Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Direktion für Völkerrecht DV

Bundesamt für Kommunikation BAKOM

satw
it's all about technology

Swiss Data Alliance

Digitale Selbstbestimmung

Stand 16.10.2020

Dieses Diskussionspapier gibt eine Einführung in die Schweizer Initiative «Netzwerk digitale Selbstbestimmung». Es wurde von einer Arbeitsgruppe bestehend aus Vertreterinnen und Vertretern der Bundesverwaltung, Forschung und Wirtschaft erarbeitet. Ziel dieses Papiers ist, das Konzept «Digitale Selbstbestimmung» für einen breiten Kreis von Leserinnen und Lesern zugänglich zu machen und Ideen für die weitere Umsetzung aufzuzeigen.

Auf einen allgemeinen Beschrieb in der Einleitung folgen Ausführungen zur Relevanz der digitalen Selbstbestimmung. Anschliessend werden Grundprinzipien, rechtliche Aspekte und der Aufbau vertrauenswürdiger Datenräume als zentrale Bausteine der digitalen Selbstbestimmung dargestellt. In den drei Anhängen finden sich illustrative, fiktive Beispiele aus den Sektoren Mobilität, Bildung und Energie.

1. Einleitung

Wir alle sind in der digitalen Welt Konsumentinnen und Konsumenten digitaler Dienstleistungen, wobei wir primär die Rolle von Nutzern (*user*) einnehmen. Das Internet und digitale Anwendungen erleichtern unser Leben, bereichern und unterhalten uns. Die Entwicklung neuer Soft- und Hardware schreitet rasant voran, neue Apps und Dienstleistungen sind wie Manna, das auf uns herabregnet. Wer an der digitalen Welt partizipieren will – heute oftmals unerlässlich, wie auch die COVID-19-Krise verdeutlicht – hat häufig keine andere Wahl, als seine Daten preiszugeben. Wir haben uns dabei derart an unsere Rolle als *user* gewöhnt, dass wir uns kaum mehr vorstellen können mitzubestimmen, wie der digitale Raum ausgestaltet sein soll.

Diese passive *user*-Haltung steht im Gegensatz zu unserem Selbstverständnis als aktive Bürgerinnen und Bürger einer demokratisch und rechtsstaatlich organisierten Gesellschaft, in der wir mitentscheiden können. Noch beunruhigt uns dieser Widerspruch zwischen Offline- und Online-Welt wenig, da die Spannungen zwischen den beiden Welten selten spürbar sind. Die digitale Transformation steht erst am Anfang und sie wird immer tiefer und subtiler in unser Alltagsleben eindringen.

Es stellt sich die Frage, ob eine selbstbestimmt partizipative oder eine konsumorientierte Rolle des Individuums die Digitalisierung prägen wird. Wird sich die Welt der selbstbestimmten Bürgerinnen und Bürger auch in der digitalisierten Zukunft durchsetzen, kann die digitale Transformation unsere Demokratie stärken und die Wohlfahrt vergrössern. Sie wird digitale Plattformen und Ökosysteme in den zentralen öffentlichen und wirtschaftlichen Bereichen ermöglichen, z.B. Energie, Gesundheit oder Mobilität, wo Daten transparent, nach klaren Spielregeln und zum Nutzen aller Beteiligten erhoben und verarbeitet werden. Bleiben wir hingegen reine *user,* wird unser Leben zunehmend fremdbestimmt, was unsere Demokratie und unseren Rechtsstaat schwächen sowie den wirtschaftlichen und ideellen Nutzen der digitalen Transformation für unser Land mindern würde.

Die Schweiz setzt sich für eine partizipative Digitalisierung ein, in der die Menschen und ihre digitale Selbstbestimmung im Zentrum stehen[1]. Die digitale Selbstbestimmung soll Bürgerinnen und Bürger, aber auch Unternehmen und öffentliche Einrichtungen befähigen, über ihr Leben und Handeln im digitalen Raum selbst zu bestimmen. Selbstbestimmung im digitalen Raum bedeutet, dass Bürgerinnen und Bürger einerseits Kontrolle und Zugang zu von ihnen bereitgestellten Daten haben[2]. Andererseits sollen sie die Relevanz dieser Daten verstehen und deren Wert einordnen können sowie wissen, zu welchem Zweck diese Daten wiederverwendet werden. Die Teilhabe an der digitalen Welt soll nicht mehr mit einem Kontrollverlust über die eigenen Daten einhergehen. Dafür braucht es neue Strukturen, die dem Individuum eine aktive Steuerung der digitalen Transformation ermöglichen.

Ein selbstbestimmter Umgang mit Daten stärkt das Vertrauen in eine nachhaltige Datengesellschaft und kommt sowohl der Wirtschaft als auch der Öffentlichkeit zugute. Konkret sollen auf dieser Basis vertrauenswürdige Datenräume geschaffen werden, welche allen Akteuren aus Wirtschaft und Gesellschaft einen Mehrwert bieten. Damit schmälern sie die Abhängigkeit von grossen Tech-Konzernen und ermöglichen eine Selbstbestimmung im wirtschaftlichen und politischen Sinn.

Die Umsetzung der digitalen Selbstbestimmung erfordert das Zusammenwirken von Verwaltung, Wirtschaft, Wissenschaft und Zivilgesellschaft. Zu diesem Zweck schaffen wir ein nationales Netzwerk, das den Rahmen für die Selbstbestimmung im digitalen Zeitalter festlegt und diese vorantreibt. Darauf aufbauend soll auch ein internationales Netzwerk entstehen, um die digitale Selbstbestimmung gemeinsam mit gleichgesinnten Partnern weltweit zu verwirklichen. So soll dem Individuum auch grenzüberschreitend ermöglicht werden, im digitalen Raum proaktiv zu handeln und mitzuentscheiden.

---

[1] Siehe dazu die Grundsätze und Kernziele der Strategie «Digitale Schweiz» des Bundesrats vom September 2020

[2] Es gilt hier jedoch auch zu beachten, dass für gewisse Daten eine gesetzliche Erhebungspflicht besteht. In einem solchen Falle wäre die Kontrollfähigkeit von Individuen beschränkt.

2. Relevanz der digitalen Selbstbestimmung

Die digitale Selbstbestimmung versteht sich als langfristiges Ziel. Unsere Gesellschaft soll das Potenzial der Datenwirtschaft auf Basis unserer demokratischen Werte optimal nutzen. Alle Akteure sollen gemeinsam zu sicheren und vertrauenswürdigen digitalen Plattformen und Datenräumen beitragen und den entstehenden Mehrwert zum Nutzen aller einsetzen.

Das Konzept der digitalen Selbstbestimmung soll als Wertehaltung und Vision in der Entwicklung von Schweizer Datenräumen dazu führen, dass die Bürgerinnen und Bürger im Mittelpunkt der digitalen Transformation stehen und zum proaktiven Handeln befähigt werden. Auch im digitalen Raum sollen Grundrechte selbstbestimmt ausgeübt und die Entscheidungsfreiheit gewahrt werden.

Daten werden heute in unterschiedlichen Lebensbereichen intransparent und ohne Kontrolle der betroffenen Individuen gesammelt und ausgewertet. Umfangreiche Informationen werden ohne explizite Zustimmung in Datenpools eingelesen, zur Profilbildung von Nutzerinnen und Nutzern verwendet und anschliessend aggregiert oder personalisiert weiterverwendet. Solche Daten werden auch routinemässig an Dritte weitergegeben oder verkauft.

Dieser Trend wird sich ohne Veränderung auf Grund der technologischen Fortschritte weiter verstärken. Während eine solche Datennutzung legitime Businessmodelle erlaubt, muss man sich über deren Konsequenzen im Klaren sein: Sie verstärkt bestehende Bedenken und schafft auf längere Sicht Abhängigkeiten und Risiken. So werden immer mehr sensitive Daten mit hohem Manipulations- oder Missbrauchspotential bei einzelnen Unternehmen konzentriert. Dies kann einerseits auf individueller Ebene zu Diskriminierungen führen[3], andererseits auf organisatorischer Ebene zu Wettbewerbsverzerrungen, überhöhter Marktmacht und politischer Einflussnahme einzelner Datengiganten.

Digitale Selbstbestimmung soll keine Business-Modelle verunmöglichen oder gar verbieten. Vielmehr sollen Alternativen und deren Mehrwert aufgezeigt werden. Die Anwendungsbeispiele im Anhang illustrieren den spezifischen Nutzen, den ein digital selbstbestimmter Umgang mit Daten für das Individuum und die Gesellschaft haben kann: Einerseits wirkt er den aktuell weitverbreiteten Gefühlen von Machtlosigkeit und Unwohlsein entgegen und schafft grösseres Vertrauen in die Sammlung und Nutzung von Daten. Andererseits ermöglicht er die Entwicklung neuer innovativer Anwendungen zum Nutzen des Individuums, aber auch des Gemeinwohls und steigert so die Lebensqualität.

Die Schweiz soll mit der Verwirklichung dieser Vision auch international Einfluss ausüben und aufzeigen, wie der digitale Wandel durch Bürgerinnen und Bürger, Politik, den öffentlichen Sektor, Wissenschaftsinstitutionen und Wirtschaft unter Wahrung der Grundrechte gemeinsam gestaltet werden kann.

Grundprinzipien

Um eine digitale Transformation mit dem Menschen im Zentrum zu realisieren, sollen die folgenden **Grundprinzipien** berücksichtigt werden:

1. **Transparenz und Vertrauen**: Dem gegenwärtigen Zustand des Unbehagens werden vertrauenswürdige Rahmenbedingungen entgegengesetzt. Diese beinhalten unter anderem Transparenz über die Erfassung, Nutzung und Verarbeitung von Daten sowie einen klar definierten Zweck und die Nachvollziehbarkeit über den Zugang Dritter zu diesen Daten.
2. **Kontrolle und selbstbestimmte Weitergabe:** Bürgerinnen und Bürger haben die Kontrolle über ihre persönlichen Daten. Sie können effektiv auf alle von ihnen bereitgestellten und für ihre Entscheidungen relevanten Daten zugreifen, die Aussagekraft und den potenziellen Wert dieser Daten einschätzen sowie deren Nutzung durch Dritte selbst bestimmen. Ausnahme bilden einzig Daten zur reibungslosen Abwicklung von Grundversorgungsleistungen. Insbesondere kontrollieren Bürger*innen die Art der Weitergabe ihrer Daten: sei es (a) anonymisiert, d.h. ein Rückschluss auf die Person ist nicht mehr möglich, (b) mit Verfahren der Differential Privacy unkenntlich gemacht, d.h. ein Rückschluss auf die Person ist auch mit Drittdaten nur mit einer gewissen, definierten Wahrscheinlichkeit möglich, (c) pseudonymisiert, d.h. die Identifikations-

[3] Vgl. Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems

merkmale wurden unkenntlich gemacht und durch ein Pseudonym ersetzt, wobei sich ein Rückschluss auf die Person unter Umständen mit weiteren Daten wieder herstellen lässt, oder sogar (d) unter Umständen auszugsweise ohne Verschleierung in Reincode.

3. **Nutzerorientierte datenbasierte Ökosysteme:** Individuen können ihre Daten effizient auf Dienstleister ihrer Wahl übertragen sowie den Dienstleister wechseln (Datenportabilität). Ökosysteme fördern den Austausch von Daten zwischen verschiedenen Akteuren. Sie ermöglichen dadurch innovative digitale Services und befähigen Individuen und Dienstleister, das Potenzial von Daten effektiver und nachhaltiger zu nutzen.
4. **Dezentralisierung und Bürgernähe:** Daten werden heute überwiegend für Dienstleistungen auf nationaler oder globaler Ebene genutzt. Lokal und regional hingegen gibt es wenig finanzstarke Akteure, die das Datenpotenzial effektiv nutzen können. Dezentrale Datenräume schaffen neue Möglichkeiten für den Gebrauch von Daten und die Verbesserung von Dienstleistungen auf lokaler und regionaler Ebene.

Auswirkungen auf Bürgerinnen und Bürger, Unternehmen und den öffentlichen Sektor

Für **Bürgerinnen und Bürger** bedeutet dies, dass

- sie die Fähigkeit haben, alle von ihnen bereitgestellten und für ihre Entscheidungen relevanten Daten zu kontrollieren und darauf zuzugreifen;
- diese Daten und ihre Relevanz eigenständig eingeordnet und verstanden werden können;
- Kenntnis darüber besteht, wer sonst noch Zugang zu diesen Daten hat, wer diese interpretieren kann oder zu welchem Zweck Algorithmen zum Einsatz kommen;
- sie Kontrolle darüber haben, wie und in welchem Ausmass Dritte zu diesen Daten gelangen und mit diesen umgehen;
- auch Personen, welche nur eingeschränkten oder gar keinen Zugang zu digitalen Infrastrukturen haben, weiterhin selbstbestimmt agieren können.

Für **Unternehmen** bedeutet dies, dass

- sie auch weiterhin die Möglichkeit haben, die von ihnen produzierten Daten zu nutzen;
- transparente und verlässliche Regeln für den Umgang mit Daten existieren;
- datenbasierte Erkenntnis- und Effizienzgewinne zur Entwicklung von neuen Dienstleistungen und Angeboten innerhalb klar definierter Rahmenbedingungen genutzt werden können;
- sie in funktionierende Ökosysteme eingebettet sind und damit über einen verbesserten Zugang zu relevanten Daten verfügen;
- die Wettbewerbsfähigkeit im relevanten Markt sowie der Schweizer Volkswirtschaft als Ganzes gesteigert werden kann.

Für den **Staat und den öffentlichen Sektor** bedeutet dies, dass

- die Informationsgrundlagen zur Ausübung staatlicher Hoheitsaufgaben sichergestellt bleiben;
- verfassungsmässige Rechte der Bevölkerung auch in der digitalen Welt weiterhin gewährleistet werden, insbesondere die Sicherung des Zugangs zu Daten und der Schutz vor (digitaler) Willkür durch andere Akteure; datenbasierte Erkenntnis- und Effizienzgewinne durch den öffentlichen Sektor realisiert werden und zur Weiterentwicklung des Service Public oder der Steigerung des öffentlichen Gemeinwohls beitragen können;
- der Staat frühzeitig und kontinuierlich über seine Lagebeurteilungen, Planungen, Entscheide und Vorkehren informiert, um selbstbestimmtes Handeln in der Zivilgesellschaft zu fördern.

3. Rechtliche Aspekte der Digitalen Selbstbestimmung

Das Rechtssystem als Teil der sozialen Ordnung steht in einem konstanten Wechselspiel zwischen den Veränderungen gesellschaftlicher Werte oder den Fortschritten der Technologie. Die verfassungsrechtlich garantierten Grundrechte gelten auch im digitalen Raum: Viele Schutzpflichten, die den Kern der digitalen Selbstbestimmung ausmachen, ergeben sich aus den bereits bestehenden Grundrechten des Individuums, wie der Meinungsäusserungs- und Informationsfreiheit, der persönlichen Freiheit und dem Schutz der Privatsphäre (insbesondere dem Schutz der «informationellen Selbstbestimmung»). Demnach obliegt es dem Individuum, zu entscheiden, dass und wofür seine Daten genutzt werden dürfen. Digitale Selbstbestimmung verlangt somit nicht nach einem neuen Grundrecht, sondern es gilt, diese im Licht der vorhandenen Grundrechte auszulegen.

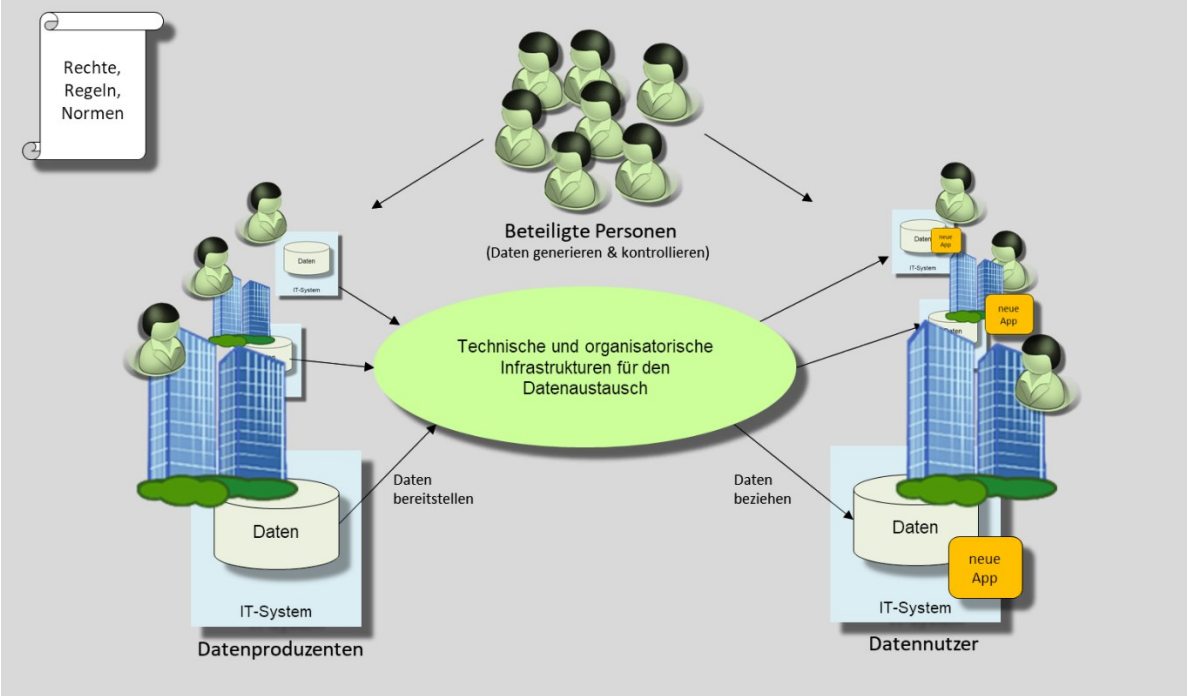
Nicht nur auf Verfassungs-, sondern auch auf Gesetzesstufe – sowohl im öffentlichen Recht als auch im Privatrecht – schützen verschiedene Vorschriften explizit oder implizit das digitale Selbstbestimmungsrecht des Individuums. Neben den datenschutzrechtlichen Bestimmungen ist beispielsweise der zivilrechtliche Persönlichkeitsschutz zu nennen.

Ersichtlich wird die integrative rechtliche Einbettung der digitalen Selbstbestimmung in unser Rechtssystem auch vor dem Hintergrund der Covid-19-Pandemie. So wird die digitale Selbstbestimmung beispielsweise im Rahmen des «Contact Tracing» herausgefordert. In der juristischen Lehre besteht Einigkeit darüber, dass die Individuen über die Bearbeitung ihrer Daten aufgeklärt werden müssen und nur mit der jeweiligen Einwilligung, einer entsprechenden gesetzlichen Grundlage oder bei überwiegendem privaten oder öffentlichen Interesse die entsprechende Bearbeitung vorgenommen werden darf. Fraglich ist, wie die Kontrolle über den ganzen Lebenszyklus von Daten – von der Erhebung, Auswertung, Verwendung und Weiterverwendung – auszugestalten ist.

Deutlich wird, dass die digitale Selbstbestimmung mehr als eine blosse Erweiterung des Datenschutzrechts ist. Die Kernelemente der digitalen Selbstbestimmung als Ausdruck unserer gesellschaftlichen Werte und der oben dargelegten Grundprinzipien sind sowohl auf Verfassungs- als auch auf Gesetzesstufe verankert und durchdringen alle Rechtsgebiete. Das Konzept der digitalen Selbstbestimmung zielt auf die Verwirklichung derselben und begnügt sich nicht mit der formalen rechtlichen Anerkennung eines individuellen Rechts. Sie setzt vielmehr ein Ökosystem mit geeigneten Rahmenbedingungen voraus, d.h. vertrauenswürdige Datenräume, in welchen sich Individuen und Unternehmen selbstbestimmt entfalten können.

4. Vertrauenswürdige und interoperable Datenräume

Datenbasierte Dienstleistungen bedingen die Nutzung von Daten über ihren ursprünglichen Verwendungszweck hinaus. Für eine vertrauenswürdige Datennutzung, welche den Grundprinzipien der digitalen Selbstbestimmung entspricht, braucht es die Verständigung und Zusammenarbeit der Datenproduzenten[4], der Datennutzer[5] und der beteiligten Personen[6]. Ein Datenraum ermöglicht eine solche Zusammenarbeit auf Basis von gesetzlich verankerten Rechten, verbindlichen Regeln sowie gemeinsamen technischen und organisatorischen Infrastrukturen. Dadurch gewährleistet ein Datenraum die Bereitstellung und den Austausch von Daten sowie deren Zugang. Datenräume können auf regionaler, nationaler und internationaler Ebene entstehen und die Datennutzung in einem bestimmten Wirtschaftssektor als auch über die Grenzen einzelner Sektoren hinaus umfassen.



Geteilte und offene Sachdaten

Damit der Austausch und die Nutzung von Daten funktioniert, ist der unterschiedlichen Zugänglichkeit zu Sachdaten Rechnung zu tragen[7]. Sogenannte «closed data» sind unter striktem Verschluss und einzig für einen eingeschränkten Benutzerkreis innerhalb einer Unternehmung oder Verwaltung zugänglich. Geteilte Daten («shared data») können unter bestimmten restriktiven Bedingungen innerhalb und ausserhalb des Unternehmens oder der Verwaltung genutzt werden. Offene Daten («open data»), die sich nicht auf Personen beziehen und auch sonst keine speziell schützenswerten Informationen enthalten, sind für die Öffentlichkeit zur freien Nutzung zugänglich.

In den letzten Jahren wurde die Nutzung von geteilten und offenen Daten, insbesondere Daten der öffentlichen Verwaltung (Open Government Data), vermehrt gefördert. Auch in der Schweiz hat der Bundesrat 2018 eine Strategie für offene Verwaltungsdaten verabschiedet[8]. Diese Entwicklungen haben allerdings erst teilweise zu Systemen zur gemeinsamen Datennutzung geführt. Hier setzten Datenräume an: Durch die Verbindung verschiedener Datenquellen und deren Einbettung in eine technische, rechtliche und organisatorische Infrastruktur ermöglichen Datenräume die institutionalisierte Nutzung und Teilung geteilter und offener Daten innerhalb eines Ökosystems.

---

[4] Unternehmen und Verwaltungen, die für Daten verantwortlich sind und solche für die Nutzung durch Dritte bereitstellen.

[5] Unternehmen und Verwaltungen, die bereitgestellte Daten beziehen und damit neue Anwendungen entwickeln und betreiben.

[6] Individuen oder kollektive Körperschaften, z.B. ein Quartier oder eine Stadt, die Rechte an den bereitgestellten Daten haben.

[7] Zum Zweck der Verständigung über diese Frage hat das Open Data Institute in London (gegründet vom Web-Erfinder Sir Tim Berners-Lee) das sogenannte Data Spectrum definiert, auf welches wir hier explizit Bezug nehmen (siehe https://the-odi.org/about-the-odi/the-data-spectrum/).

[8] Siehe https://www.admin.ch/opc/de/federal-gazette/2019/879.pdf.

Personenbezogene Daten

Daten, welche sich auf eine bestimmte oder bestimmbare Person beziehen, unterstehen einem besonderen Schutz und sind rechtlich in der Datenschutzgesetzgebung geregelt. Diese Gesetze schützen die einzelne Person vor Missbrauch der sie betreffenden Daten. Die Wertschöpfung, welche mit der Nutzung personenbezogener Daten erzielt werden kann, ist hingegen nicht geregelt.

Datenräume und weitere Formen der gemeinsamen Datennutzung

Datenräume können in verschiedenen Formen gestaltet werden. Datenproduzenten und -nutzer definieren unter Einbezug der beteiligten Personen den Umfang und die Formate der Daten, die über die gemeinsamen technischen Infrastrukturen ausgetauscht werden sollen. Sie regeln deren Bereitstellung, Austausch und Bezug sowie die Kontrolle dieser Abläufe durch die beteiligten Personen. Die Teilnehmer des Datenraumes bauen die technischen Infrastrukturen für den Datenaustausch schrittweise auf und finanzieren deren Betrieb.

Rechtsform, Struktur, Mitgliedschaft und Regeln eines Datenraumes richten sich nach Umfang und Zielen des Datenaustausches und der aufzubauenden Infrastrukturen – unter Einbezug genereller Grundprinzipien. Es sind zeitlich limitierte multilaterale Vereinbarungen, zivilrechtliche Vereine, Stiftungen, Genossenschaften oder Gemeinschaftsunternehmen denkbar. Datentreuhänder («Data Stewards») können im Auftrag der Datenproduzenten, den Datennutzern und weiteren beteiligten Personen die Abwicklung des Austausches übernehmen. Auch öffentliche Verwaltungen, staatsnahe Unternehmen und Forschungseinrichtungen kommen als Träger für Datenaustausch-Infrastrukturen in Betracht.

Über Datenräume hinaus sind weitere Formen der gemeinsamen Datennutzung denkbar und ansatzweise bereits vorhanden. So können Datenproduzenten und -nutzer Daten mit beschränkter Zugänglichkeit in einem Markt handeln. Oder Produzenten können Daten über öffentliche Plattformen unbekannten Nutzern offen oder unter restriktiven Bedingungen zugänglich machen[9]. Eine weitere Form der gemeinsamen Datennutzung sind Digitale Zwillinge («Digital Twins»), die materielle Infrastrukturen auf der Basis von Echtzeitdaten digital nachbilden.

Ein aktuelles Beispiel für den Aufbau eines sektoriellen Datenraumes in der Schweiz ist das Projekt «Nationale Datenbewirtschaftung»[10]. Damit schafft der Bund zusammen mit den Kantonen und Gemeinden einen Datenraum sowie eine Infrastruktur zur gemeinsamen Datennutzung im Rahmen der öffentlichen Verwaltung. Ein weiteres Beispiel ist der Politikbereich. Gestützt auf den Civic-Tech-Bericht[11] hat der Bundesrat die Bundeskanzlei mit der Entwicklung eines übergeordneten und technologieneutralen Datenmodells für politische Geschäfte und der dazugehörigen Materialien beauftragt. Er schafft damit den konzeptionellen Rahmen für einen einheitlichen Datenraum in der Schweizer Politik.

Regeln

Für Datenräume sind Regeln zu vereinbaren, welche den Prinzipien der digitalen Selbstbestimmung Geltung verschaffen. Zudem braucht es Massnahmen, welche deren Einhaltung durch die beteiligten Akteure überwachen. Dazu gehören u.a. die folgenden Punkte:

Die beteiligten **Personen** können

- einsehen, welche Daten (und Metadaten) zu welchem Zweck über sie erhoben werden;
- sicher sein, dass nicht weitere Daten über sie gesammelt werden;
- sicher sein, dass Daten nicht unkontrolliert an Dritte weitergegeben werden;
- ihre explizite Zustimmung zur Verwendung von gewissen Daten geben und diese jederzeit widerrufen (und werden davor geschützt, diese Zustimmung nicht zu Zwecken zu geben, die unkontrolliert oder für sie nachteilig sind = Missbrauchsvorbehalt);
- die Ergebnisse der Verwendung einsehen und soweit möglich nachvollziehen;
- an den Ergebnissen der digitalen Transformation (wirtschaftlich oder ideell) partizipieren.

---

[9] Bereits bestehende oder geplante Beispiele für solche Plattformen in der Schweiz sind die Infrastruktur für gemeinsame Daten und Services im Bereich Mobilität (siehe Anhang 4), der Schweizer Energy Data Hub (siehe Anhang 5), Datenkooperation touristischer Leistungsträger der Region Luzern und Vierwaldstättersee (NRP-Projekt) oder die Open Government Data Plattform Schweiz

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

[11] Siehe https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-79052.html.

Die **Datenproduzenten**

- verpflichten sich, nur diejenigen Daten (und Metadaten) herauszugeben, für welche sie entweder die gesetzliche Pflicht oder die Zustimmung der beteiligten Personen (Missbrauchsvorbehalt, siehe oben) und allenfalls weiterer Datenberechtigter erhalten haben;
- sorgen dafür, dass alle Datennutzer auf diskriminierungsfreie Art und Weise Zugang zu den Daten erhalten;
- stellen Unterlagen bereit, welche zum Verständnis der Daten notwendig sind;
- sorgen dafür, dass die Daten so lange erhalten bleiben, wie sie gemäss Vereinbarung von den Datennutzern in Anspruch genommen werden können.

Die **Datennutzer**

- verwenden Daten ausschliesslich im Rahmen der vereinbarten Zwecke;
- legen die Datennutzung offen, machen sie transparent und nachvollziehbar;
- stellen beteiligten Personen die Ergebnisse der Nutzung gemäss Vereinbarung zur Verfügung;
- löschen die Daten, sobald die vereinbarte Verwendungsdauer abgelaufen ist.

Datenräume im nationalen und internationalen Kontext

Eine sektorspezifische lokale, regionale oder nationale Verankerung von Datenräumen entspricht der föderalen, dezentralen und auf Autonomie der Akteure bedachten politischen Kultur der Schweiz. Datenräume ermöglichen es KMU, Verwaltungen und zivilgesellschaftlichen Organisationen pragmatisch in einem überblickbaren Rahmen zusammenzuarbeiten und mit konkreten Anwendungen schrittweise Erfahrungen bei der gemeinsamen Nutzung von Daten zu sammeln. Gezielt sollen Austausche und Koppelungen zwischen den sektorspezifischen Datenräumen geprüft werden, um die Nutzung von Daten über ihren ursprünglichen Verwendungszweck hinaus im Interesse aller Beteiligten zu ermöglichen.

Dieses Modell könnte auch für andere Länder von Interesse sein. Die Schweiz kann es in die internationalen Gespräche mit anderen Staaten und sonstigen Akteuren einbringen und im Gegenzug von anderen Ansätzen beim Aufbau von Datenräumen profitieren. Die Datenstrategie der EU beispielsweise fasst die Schaffung eines einheitlichen europäischen Datenraumes ins Auge[12]. Die EU will zehn europäische Datenräume in strategischen Sektoren und Bereichen von öffentlichem Interesse aufbauen[13]. Dazu zählen u.a. ein Datenraum für den europäischen grünen Deal, ein Mobilitätsdatenraum sowie ein Gesundheitsdatenraum. Vor diesem Hintergrund gilt es für die Schweiz in den kommenden Jahren den Aufbau von Datenräumen zu fördern, diese untereinander und international zu vernetzen und die Erfahrungen zu systematisieren.

Digitale Selbstbestimmung wird in der Schweiz insbesondere dann erfolgreich sein, wenn es gelingt, deren Prinzipien auch ausserhalb der Schweiz zu verankern. Anzustreben ist daher eine enge Zusammenarbeit mit anderen Ländern, welche ähnliche Grundwerte wie die Schweiz vertreten und Interesse am Aufbau von inklusiven und fairen Datenräumen zeigen. Dazu soll ein internationales Netzwerk aufgebaut werden, welches lokale, regionale und nationale Datenräume über die Grenzen der einzelnen Länder und Anwendungsbereiche hinweg miteinander verbindet. Im Rahmen dieses Netzwerkes sollen Ressourcen geteilt, technische Standards für den Datenaustausch definiert und die globale Verbreitung der digitalen Selbstbestimmung gefördert werden.

Technische Infrastrukturen für den Datenaustausch

Bereitstellung, Austausch und Nutzung von Daten kann mit Hilfe verschiedenster Technologien bewerkstelligt werden. Die Auswahl dieser Technologien richtet sich nach den konkreten Anforderungen der Datennutzer resp. der Use Cases für welche die Daten eingesetzt werden. Dabei ist insbesondere auch

---

[12] Die am 19.2.2020 von der EU Kommission publizierte Europäische Datenstrategie postuliert den Aufbau eines europäischen Datenraumes wie folgt: “Ziel ist die Schaffung eines einheitlichen europäischen Datenraums, eines echten Binnenmarkts für Daten, der für Daten aus aller Welt offensteht, in dem sowohl personenbezogene als auch nicht-personenbezogene Daten, darunter auch sensible Geschäftsdaten, sicher sind und in dem Unternehmen auch leicht Zugang zu einer nahezu unbegrenzten Menge hochwertiger industrieller Daten erhalten.” (siehe S. 6 der Datenstrategie).

[13] Ebenda S. 25 ff.

auf die Datenqualität, eine angemessene Dokumentation (Metadaten[14]) sowie den Schutz vor unbefugtem Zugriff und Manipulation der Daten zu achten.

Eine spezielle technische Herausforderung liegt in der Kontrolle der Daten durch die beteiligten Personen. Dies erfordert Instrumente, welche über Existenz und Inhalt der personenbezogenen Daten Auskunft geben, deren Bezug ermöglichen, die Weitergabe und deren Form an Dritte unterstützen oder eine solche unterbinden können. Bis anhin bestehen personenbezogene Dateninfrastrukturen erst in Ansätzen oder auf experimenteller Basis. Beispiele sind die in der Schweiz entwickelte Plattformen der Daten-Genossenschaft «Midata.coop»[15], die Mobilitäts-App «SmartWay» der SBB[16] oder das Personal Information Management System «Bitsabout.me»[17].

Herausforderungen und Risiken

Die fehlende Akzeptanz neuer Datenräume im Markt könnte eine grosse Herausforderung darstellen. Ökosysteme sind nur dann erfolgreich, wenn sie dank ihrer Vertrauenswürdigkeit gute Verbreitung finden und benutzerfreundlich sind. Mit der Lancierung eines Datenraumes sind neue Infrastrukturen für den Datenaustausch aufzubauen (z.B. über breite Trägerschaften). In jedem Fall ist mit einer längeren Phase der experimentellen und pilotmässigen Nutzung dieser Infrastrukturen zu rechnen, in welchen die beteiligten Akteure Erfahrungen in der datenbezogenen Zusammenarbeit mit anderen Unternehmen – oft Konkurrenten – und Verwaltungen sammeln können.

Einzelne Datensätze können für sich genommen – je nachdem was sie beinhalten – harmlos sein und in der Regel gut geschützt werden. Erst die Verknüpfung und Aggregation grosser Datenmengen schaffen eine Machtkonzentration bei den Betreibern der Dateninfrastrukturen. Die Herausforderung besteht darin, Kontrolle zu gewährleisten: Sowohl die Kontrolle einer einzelnen betroffenen Person über ihre individuellen Daten als auch die Kontrolle mehrerer Personen über die Nutzung von gemeinsam generierten Daten.

Die Vertrauenswürdigkeit eines Datenaustausches basiert auf Regeln, deren Einhaltung überwacht werden müssen. Verstösse sollen angemessen geahndet werden. Das Risiko besteht, dass Regelverstösse nicht entdeckt oder nicht geahndet werden und dadurch das Vertrauen in die Datenkooperation bei den beteiligten Akteuren schwindet. Dieses muss im Rahmen der Gouvernanz der Datenräume minimiert werden.

Der Betrieb von technischen Infrastrukturen für den Datenaustausch birgt weitere Risiken, welche von Manipulationen bis zu unzureichenden finanziellen Mitteln reichen. Insbesondere kann der Betreiber unterschiedliche Daten zu einer Person miteinander verknüpfen und dadurch unerlaubterweise Persönlichkeitsprofile erstellen. Solchen Risiken muss im Rahmen von Leistungsvereinbarungen mit den Betreibern und mit robusten Geschäftsmodellen begegnet werden.

Technologisch ergeben sich zahlreiche Herausforderungen aus der Tatsache, dass zuweilen sehr sensitive Daten über die Dateninfrastrukturen bereitgestellt werden, was letztere zu attraktiven Angriffszielen für Cyberkriminelle machen könnte. Umfassende technische und organisatorische Massnahmen zum Schutz der Daten helfen, diese Risiken zu minimieren. Nur schon aus diesem Grund sind Datenräume dezentral bzw. netzwerkförmig aufzubauen; zentrale «Superinfrastrukturen» sind zu vermeiden.

---

[14] Siehe dazu auch das Projekt Nationale Datenbewirtschaftung (https://www.bfs.admin.ch/bfs/de/home/nadb/nadb.html).
[15] https://www.midata.coop/en/home/
[16] https://www.sbb.ch/en/timetable/mobile-apps/smartway.html
[17] https://bitsabout.me/de/

5. Anhänge

Anhang 1: User-Story im Bereich Mobilität

Anwendungsbeispiel Ist-Zustand

Frau Müller möchte von Zürich-Witikon in die Lenzerheide reisen, um mit ihrem Bekannten, Herrn Schuhmacher, ein Wochenende in den Bergen zu verbringen. Sie plant ihre Reise mit Google Maps. Da Herr Schuhmacher in Chur wohnt, beschliesst Frau Müller mit dem ÖV nach Chur zu reisen. Danach könnten sie mit dem Postauto weiterfahren, was aufgrund einer langen Wartezeit und der Distanz von der Postauto-Haltestelle zum Chalet in der Lenzerheide aber ungünstig ist. Zudem ist das Postauto an schönen Wochenenden regelmässig überfüllt. Die beiden beschliessen, mit dem Auto von Herrn Schuhmacher von Chur bis in die Lenzerheide zu fahren.

Frau Müller nimmt die von Google Maps vorgeschlagene Bus- und Zugverbindung von Witikon ZH nach Chur und löst die Tickets an den jeweiligen Automaten. Im Zug und am Bahnhof nutzt Frau Müller das SBB-WiFi. Die SBB erhebt punktuell ihre **Lokalisationsdaten** und schaltet **personalisierte Werbung**. Frau Müller ist sich dessen nicht bewusst, da sie die Nutzungsvereinbarung ungelesen akzeptiert hat. Durch ihr weiteres Surfverhalten u.a. via Google Search werden ihre **Präferenzen** in einen **Datenpool eingelesen**. Darauf basierend können Dritte Werbung an Frau Müller ausspielen, wenn sie deren Seite besucht.

Um von Chur mit dem Auto in die Lenzerheide zu kommen, nutzt Herr Schuhmacher das Navigationssystem von Google Maps. Dieses trackt das Mobile von Herrn Schuhmacher im Hintergrund, und die **Positionsdaten** werden ohne sein Wissen an Verkehrsdienstleister **verkauft**. Frau Müller und Herr Schuhmacher haben beide Google Maps auf ihrem Mobile installiert. Die App erhebt ihren Standort via Lokalisierung, auch wenn sie nicht gebraucht wird. Beiden ist dies nicht bewusst und weil sie das Tracking nicht aktiv abgeschaltet haben, werden ihre **Lokalisationsdaten kontinuierlich abgespeichert**. Google speichert so die gesamte Reise von Frau Müller von Witikon ZH über Chur bis in die Lenzerheide und verwendet die erhobenen **Daten für kommerzielle Zwecke**.

Anwendungsbeispiel Digitale Selbstbestimmung

Einige Jahre nach ihrem letzten Aufenthalt mit Herrn Schuhmacher in der Lenzerheide plant Frau Müller erneut ein gemeinsames Wochenende. Mit einer Mobilitäts-App kann sie die **gesamte Reise auf einer einzigen Oberfläche planen:** sei es mit Bus, Zug, Postauto – oder auch Taxi, Velo und Carsharing.

Während der Planung meldet die App eine **Optimierungsmöglichkeit:** Zwei Personen würden für den Reiseabschnitt Chur–Lenzerheide ein Mobility-Car teilen. Frau Müller beschliesst mit Bus, Zug und Carsharing zu reisen und bestätigt die Reise für sich und Herrn Schuhmacher. Dadurch werden alle Reservierungen getätigt, die Bezahlung erfolgt in der App nach Finalisierung der Reise. Frau Müller gibt in der App an, dass die involvierten Verkehrsunternehmen und der Tourismusort Lenzerheide von ihrer Reise erfahren sollen, allerdings ohne Namensnennung oder Verknüpfungen zu sonstigen Präferenzen.

Am Morgen der Reise erhält Frau Müller eine gute Nachricht: Dank Online-Ticketbuchungen erkannten die Verkehrsbetriebe Zürich (VBZ), dass viele Leute in ihrer Nachbarschaft den Bus 31 nehmen. Die VBZ reagierte auf diese Nachfrage, passte die Route an und plante einen zusätzlichen Stopp ein.

Am Ende ihrer Reise sehen Frau Müller und Herr Schuhmacher auf ihren Apps, wie lange sie mit welchen Transportmitteln gereist sind. Die Informationen sind **verständlich und transparent** aufbereitet und umfassen die Kosten sowie den CO_2-Ausstoss ihrer Transportmittel. Sie **kontrollieren,** ob diese Daten via einem Mobilitätsdatenraum weiteren Dienstleistungsanbietern zugänglich sind.

Durch Auswertung dieser Daten gibt es Möglichkeiten zu Optimierungen:

- Neue Dienstleistungen (z.B. flexible ÖV-Routen, Carsharing in Echtzeit)
- Verbesserte Störungsinformationen sowie bessere Planung für Infrastrukturinvestitionen
- Auslastung von ÖV-Netz und Strasse kann besser gesteuert werden – dadurch ergeben sich Zeit- und Effizienzgewinne sowie Energieeinsparungen (z.B. durch Carsharing-Möglichkeiten)
- Preissenkungen durch verbesserte Effizienz

Dienstleister verpflichten sich mit der Teilnahme am Mobilitätsdatenraum dazu, einen Schutzstandard und eine explizite Kontrollbefugnis für individuelle Daten einzuhalten. Frau Müller und Herr Schuhmacher haben daher Gewissheit, dass ihre **Daten nie unkontrolliert an Dritte** weitergegeben werden.

Nächste Schritte und mögliche sektorspezifische Massnahmen:

- Erarbeitung möglicher Gouvernanz-Modelle für Datenräume im Bereich Mobilität
- Definition der nötigen rechtlichen, technischen und wirtschaftlichen Bedingungen für eine Umsetzung von Datenräumen im Bereich Mobilität.

Anhang 2: Fiktive User-Story im Bereich Bildung

Anwendungsbeispiel Ist-Zustand

Ida besucht die 6. Klasse einer Volksschule in Basel. Ihre Eltern erhalten von der Schule die Aufforderung, sich bei «G Suite for Education» zu registrieren, der **Datenweitergabe** an Google durch die Schule einzuwilligen und deren Nutzungsbedingungen zu akzeptieren. Dies umfasst auch die **Analyse der Nutzungsdaten** und sei für einen reibungslosen Unterricht notwendig. Zudem erhält Ida ein Tablet mit Android-Betriebssystem zur Nutzung in der Schule, bei dem die Eltern die **Einwilligung** zur **Nutzung** des **Betriebssystems** und zur **Verarbeitung der Nutzungsdaten** durch Google geben müssen. Schliesslich bittet die Schule Idas Eltern um die Einwilligung zur Datenweitergabe der Nutzungsdaten an eine **adaptive Lernplattform**. Die Lernplattform bietet die Möglichkeit, Lernprozesse teilweise zu automatisieren. Die Plattform generiert Leistungsdaten zur Erstellung weiterer Aufgaben.

Ida und ihre Eltern können nicht abschätzen, was ihre Zustimmung für die Nutzung der Daten bedeutet. Sie stimmen dennoch zu, da alle anderen Eltern der Klasse dies auch getan haben und sie glauben, andernfalls den Lernfortschritt ihrer Tochter zu behindern. Allerdings bleibt ein gewisses **Misstrauen** bestehen, und das Thema wird im Elternbeirat intensiv diskutiert.

Ida muss ihre Hausaufgaben in Deutsch meist über «G Suite for Education» erstellen und mit dem Lehrer auf der Plattform teilen. Sie leidet zwar nicht an Legasthenie, hat aber Mühe mit der Rechtschreibung. Diese wird von Google Docs automatisch korrigiert. Google speichert dabei ständig die **Fehlermuster** während der Eingabe, ohne dass Ida oder ihre Eltern dies merken. Im nächsten Geschichtsunterricht sollen die Schulkinder auf dem Tablet zu politischen Strukturen im Griechenland der Antike recherchieren und eine Gruppenaufgabe bearbeiten. Bei Ida führt die Google-Suche auf Grund ihres **Profils** zu Texten mit «einfacher Sprache». Sie braucht länger, um die richtigen Informationen zu finden und die Mitschülerinnen sind unzufrieden mit ihrer Mitarbeit in der Gruppe. Ida fühlt sich unwohl und ihre schulischen Leistungen leiden darunter.

Die adaptive **Lernplattform kauft Nutzungsdaten** bei Google ein, um ein «verbessertes Angebot» zu erstellen. Die Daten sind pseudonymisiert, aber lassen sich auf Basis der von der Lernplattform erhobenen Nutzerdaten wieder zuordnen. Ida erhält **automatisch einfachere Aufgaben** als viele ihrer Mitschülerinnen. Der von der Plattform erhobene Lernfortschritt von Ida bleibt hinter dem Klassendurchschnitt zurück. Im Ergebnisanalysetool erhält die Lehrerin so einen falschen Eindruck von Idas Leistungsfähigkeit. Dies wird sich auf ihren weiteren **Bildungsfortschritt negativ auswirken**.

Anwendungsbeispiel Digitale Selbstbestimmung

Ida besucht die Klasse 2a einer Sekundarschule in Basel. Sie kann mit dem Schul-Tablet auf unterschiedliche Inhalte zugreifen. Die Identität, die Ida für den Zugang zu ihrem Tabletprofil verwendet, ist in der Föderation der Identitätsdienste im Bildungsraum Schweiz – Edulog – föderiert. Die **Personendaten** von Ida sind zwar für Edulog **einsehbar,** für den Bereitsteller der unterschiedlichen Dienstleistungen bestehen **aber Einschränkungen**. Mit dem Tablet und ihrem Edulog-Pseudonym kann sich Ida auf den Lernplattformen einloggen, die ihr von der Schule zur Verfügung gestellt werden.

Google konnten bessere Bedingungen abgerungen werden und der Konzern **speichert** die **Nutzungsdaten nicht mehr standardmässig**. Die Schreibfehler von Ida haben daher keinen Einfluss auf die Vorschläge und den Lernerfolg in anderen Bereichen. Idas Eltern können über ein Portal alle bei den Dienstanbietern gespeicherten Daten einsehen und Nutzungsrechte vergeben. So können sie entscheiden, ob alle ihre **Daten in pseudonymisierter Form** von kantonalen Behörden oder etwa für Forschungszwecke **genutzt werden dürfen** oder der Zugriff nur eingeschränkt möglich ist. In der Schule wird der Umgang mit den Plattformen diskutiert und aufgezeigt, wie die Schüler Kontrolle über ihre

Daten ausüben können. Dies alles stärkt das Bewusstsein bei Ida und ihren Eltern für den Wert der erhobenen Daten. Die schweizerische Bildungsforschung erhält durch den erweiterten Zugang zu Daten neuen Schwung und arbeitet eng mit **lokalen Start-ups und Unternehmen** bei der Entwicklung neuer Lösungen zusammen. Der Kanton kann auf **Grundlage der Daten besser entscheiden**, welche Lehrmittel beschafft werden sollen. Lehrerinnen, Lehrer sowie Schülerinnen und Schüler profitieren von einem **erweiterten Angebot** an digitalen Lehrmitteln, wodurch der Unterricht adaptiver wird. Ida konnte ihren Lernerfolg und ihre persönliche Zufriedenheit in Mathe und Chemie dank neuen Lehrmitteln wesentlich verbessern.

Nächste Schritte und Massnahmen:

Aufbauend auf dem Bericht «Daten in der Bildung – Daten für die Bildung, Grundlagen und Ansätze zur Entwicklung einer Datennutzungspolitik für den Bildungsraum Schweiz» (siehe https://www.educa.ch/sites/default/files/uploads/2019/08/daten_in_der_bildung_high.pdf) wird eine Programmstruktur für die Elemente einer zukünftigen Daten-Gouvernanz des Bildungswesens erstellt.

Anhang 3: User-Story im Bereich Energie

Anwendungsbeispiel Ist-Zustand

Herr Müller möchte **Zugriff** auf seine **Stromverbrauchs-** und **produktionsdaten,** diese analysieren und Massnahmen ergreifen, um den Stromverbrauch zu reduzieren und seine **Stromnutzung** zu **optimieren**. Er hat kürzlich eine Photovoltaik-Anlage (PV-Anlage) auf seinem Dach installiert und ist dabei ein Elektromobil zu erwerben. Dank der Energiestrategie 2050 hat er ein elektronisches Strommessgerät (Smart Meter) vom Verteilnetzbetreiber (VNB) erhalten, das **digitale Daten** aufnimmt. Bisher erreichen ihn alle drei Monate Rechnungen mit der Aufforderung für Akonto-Zahlungen. Nun möchte er mehr erfahren.

Trotz Bemühungen erhält Herr Müller **keinen Zugriff** auf seine Daten. Sein Energieversorgungsunternehmen (EVU) verweist ihn jeweils an verschiedene Stellen im Unternehmen. Er schaut sich im Energiedienstleistungsmarkt um und wendet sich an einen unabhängigen Dienstleister. Diesen berechtigt er seine Daten zu nutzen und füllt händisch ein Formular aus. Der Dienstleister gelangt an das EVU. Dieses äussert Vorbehalte, zweifelt die Berechtigung an und überprüft diese, was Wochen dauert. Schliesslich werden dem Dienstleister per E-Mail einige **Daten** in einem **schlecht handhabbaren Format** zugesendet. Auf Nachfrage nach einem gängigen, **maschinenlesbaren Format** in kürzeren Fristen oder einem Anwendungsschittstellen-Zugang **(API-Zugang)**, erhält er die Nachricht, dass dies nicht möglich ist und zusätzliche Kosten nach sich zieht. Ebenso ist **keine Schnittstelle** vorhanden, über die Daten zeitnah übermittelt werden könnten.

Der Dienstleister greift auf die durch die Energiestrategie 2050 regulatorisch geforderte, offene **Endkundenschnittstelle** des Smart Meters zu. Diese ist jedoch **deaktiviert**. Auf Nachfrage ist eine Aktivierung derzeit technisch nicht möglich. Die Pflicht zur Aktivierung wird in Frage gestellt sowie werden Kosten indiziert. Schliesslich entscheidet sich Herr Müller für ein **separates Messgerät**, die Installationskosten trägt er selbst. Die nun gemessenen Daten landen in einer **Cloud** des Dienstleisters **im Ausland**. Herr Müller weiss nicht genau, was mit seinen Daten passiert. Er **verliert** das **Vertrauen** in den Dienstleister und deinstalliert das Messgerät wieder für zusätzliche Kosten. Er erhält weiterhin keine Daten, zahlt noch immer Akonto-Rechnungen und hat das Interesse an Optimierungen verloren.

Anwendungsbeispiel Digitale Selbstbestimmung

Herr Müller möchte seine Stromverbrauchs- und produktionsdaten analysieren und die Stromnutzung optimieren. Er hat ein Smart Meter vom VNB erhalten. Sein lokales EVU bietet ihm keine für ihn geeigneten Dienstleistung an. Er sucht am Markt und wird bei einem Dienstleister fündig.

Herr Müller nutzt die Möglichkeiten der nationalen **Energiedateninfrastruktur** und der digitalen Selbstbestimmung. Er loggt sich auf der Website der nationalen Energiedateninfrastruktur mit seiner elektronischen Identität ein. Hier sieht er **transparent, welche Daten über ihn verfügbar sind und wer diese zu welchem Zweck verwendet**: Rechnungsadresse, Granularität seiner Daten/Verbrauchs- und Produktionsmessungen, Teilnehmer des Strommarktes, die diese **in verschiedenen Formen** (aggregiert, pseudonymisiert, personenspezifisch) zu **bestimmten Zwecken**, z.B. Netzabrechnung, Energieabrechnung, etc., nutzen. Einiges davon kann Herr Müller **nicht ändern**; dazu gehören Daten im Zusammenhang mit seiner Stromlieferung sowie **systemnotwendige Daten**. Er entschliesst sich, den Dienstleister per Mausklick freizuschalten. Der Dienstleister hat sich **akkreditieren** lassen und ist **berechtigt** auf die

API der Energiedateninfrastruktur zuzugreifen. Der Dienstleister erhält nun die **benötigten Daten** für die Dienstleistung über die API. Diese werden dezentral aus bei dem lokalen VNB gespeicherten Daten vollständig automatisiert und in kurzer Frist geroutet. Herr Müller erhält bereits am nächsten Tag Auswertungen und Vorschläge zur Optimierung seines Stromverbrauchs.

Ein zweiter Dienstleister offeriert Herr Müller die **Optimierung** des **Strombezugs** seines neu erworbenen **Elektromobils** mittels der bestehenden **PV-Anlage**. Wieder berechtigt er diesen Dienstleister zur Nutzung seiner Daten über eine standardisierte API. Die erworbene digitale Dienstleistung ist auf den nächsten Tag aktiv und der Dienstleister erhält über die Energiedateninfrastruktur alle relevanten Daten über die installierte PV-Produktion wie Leistung, Ausrichtung, Produktions- und Einspeisewerte.

Wenig später entscheidet sich Herr Müller, den ersten Dienstleister nicht mehr zu berechtigen und vollständig auf den zweiten zu setzen. Er **deaktiviert** den **Zugang** des ersten Dienstleisters, worauf dessen Berechtigung für den Zugriff entfällt. Der erste Dienstleister erhält eine **Aufforderung**, die bereits **vorhandenen Daten** zu **löschen**. Ein etwaiger Verstoss wird mit Ausschluss aus dem Ökosystem und einer Busse geahndet.

Herr Müller nimmt an einer Hochschul-Veranstaltung teil und informiert sich über den Klimawandel. Dabei wird über ein Forschungsprojekt berichtet, das auf Basis der Stromverbrauchsdaten den Klimaabdruck der Schweiz berechnet. Er möchte daran partizipieren und dem Forschungsinstitut ihre **Daten zur Verfügung stellen**. Per Mausklick erteilt er der Hochschule die Berechtigung zur Nutzung seiner **pseudonymisierten** Daten. Das Forschungsinstitut ist nun in der Lage, die Daten für statistische Auswertungen im Rahmen des Forschungsprojekts zu nutzen.