den Nutzen zur Datensammlung auszuweiten und dafür zu motivieren sowie Vorbehalten aus der Bevölkerung vorzubeugen.

9.5 Erfahrungsaustausch und Wissenstransfer zwischen Sektoren sicherstellen

Um von bestehendem Wissen zu profitieren und gewonnene Erkenntnisse aus anderen Bereichen möglichst rasch adaptieren zu können und die Interoperabilität sicherzustellen, ist ein entsprechendes Gefäss für einen regelmässigen Austausch zwischen Schweizer Datenräumen zu institutionalisieren. Es braucht in der Schweiz einen gut moderierten intersektoriellen Austausch über Best Practices in der Umsetzung von Infrastrukturen, Definition von Standards etc. Es sind

[49] Vgl. z. B. https://creativecommons.org/licenses/by-sa/4.0/

bereits viele Initiativen in verschiedenen Sektoren unterwegs und ein grosser Erfahrungsschatz vorhanden. Dieser sollte über die Sektorgrenzen hinaus geteilt werden.

Das Prinzip Global Standards - Local Governance sollte berücksichtigt werden. Es wird für die Schweiz wichtig sein, Gruppen zu formieren, die in der Standardisierung wirken. Diese Standards können dann mit allen Stakeholder:innen geteilt werden, was die Maturität in den einzelnen Sektoren stark fördert. Die Rollen bestehender Organisationen wie *Digitale Verwaltung Schweiz DVS* und der Verein *eCH* sollten im Zusammenhang mit Schweizer Datenräumen geklärt werden. Auch der Austausch und die Mitwirkung in den entsprechenden Aktivitäten auf europäischer und globaler Ebene sind weiterzuverfolgen und wo nötig zu intensivieren.

9.6 Datensouveränität und internationalen Anschluss sichern

Um Datensouveränität zu erlangen, sollte die Schweiz mittels bilateraler Verträge die drei Ziele Kompetenzwahrung, Gestaltungsfreiheit und Abwehrfähigkeit sichern. Dafür kann sie mit anderen Staaten Vereinbarungen schliessen – z. B. damit Anfragen unter dem US CLOUD Act nur in Abstimmung mit dem *Bundesamt für Justiz (BJ)* erfolgen. Dabei sind innovative Ansätze möglich, bei denen das *BJ* neu eher eine Aufsichtsinstanz als wie bisher eine Genehmigungsinstanz wäre. So blieben die zentralen Rechtsgrundsätze der schweizerischen Verfassung gewahrt.

Die Schweiz könnte solche Mechanismen auch anderen Staaten anbieten und so ihre Rolle als Garantin für die Institutionen im Genève Internationale (*UNO, IKRK* etc.) weiterhin wahrnehmen. Die Diskussion um die Datensouveränität kann zur Chance für die Schweiz werden, wenn sie ihre Garantieverantwortung konzeptionell vertieft.

Die Schweiz sollte ihre Anschlussfähigkeit an die entstehenden europäischen Datenräume sicherstellen und sich entlang der Wertschöpfungskette von Datenproduzent:innen und Datenkonsument:innen positionieren.

- Die Gesetzgeber sollten für diese Aktivitäten einen geeigneten rechtlichen Rahmen entwickeln. Nachhaltige Modelle und Prinzipien für eine zukunftsweisende Datengouvernanz sind entscheidend für eine erfolgreiche zukünftige Datennutzung.
- *Die Zivilgesellschaft und Öffentlichkeit* sollte die Politik unterstützen, eine führende Rolle auf dem Gebiet der Datengouvernanz zu übernehmen. Die Schweiz hat mit ihrer ausgeprägten Diskussionskultur und einfach gehaltenen Gesetzgebungstradition gegenüber anderen Rechtsordnungen viel zu bieten.
- Unternehmen und Behörden sollten die Möglichkeiten von Datenräumen möglichst bald evaluieren und praktisch umsetzen: Wertvolle Datenbestände erschliessen, Infrastruktur bereitstellen und innovative Analysekompetenzen aufbauen.

Drei Akteursgruppen in der Schweiz sollten Datenräume und -marktplätze vorantreiben:

1. Industrie- und Wissenschaftsverbände sollten analysieren, was die Datenstrategie der *EU* für ihre Mitgliedsorganisationen bedeutet. Sie sollen ihren Mitgliedern deren Auswirkungen verständlicher machen, Chancen aufzeigen und politische Antworten identifizieren.
2. Politische Parteien sollten sich der rechtlichen und regulatorischen Auswirkungen der europäischen Datenstrategie auf die Schweizer Gesellschaft bewusstwerden und allenfalls eigene gesetzgeberische Antworten entwickeln. Parteien sollten diese Themen in die Öffentlichkeit tragen und eine breite Unterstützung der anvisierten Massnahmen sichern.
3. Organisationen und Unternehmen sollten schon heute damit beginnen, das Innovationspotential aus Daten systematisch zu analysieren und zu bewerten.

10 Involvierte Personen

10.1 Autor:innen übergreifende Aspekte

2 Vorwort	Matthias Michel, Ständerat (Zug)
3.1 Netzwerk digitale Selbstbestimmung	Manuel Kugler, SATW
3.2 Vertrauenswürdige Datenräume	Manuel Kugler, André Golliez
4.1 Datensouveränität	Christian Laux, *Laux Lawyers*
4.2 Die europäische Datenwirtschaft	Giulia Fitzpatrick & André Golliez
4.3 *Gaia-X* und internationale Data Hubs	Jonas Bärtschi/Thomas Gees, *BFH*
4.4 Die digitale Identität als Katalysator für vertrauenswürdige Datenökosysteme	Daniel Säuberli, *DIDAS*

10.2 Autor:innen Mobilitätsdatenraum

- Andreas Kronawitter, *its-ch*
- Manuel Kugler, SATW
- Andreas Schlag, *Ti&M*
- Oliver Buschor, *Rapp*
- Thomas Teichmüller, *AWK*
- Peggy Neubert, *VBZ*
- Andreas Bieniok, *Scheidt-Bachmann*
- Richard Lutz, *Postauto AG*

10.3 Autor:innen Gesundheitsdatenraum

- Roger Abächerli, *Institut für Medizintechnik*, *HSLU*
- Serge Bignens, *Institut für Medizininformatik*, *BFH*
- Mathis Brauchbar, *santeneXt/advocacy*
- Manuel Kugler, SATW
- Marie-Jeanne Semnar, *Interpharma*
- Stefan Spycher, *Stiftung Careum*

10.4 Autoren Bildungsdatenraum

Autoren: Prof. David Schiller, Dr. Sebastian Sigloch

Expert:innen der Arbeitsgruppen

- Nicolas Brandenberg
- André Golliez
- Manuel Kugler
- Clemens Mader
- Daniela Melone
- Tobias Röhl
- David Schiller
- Sebastian Sigloch
- Christoph Wittmer