Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of the Environment, Transport, Energy and Communications DETEC

Federal Department of Foreign Affairs FDFA

Bern, 30.03.2022

Creating trustworthy data spaces based on digital self-determination

Report from the DETEC and FDFA to the Federal Council on 30 March 2022

Inhaltsverzeichnis

Executive summary

Digitalisation poses a number of challenges, particularly regarding how to build a sustainable data-driven society. Making better use of data can help many parts of society and the economy better meet their needs. Better use of data also promotes innovation and enables the efficient, sustainable use of resources. Data can yield advances in medicine[1] such as new forms of diagnostics, and advances in agriculture[2] such as new insights into fertiliser patterns. At the same time, however, many people fear that this increased use of data means losing control over their personal data.

Our central question is: how can we more fully harness the potential that data holds for society and the economy? There are three main tendencies that illustrate why this potential has not yet been exhausted. Firstly, data is becoming increasingly concentrated in the hands of a few global players – a development that is impacting more and more sectors. While these players can collect and analyse data for the purposes of innovation and increasing their own efficiency, they do not have any incentives to share this data with others. Secondly, many private and public service providers cannot or do not wish to harness the potential of the data they collect. This may be because they lack the expertise or resources, they fear weakening their current position, or they face administrative, technical or legal barriers. Thirdly, there is mistrust among a growing segment of the population when it comes to the use of data. Reasons include fear of being manipulated, fear of losing one's privacy or having it abused, and the lack of incentives for data sharing (see Chapter 2).

Unless countermeasures are taken, these developments are likely to accelerate and impact more and more segments of our society. In a sustainable data-driven society, people should not have to choose between protecting and maintaining control over their data and enjoying the advantages of data sharing. Instead, both options should be made possible by applying a model of digital self-determination: the idea that individuals, companies and society as a whole should be able to determine what actions they take in our digital ecosystem. This includes the ability of users to determine the relevance and value of information that is important to them, to have access to and control over said data, and to determine how it is used (see Chapter 3).

To ensure that users stay in control while promoting data sharing and usage, there is a need to establish *trustworthy data spaces*. This is a special category of data space characterised by the ability of participants to maintain the necessary level of control over their data while voluntarily sharing it in the space for the purpose of social and economic value creation. There are certain fundamental requirements that need to be in place for trustworthy data spaces of this kind to be established. This report proposes five basic principles: transparency, control, fairness, responsibility and efficiency. These five basic principles, along with their corresponding indicators, form the core of the response to the Federal Council's question of which technical, legal, economic and societal requirements are needed in order to facilitate the creation of trustworthy data spaces (see Chapter 4).

The development of data spaces is already underway in Switzerland today. This report will explore concrete examples of data space projects in the mobility, energy, finance, healthcare and education sectors that are on the path towards digital self-determination. Details will be given regarding how these projects qualify as trustworthy data spaces (see Chapter 5).

[1] *Federal Council (2019)*, "Health Policy Strategy 2020-2030", p. 12.
[2] See the Agroscope *Smart Farming Project* <https://www.agroscope.admin.ch/agroscope/en/home/topics/economics-technology/smart-farming.html> (accessed on 03.02.2022), e.g., "Site-Specific N-Fertilisation".

Data frequently flows across national borders. Different views on how to regulate this flow have emerged across the world over the past several years. This has led to increased regulatory fragmentation, which has created hurdles for the free transnational flow of data. If we want to harness the enormous potential of international data flows, we need to create data spaces that are internationally compatible – not only from a technical perspective, but also in terms of how they are organised and which standards they apply. Interoperability is key. For Switzerland, this will require participating in international and European committees to help establish common standards when it comes to digital self-determination. Over the longer term, Switzerland should aim to create a secure international legal framework and to counteract regulatory fragmentation. This is important for Switzerland as a mid-sized, highly networked economy and can help secure the country's access to both international markets and the EU's single market. Taking a digital self-determination approach can open up new opportunities in this context (see Chapter 6).

Although there are efforts underway in diverse areas to define up-to-date cross-sector parameters for data spaces, these efforts must be intensified in order to promote data usage and counteract certain tendencies (such as the concentration of data in the hands of a few players) while also creating transparency, trust and additional control for users. The data spaces being established now will lead the way for how we as a society make use of these spaces and how we handle the large-scale exchange of data in the future. Switzerland must also work to create the right parameters here. In a first step, this report suggests the following measures for promoting trustworthy data spaces based on the concept of digital self-determination (see Chapter 7):

1. **Code of conduct:** Data spaces are in their infancy in many sectors but are increasingly on the rise. Switzerland should draft a voluntary code of conduct to guide the development of trustworthy data spaces. The code of conduct should be based on the basic principles of this report. It should be formulated by the national Digital Self-Determination Network in a multi-stakeholder process and be understood as a coordinated approach to self-regulation.
2. **Swiss data hub and interoperability:** Data hubs for businesses, research institutes, associations and country-specific public authorities are increasingly appearing in Europe. These hubs do not include technical infrastructure, but rather support the development of data spaces by acting as central points of contact for related questions. In line with ongoing efforts, there are plans to review whether a similar data hub should be established in Switzerland. There is also a need to develop approaches to ensuring interoperability between national and international data spaces; here the work of the national data management programme (NaDB) should be taken into account.
3. **International measures:** Switzerland needs to advocate internationally for trustworthy data spaces based on digital self-determination and interoperability in order to harness the potential of transnational data exchange. To this end, Switzerland is identifying suitable partners from all stakeholder groups and supporting and developing relevant processes. Wherever possible, Switzerland should consider International Geneva as a venue for these discussions. The international Digital Self-Determination Network should serve as a platform for working together with partners to draft international guidelines for data space operators. These guidelines should reflect the Swiss code of conduct as far as possible.

It is possible that these initial measures will result in further steps that may require adjustments, particularly in sectoral legislation.

1 Mandate

This report fulfils the mandate assigned to DETEC and the FDFA by the Federal Council's decree on the Digital Switzerland Strategy from 11 September 2020:

> *DETEC (OFCOM) and the FDFA (DIL) were asked to work together with the FDHA (FSO) and the FCh to produce a report for the Federal Council by the end of 2021 on the technical, legal, economic and societal parameters necessary for creating trustworthy data spaces that respect the principles of digital self-determination. The report should cover national and international perspectives and illustrate potential areas for action while taking relevant work from other departments and federal offices into consideration.*

This report aims to use experience from the mobility, energy, healthcare, education and finance sectors to **establish common principles** that should serve as a foundation for trustworthy data spaces both domestically and internationally. We will also cover issues surrounding the necessary **infrastructure** and **governance** for data spaces. Taken together with the report on digital public services to be published by DETEC (OFCOM) in mid-2022, this report also covers aspects from postulate 19.3574, particularly regarding healthcare and education.

This report does not yet examine in detail which legal requirements must be complied with or redesigned when the state takes activities in favour of the development of trustworthy data spaces. In a first step, the concrete proposed measures remain within the framework of applicable law. However, it is possible that new, in particular sectoral legislation, will have to be developed at a later stage.

1.1 The principles of digital self-determination

The groundwork for Switzerland's vision of digital self-determination was laid by a cooperation between the FDFA (DIL), DETEC (OFCOM), the Swiss Academy of Engineering Sciences (SATW) and the Swiss Data Alliance (SDA). This working group produced a discussion paper that defines the concept of digital self-determination and illustrates some initial ideas for how to put it into practice.[3] Under the concept of digital self-determination, new or newly balanced approaches are gathered that are based on and build upon recognised fundamental rights as well as on the multifaceted interests in the use of data.

The Digital Switzerland Strategy from 11 September 2020 marked the first time that the concepts of digital self-determination and trustworthy data spaces were introduced on the federal level in Switzerland. The Federal Council outlined the following goals in this strategy:

> *Switzerland should have trustworthy data spaces in which residents can exercise control over their own data. [...] There should be clearly defined relationships between data producers, data users and affected parties. This framework should allow all actors to securely and voluntarily consent to sharing existing data sets within digital ecosystems beyond their originally intended purposes. These data spaces foster innovation and new business models, both within and across different sectors.*[4]

[3] *OFCOM, FDFA, SDA and SATW (2020)*, "Diskussionspapier Digitale Selbstbestimmung".
[4] *Federal Council (2020b)*, "Digital Switzerland Strategy", Goal 7.5.

There are references to the international aspects of digital self-determination in the Foreign Policy Strategy 2020-23 and the Digital Foreign Policy Strategy 2021-24.[5]

In May 2021, the **national Digital Self-Determination Network** was founded by DETEC (OFCOM), the FDFA (DIL), the SATW and the SDA.[6] This network brings together experts from various segments of the private sector, public administration, academia and civil society and plays a central role in making digital self-determination a reality in Switzerland. The network is developing practical approaches to setting up trustworthy data spaces and provides a platform for different actors and sectors to exchange ideas. This promotes interdisciplinary discourse and the development of multifaceted perspectives on the topic.

1.2 Relationship with other reports

Developments in data policy have increasingly become an object of focus on the federal, cantonal and local level over the past several years. The present report can be thought of as part of a series of reports that deal with data policy issues (see overview in Appendix 1). In the second half of 2022, DETEC (OFCOM) is scheduled to publish a report on digital public services that focuses on the role of the public authorities in digital and data policy issues. Additional relevant publications include the IPI report on access to non-personal data in private industry (March 2021)[7] and reports recently published by the SIF[8] and the SFOE[9]. A legal foundation for creating national data infrastructure for energy has already been submitted to Parliament in the dispatch on the consolidation bill for secure renewable energy supply.[10] The FOT is currently working on a dispatch on a federal law on mobility data infrastructure.[11] Furthermore, the Swiss federal strategy for geographical information was passed in 2020.[12]

This report attempts to create an overview of these various efforts and to work out common principles for creating and operating trustworthy data spaces – principles that increase individual responsibility and facilitate data usage, thereby making an active contribution to domestic and international data policy.

2 Background

Both the economy and society have been fundamentally transformed in recent years by digitalisation and the power of data. The volume and diversity of data, as well as the speed of data processing, have all undergone rapid increases and opened up new possibilities. A study commissioned by IPI put the growth rate of the Swiss data market at 8% between 2017 and 2018, with the EU average coming in at 10%.[13] For this reason, it is hardly surprising that an expert report on the future of data processing and security declared data to be the "basic unit of the [...] digital revolution".[14]

[5] *Federal Council (2020a)*, "Foreign Policy Strategy 2020-23", p. 19; *Federal Council (2020c)*, "Digital Foreign Policy Strategy 2021-24", p. 14.
[6] See <https://digitale-selbstbestimmung.swiss/home/> (accessed on 04.02.2022).
[7] *IPI (2021)*, "Zugang zu Sachdaten in der Privatwirtschaft".
[8] *SIF (2022)*, "Digital Finance: Handlungsfelder 2022+".
[9] *SFOE (2021)*, "Datahub Schweiz: Kern zukünftiger Dateninfrastruktur digitalisierter Strom- und Gasmärkte".
[10] *Federal Council (2021)*, "Botschaft zum Bundesgesetz über eine sichere Stromversorgung mit erneuerbaren Energien vom 18. Juni 2021", Federal Gazette 2021, 1666 et seq.
[11] *FOT (2022)*, "Erläuternde Bericht zum Bundesgesetz über die Mobilitätsdateninfrastruktur (MODIG)".
[12] *Federal Council and DPPE*, "Strategie Geoinformation Schweiz".
[13] *IDC (2020)*, "Analysis of the Data Market: 2017-2018, 2025 for Switzerland and other EU28 Member States"; *IPI (2021)*, "Zugang zu Sachdaten in der Privatwirtschaft", p. 12.
[14] *Gadient B. M. et al. (2018)*, "Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit", p. 24.

This report refers notably to data as digital data. Data constitutes *values that can be transferred, processed or read in digital form* (→ data). Both the proliferation of data and the improved possibilities for analysing and using it form the foundation for innovation and progress today. Data provides a knowledge base for analysing and improving existing situations and processes and for developing new approaches. Data can provide information about the preferences of customers, the state of materials, the availability of resources or the effectiveness of measures, to name a few examples. Data opens up new possibilities for diagnosing and preventing disease[15], for improving our understanding of fertilisation and feeding patterns[16] or for offering more efficient services to organisations and individuals.

Data is not valuable *in and of itself*. It only becomes valuable when a specific purpose is identified and data is used to that end. This makes data part of the digital value chain (→ digital value chain): only by connecting different *data* together can we generate *information* (→ information). Then, by analysing this information and data with a specific purpose in mind, we generate *knowledge* (→ knowledge) that is understandable and can guide our actions (see Figure 1).[17]

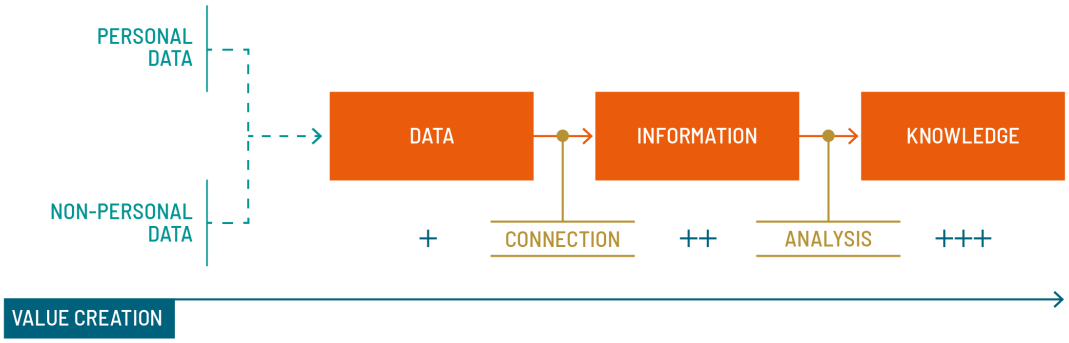

Figure 1: The digital value chain[18]

Data also has *specific characteristics* that hold enormous potential for social and economic applications. Some key characteristics of data include:

- Data is **non-rival**, meaning that the same data can be used, exchanged, connected and reused by different actors and even for different purposes without the data losing its value.
- Data is also **not automatically excludable**: in order to prevent third parties from viewing or using data, there need to be measures taken on a technical, legal or organisational level. This can be done for a variety of reasons – for instance, for regulatory reasons such as data protection or for the business reason of competitive advantage. Without measures of this kind, data is principally accessible.
- Data is **easy to reproduce and process**: data is easy to copy and when put into open formats and read by computers, data is also easily processed and shared.

[15] *Federal Council (2019)*, "Health Policy Strategy 2020-2030", p. 12.
[16] See Agroscope *Smart Farming Project* <https://www.agroscope.admin.ch/agroscope/en/home/topics/economics-technology/smart-farming.html> (accessed on 03.02.2022), e.g., "Milk and Meat Production Technologies" or "Site-Specific N-Fertilisation".
[17] *Swiss Economics (2021)*, "Vertrauenswürdige Digitale Datenräume: Schlussbericht Konzeptualisierung und Anforderungen", p. 7.
[18] Graphic based on *Swiss Economics (2021)*, "Vertrauenswürdige Digitale Datenräume: Schlussbericht Konzeptualisierung und Anforderungen", p. 8.

- Data as a **by-product**: data is sometimes generated as a by-product of another economic or social activity (e.g., using a device, concluding a business transaction, etc.). This means that unlike other prerequisites for innovation, data can sometimes be generated without costly investments or expensive research and development efforts.[19]

These properties of data make it suitable for collective use (→ collective data use), thereby making it available as a knowledge and innovation base to a broad spectrum of players with different business models. Currently, however, data is primarily used by individual actors. Many of the most successful internet companies are based on a proprietary data model, i.e., the data is managed by a private platform and used for commercial purposes. The following section explores the phenomenon of these platforms as the currently dominant business model of digitalisation.

2.1 Platforms: the dominant digitalisation business model of today

Platform-based business models have laid the foundation for a new interplay between business and societal actors. They massively reduce transaction costs for their users by standardising data (→ standardisation) and by easily and quickly connecting users with each other (e.g., *Twitter*). Platforms also act as intermediaries (→ intermediaries), providing the infrastructure for third-party providers to offer their own services. These providers use the platform to easily interact with customers and conduct transactions (e.g., marketplaces such as *eBay* or *booking.com*). They also give intermediaries the possibility to directly offer products or services to customers themselves (e.g., *Amazon*). It is often the case that several of these relationships are combined on one platform (known as → multi-sided markets). One example of a multi-sided market is *Facebook*, which connects users with each other while also offering advertisers the possibility of presenting these users with ads. There are a variety of different platforms that can be categorised according to different criteria (business model, type of interaction, governance → governance, size, etc.).[20]

In general, companies have an interest in generating market-related data, for instance regarding customer behaviour, preferences, locations, browsing times and optimal price structures. Due to their **status as intermediaries**, platform-based businesses enjoy particularly easy access to data of this kind. Platform companies have geared themselves towards knowing the needs of their users to the best extent possible by using data generated on the platform itself. This data allows companies to offer personally tailored services (efficiency gains, easier and more convenient decisions, etc.). Because of the added value that this creates, users are often prepared to use these platforms' services even if they are only partially aware of how their data is being used.

Because of the diverse interactions taking place on platforms, they have access to a considerable amount of data from different sources. This is due in part to strong network effects: the more users who are active on a platform, the more attractive the platform becomes for third-party providers as a place to offer their services or products (→ network effect). This in turn increases the appeal to users, for instance because of cheaper prices or a bigger selection of products. This can also cause rigid customer loyalty, however. Network effects also mean that these platforms generate more data that can be used for new innovations (→ data network effect).[21] This data network effect helps platforms establish

[19] *IPI (2021)*, "Zugang zu Sachdaten in der Privatwirtschaft", p. 13.
[20] *Asadullah A., Faik I. and Kankanhalli A. (2018)*, "Digital Platforms: A Review and Future Directions".
[21] *Collovà P. et al. (2021)*, "Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung", p. 8.

themselves more firmly, either because they can monetise the data they have collected (i.e., by selling it to third parties who need it for their own value chains in areas such as advertising or product development) or because platforms can use the data to develop new products or services.[22] In contrast, third-party providers who enjoy greater reach due to their (paid) access to platform infrastructure do not enjoy direct access to customer needs and customer data.

Unlike other companies that use their own proprietary data, platform businesses achieve above-average efficiency in fusing together data from different sources. The proprietary data generated thanks to network effects constitutes a significant competitive advantage and can lead to companies taking a dominant position that can even extend beyond their original sector and scope. In this way, data-driven platform companies can gain extensive control over the value chain (known as → vertical integration). A commonly cited example is *Amazon*, which has grown from a bookseller into a retail giant and logistics and IT service provider (*Amazon Logistics, Amazon WebServices*).[23] It can be assumed that 'platformisation' will continue to take hold in all areas of our economy and society thanks to the large efficiency gains brought about by data-driven personalisation. This dynamic does not mean that all current platforms will ultimately prevail over the longer term, however. The success of a platform depends on its business model. We can already observe how users change their preferences, and new actors emerge onto the scene (e.g., *TikTok*).

2.2 The untapped potential of data

In the media and retail industries, data-driven platforms have revolutionised data usage by merging different sources of data together. The resulting products and services create immense added economic value for companies and their users. Personalised services also hold great potential for creating improvements in other important areas of society such as mobility, healthcare and education. Data acts as a driver of innovation and efficiency, which are of interest to society as a whole. Data could help counteract the effects of climate change, contain pandemics and create more efficient and needs-oriented public services in the healthcare system and public transport, to name a few examples. A knowledge base that is generated by analysing data can also be of great significance in public administration and the democratic decision-making process, both as a foundation for informed opinion formation and also as a guide for carrying out projects. It therefore follows that harnessing the power of data is an important and interesting matter from an economic, societal and social perspective.

It is often the case, however, that traditional providers in the aforementioned areas – both private and public – cannot or do not wish to tap into the potential offered by data. Furthermore, data users and producers are often not willing to consent to having their data used. They fear that others will gain too much insight into their business models, thereby creating a competitive disadvantage. Data producers also fear losing control over the data that they collect, analyse and reuse. There is insufficient trust in and understanding of the opportunities and advantages offered by exchanging and using data.[24] Other reasons include having an insufficient understanding of the legal situation or facing legal and technical barriers in accessing data (e.g., lack of standardised interfaces → standards, → interfaces and APIs →

[22] *Collovà P. et al. (2021)*, "Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung", p. 8; see also *IPI (2021)*, "Zugang zu Sachdaten in der Privatwirtschaft", p. 14.
[23] *Zhu F. and Liu Q. (2018),* "Competing with Complementors: An Empirical Look at Amazon.com".
[24] See *IPI (2021)*, "Zugang zu Sachdaten in der Privatwirtschaft"; *OECD (2019)*, "Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies"; *European Commission (2016)*, "Study on Data Sharing between Companies"; *European Commission (2018a)*, "Towards a common European Data Space"; *European Commission (2018b)*, "Staff Working Document – Guidance on Sharing Private Sector Data in the European Data Economy".

application programming interface).[25] There may also be a lack of expertise, resources and infrastructure (e.g., for storing and analysing data) for harnessing the potential of data. A recently published report by the European Commission highlighted the fact that data usage is also lagging behind in the public sector. This lag is attributed to technical, organisational and legal barriers as well as a lack of a culture of shared data usage.[26]

Furthermore, according to a study from the Bern University of Applied Sciences, a great deal of relevant data that could be used as a knowledge/information base is increasingly being concentrated in the hands of large international platforms. This is because these companies – due to network effects, company size and the resulting dominant market position – know how to effectively deploy their proprietary data and generate clear added value for their users (see Chapter 2.1).[27] This can lead not only to skewed competition between companies, but also to a knowledge and informational imbalance compared to the state and society as a whole. Over the medium and longer term, cross-sector concentrations of data could emerge, and the lack of diversity of ideas could make innovation more difficult,[28] both inside and outside the platform ecosystem. This could also create undesirable dependencies on important services provided by private players (e.g., public services).

When it comes to promoting extensive data use and fully harnessing the potential of data, these are unwelcome developments. They show that the overall societal potential of data is far from being exhausted. They also demonstrate the need for individuals, companies (especially SMEs) and academia to be willing to increasingly exchange and make use of data in order to wield its full potential.[29] The reasons for underutilising the society-wide potential of data are different depending on the sector and company. It is commonly agreed upon, however, that Switzerland has not yet unlocked the full potential of data use.[30] When compared to the rest of Europe, the Swiss data economy can be considered rather mature. In many sectors, however, Switzerland lags behind the top players.[31]

2.3 Growing mistrust towards data usage

The growing use of data is creating challenges for citizens, particularly when it comes to protecting and exercising their fundamental rights to privacy and personal data, respectively informational autonomy (see Chapter 3.2).

Anyone who wants to participate in the digital world often has no choice but to relinquish control over their information. Currently, data is often not shared on a basis of transparency or trust, but rather demanded from individuals in return for access to digital applications.[32] This passive relationship often contradicts the reigning self-conception in democratic societies based on the rule of law, where citizens are active participants in the decision-making process. These developments partially challenge the formally existing right of every person not to disclose their data to other individuals or to allow them only a desired use of their data. This report examines approaches that are intended to support the effective enjoyment of this right.

[25] As part of its work on access to non-personal data in the private sector, the IPI has made efforts to alleviate legal concerns, for instance by drawing up sample contracts available here: <https://www.ige.ch/en/intellectual-property/ip-and-society/data-processing-and-data-security> (accessed on 04.03.2022).
[26] *European Commission (2021)*, "Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest: Final Report prepared by the High-Level Expert Group on Business-to-Government Data Sharing", p. 24-28.
[27] *Collovà P. et al. (2021)*, "Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung", p. 9.
[28] See also *IPI (2021)*, "Zugang zu Sachdaten in der Privatwirtschaft", p. 15.
[29] *OECD (2019)*, "Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies".
[30] *Gadient B. M. et al. (2018)*, "Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit".
[31] *SIF (2022)*, "Digital Finance: Handlungsfelder 2022+".
[32] *Collovà P. et al. (2021),* "Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung", p. 3.

Private actors and governments are increasingly confronted with the challenge of users' growing scepticism towards sharing their data. The reasons for this growing reticence are understandable. Processing, connecting and analysing different sources of data has not been a merely academic undertaking, but rather has created increasingly precise depictions of social behaviours and of us as individuals. This has led to new possibilities such as creating data-driven personality and behavioural profiles (→ profiling), triggering unease among users who fear the (real and potential) abuse of this information. These fears are based on private companies' and public authorities' sometimes careless use of user data. Some of these concerns include the possibility of data-driven discrimination, the widening of existing inequalities, the lack of transparency regarding how and by whom data is (or will be) used, and the fear of manipulation. There is a paradox, however, in that these same users will reveal their private information to global platforms in order to benefit from their services, often without exactly knowing what will happen with their data (→ privacy paradox). Researchers have partially explained this phenomenon by citing the weaker market position of users compared to big tech platforms, which leads to favouring affective decision-making against one's own preferences and at the expense of rational cost-benefit analysis.[33]

2.4 Data usage and its challenges

The growing use of data is creating new types of challenges for societies, economies and governments. On a macro level, there is the need to better wield the power of data while at the same time counteracting society's growing mistrust towards increased data use. This is particularly the case when powerful actors such as the public sector or transnational companies hold the keys to this data.

This creates the following problem: in order to increase trust and control, the exchange of data generally needs to be limited. At the same time, more exchange and merging of data will be required in order to unlock its value creation potential.[34] Data policy acknowledges this challenge as the tension between data privacy and data usage. This tension is often portrayed as a binary, win-lose situation. This creates the impression that one must decide between effective protection and the increased deployment of data.

Drawing on our discussions in Chapter 2, we conclude that the following challenges are contributing to the current lack of trust and awareness among a growing segment of the population regarding the sustainable use of data:[35]

1. **The concentration of data and lack of transparent decision-making structures:** Data is distributed unequally and is increasingly becoming concentrated in the hands of a few big tech companies and other actors who enjoy broad market reach in non-tech sectors. In this context, data is often used in a proprietary fashion to generate added value for the organisation in question. This often occurs without meaningful controls on the part of the user and can erode their autonomy while buttressing the dominant position of the organisation that controls the data. If organisations are careless with user data, users lose trust and become less willing to share their data voluntarily.

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

2. **Lack of organisation among users:** In the current platform ecosystem, users (this includes both individuals as well as companies who are dependent on platforms) hardly have any organisation with sufficient influence that advocates on their behalf. Users are usually not collectively organised, and the individual data contribution of a single user is often not significant enough to create any change in the behaviour of the platform operator.[36] This imbalance of power and the strength of network effects with regard to platform behaviour can cause users to accept conditions that are unfavourable to them, both in terms of privacy and economically. This imbalance may partially be mitigated by strong data protection authorities.[37]
3. **Insufficient decision-making context for users:** Users have limited decision-making ability in a digital context. They often lack the necessary knowledge base to make autonomous decisions.[38] At the same time, decisions on whether to share data are always context dependent, and in everyday situations, affective decision-making and the privacy paradox are often at play. This leads to users unthinkingly sharing data primarily in situations where they would otherwise be denied access to a service. Furthermore, the digital divide (→ digital divide) can lead to people being shut out from life in the digital sphere.
4. **Lack of incentives for data sharing:** To create a trustworthy system for data sharing, sufficient incentives need to be in place, both for individuals as well as for companies besides the necessary protective measures. Currently the incentives for data sharing are distributed unevenly, with companies that hold proprietary data often being the primary beneficiaries. These companies tend to have few incentives to change anything that would affect their privileged status, which prevents the potential of data from being fully harnessed.

3 Digital self-determination

In order to better tap into the social and economic power of data while also preventing users from losing control over their own data, Switzerland must develop a data policy approach that overcomes the supposed tension between data privacy and data use.

Digital self-determination aims to be a new approach in this area. At its foundation is the idea that individuals, companies and society as a whole should be able to determine what actions they take in our digital ecosystem. This includes giving these actors the ability to determine the relevance and value of data that is important to them, to have access to and control over this data, and to determine how said data is used. By improving the level of control that individuals and organisations have over their own data, we can increase their trust in our data-driven society and raise their willingness to share and make use of data. Increased data sharing between different actors will increase access and growth opportunities for various players and sectors and open up completely new ways of using and combining data. This will lay the foundation for developing innovative applications with individual and collective benefits.[39] Society as a whole should benefit from the efficiency gains and innovative potential brought about by data – without losing democratic control over basic societal functions in important sectors. We therefore conceive of digital self-determination as a long-term goal.

[36] For counterexamples please refer to *EU Court of Justice (2020)*, "Data Protection Commissioner vs. Facebook Ireland Limited and Maximilian Schrems"; projects and complaints by the non-profit organisation noyb <https://noyb.eu/en> (accessed on 03.03.2022).
[37] Under Art. 49 revFADP, the FDPIC is obliged to initiate an investigation ex officio of upon notification if there are sufficient indications that a data processing operation could violate the FADP. Is the affected individual the complainant, he or she must be informed by the FDPIC about the follow-up measures and the outcome of any investigation. However, these authorities must be equipped with sufficient resources.
[38] This not only involves access to important personal data but also to non-personal data in some situations. The cost of this information is high and lacking in clarity due to the high degree of technical and economic complexity. For more, see *Collovà P. et al. (2021)*, "Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung", p. 7-9.
[39] *OECD (2019)*, "Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use Across Societies", p. 60-76.

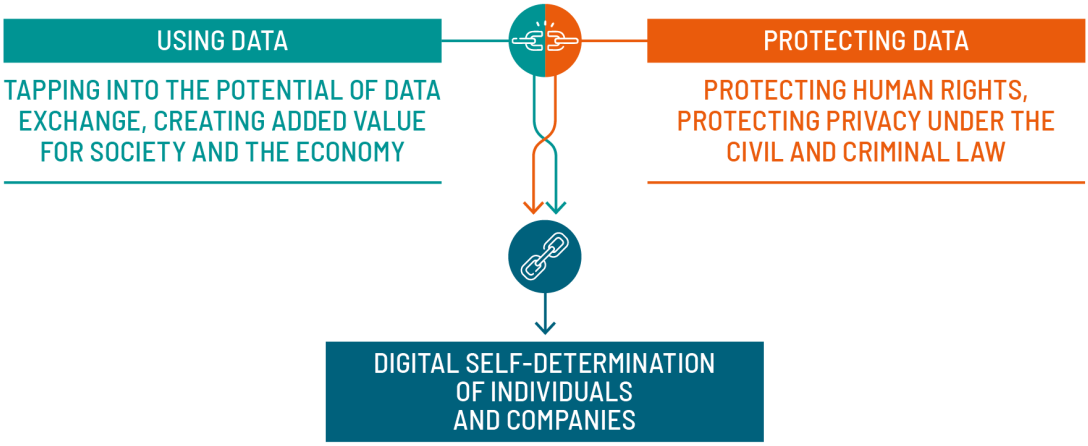

Figure 2: Tension between data use and data protection

3.1 Components of digital self-determination

Self-determination is often understood as the right of every person to freely decide how they wish to live. Self-determination applies not only to individuals but also to entire societies or peoples who are permitted to decide their fate. Self-determination in a digital context also consists of individual and collective aspects.

Individual components

Having knowledge, the freedom to make one's own decisions and the ability to take action are crucial for the self-determination of individuals in the digital space:

- **Knowledge** includes the ability to understand and use digital applications, to have enough information to understand the consequences of this use, and to have a clear understanding of how to implement one's own personal preferences in the digital space.[40]
- **Freedom to make decisions** includes the possibility to independently form opinions in a digital context and to have freedom of choice and decision-making.
- **Ability to take action** includes the possibility to implement one's decisions in the digital space.

Collective components

Collective components of digital self-determination include the following:

- **Social and cultural self:** In the digital space, the self is only conceivable in a networked context. The social and cultural environment forms the basis for how the right to self-determination is exercised.

[40] Part of this requirement includes aspects that are often called *digital literacy* or *data literacy* – in other words, having access to training and having experience in dealing with digital applications and data. However, this is only one aspect of what knowledge means in this context. Knowledge should be understood more broadly as something that all actors need to contribute. For service providers, this means providing and making sufficient information available about how their application works (see also Chapter 4.1).

- **Shared use of data:** Different actors can jointly use and exchange data. This should promote participation in collective forms of data use, and data sharing should expand the scope of action for all players involved.
- **Data as a public good:** A great deal of data, particularly non-personal data (→ non-personal data), can be in the public interest. This kind of data can be understood as a public good that should be available to members of a community.[41]
- **Orientation towards the public good:** Data is used to solve shared problems (e.g., pandemics, climate change), to contribute to efficiency gains and increased prosperity, and to ensure democratic control over the core functions of our society.

3.2 Legal basis

Digital self-determination aims to overcome the supposed opposition that exists between data privacy and data use. From a legal perspective, this means that the concept of digital self-determination consists of two different categories:

- Legal principles that primarily **protect the individual person** and their privacy and guarantee their ability to **participate in the digital space**, and
- Legal principles that primarily reflect **data use** and the associated aspects of economic freedom and the potential for progress and innovation.

3.2.1 Protection and participation in the digital space

Digital self-determination is based on human rights that are enshrined in the Swiss constitution as well as in international law. The following rights are paramount: the right to personal freedom (Art. 10 para. 2 Cst.), the right to privacy, informational autonomy and protection from abuse of personal data (Art. 13 Cst., Art. 8 ECHR, Art. 17 ICCPR), and freedom of information (Art. 16 Cst., Art. 10 ECHR, Art. 19 ICCPR). The collective aspects of digital self-determination are based primarily on political rights (Art. 34 Cst.).

The *right to informational autonomy* is particularly important to the concept of digital self-determination. It states that everyone can always decide who they entrust with their personal data (→ personal data) and under which circumstances and for what purpose.[42] The protection under this right is not absolute, however. Firstly, restrictions of this right are permissible, provided they are proportionate and based on a legal basis. Secondly, the state is the primary duty bearer of fundamental rights. Nevertheless, fundamental rights must be upheld throughout the legal system, and the authorities must ensure that fundamental rights, where appropriate, apply to relationships among private persons (Art. 35 Cst).

In this sense, the legal aspects of personal privacy and informational autonomy are specified in more detail in Articles 27 and 28 of the Swiss Civil Code (CC) and the FADP. Data protection legislation is binding both for public authorities and private actors when it comes to processing personal data and holds different rules for both categories. While in the case of data processing by private actors consent is the primary justification (Art. 13 FADP and Art. 31 revFADP, Federal Gazette 2020 7639), in the case of data processing by public authorities, a legal basis is required instead of consent.[43] Formally

[41] See *types of data* in Appendix 2.
[42] *Häfelin U. et al. (2020)*, "Schweizerisches Bundesstaatsrecht", p. 122-123; personal data means any information that refers to a certain person or identifiable natural person, i.e., data that can be traced back to an individual (Art. 5 let. a, revFADP).
[43] *Häfelin U. et al. (2020)*, "Schweizerisches Bundesstaatsrecht", p. 122-123; *Ghielmini S. et al. (2021)*, "Grund- und Menschenrechte in einer digitalen Welt", p. 41-42.

speaking, the individual affected has thus generally the sole right to decide on the use of their data. The Swiss criminal code and secondary criminal law also contain provisions that penalise the misuse of data.

3.2.2 Economic freedom and innovation

Digital self-determination is also rooted in legal principles related to utility and economic activity. Important examples include freedom of contract in the Swiss Code of Obligations (CO) as well as *economic freedom* (Art. 27 and 94 Cst.) and *scientific freedom* (Art. 20 Cst.).

Freedom of contract and economic freedom support the freedom to do business, which states that natural and legal persons should be as free as possible to conduct and arrange their private economic affairs. This also applies in the digital sphere. Both of these legal concepts enshrine the basic necessity of a free and self-determined way of living and an economic system based on competition and market principles.[44] There is therefore a strong connection between these legal guarantees and the ability to exercise digital self-determination.

The same can be said for scientific freedom, which guarantees the right to conduct research and share the findings thereof, and which also includes the right to access the research findings of others.[45] Article 15 paragraph 1 letter b of the International Covenant on Economic, Social and Cultural Rights also recognises the right of each individual “to enjoy the benefits of scientific progress and its applications”. As such, the right of scientific freedom highlights central elements of digital self-determination (data use and exchange) and supports an approach that harnesses the potential of data in order to create added economic and societal value.

3.2.3 Digital self-determination as the exercise of existing rights

Digital self-determination is broadly embedded in existing national and international law and reflects Switzerland’s social values and fundamental principles. This broad integration into the current legal framework, particularly as it relates to utility- and economic-oriented principles, makes it clear that digital self-determination is more than a mere issue of data privacy law. Digital self-determination requires appropriate parameters to be in place so that individuals and companies can develop autonomously in accordance with the aforementioned principles of the Swiss legal system and social order.

3.3 The potential of data spaces

Digital self-determination can be exercised in a number of different ways. For example, there are approaches that involve creating an account for users to manage their own personal data.[46] This sub-chapter focuses on the potential of trustworthy data spaces as a way of making digital self-determination a reality.

[44] *Häfelin U. et al. (2020)*, “Schweizerisches Bundesstaatsrecht”, p. 196-201.
[45] *Häfelin U. et al. (2020)*, “Schweizerisches Bundesstaatsrecht”, p. 161-162; *Ghielmini S. et al. (2021)*, “Grund-und Menschenrechte in einer digitalen Welt”, p. 70.
[46] For example, applications such as *BitsaboutMe AG*, *digi.me* and *Solid*, which save the data of customers in a decentralised manner and grant them full control over and access to this data.

3.3.1 Data spaces

Data can only be used by multiple parties if it can be easily saved and made accessible. Data spaces facilitate this: by directly connecting the supply and demand sides for data, spaces can help individuals, companies and other organisations have better access to data and tap into new data sources.

A *data space* (→ data space) can be understood as an organisational structure with technical and physical components that connects data users and data providers with sources of data. Data spaces set out rules governing access and how data is processed and used.

The technical and physical aspects of a data space are covered by *data infrastructure* (→ data infrastructure), which is designed to ensure that the space functions properly.[47] The infrastructure should connect supply and demand for data on a technical level in the most efficient way possible, for example via interfaces and common standards. Data infrastructure also makes it possible, via certain operations such as assigning metadata and storing, converting and importing/exporting data, to circulate data from different sources within a data space and to ensure that different actors can make use of it. At the same time, a data space also acts as a *governance structure* that includes organisational aspects. The governance structure sets out the conditions under which data can be exchanged and assigns roles, obligations and rights to all participants.

To summarise, a data space is an environment that facilitates the use of data via data infrastructure by connecting the supply and demand for data under predefined conditions and rules (i.e., a governance structure). Please refer to Appendix 2 for more on the individual components of a data space.

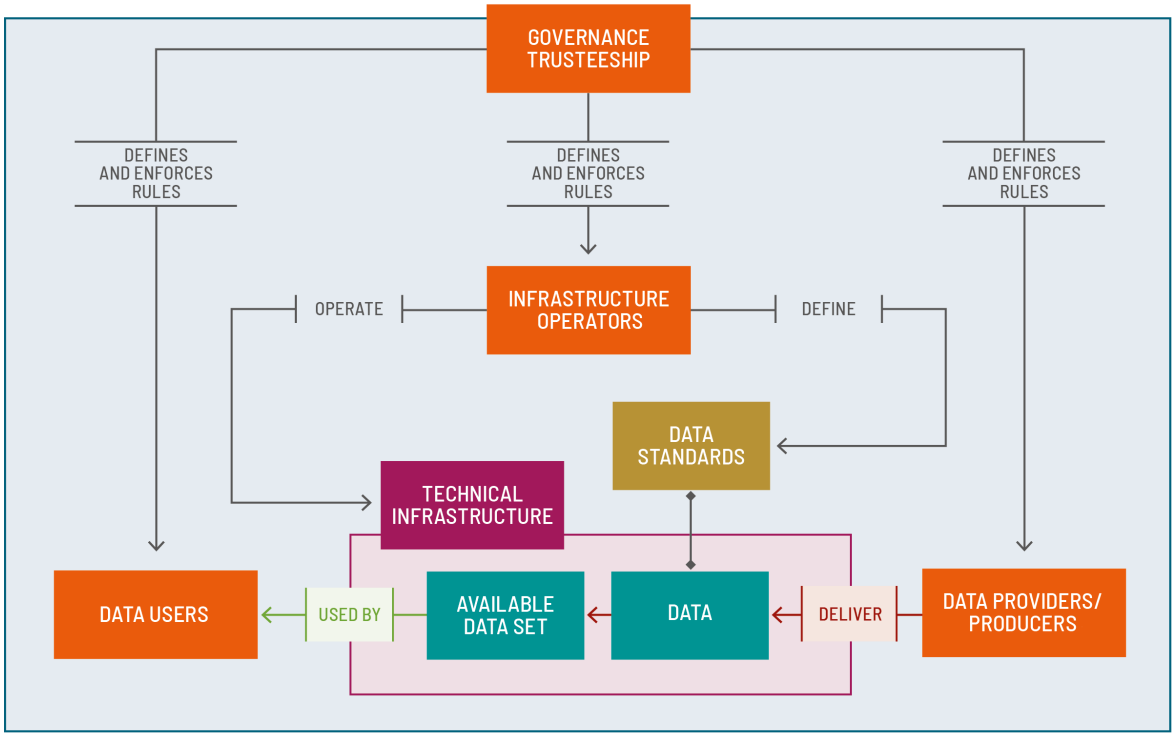

Figure 3: Model of a typical data space

[47] Data spaces don't necessarily need their own physical infrastructure. Decentralised data spaces in particular can make use of already existing physical infrastructure belonging to the people or organisations involved in the space.

3.3.2 Trustworthy data spaces

There is growing recognition of the advantages offered by data spaces in various economic and social areas. The EU, for instance, is committed to creating data spaces in various sectors with the aim of generating economic efficiency gains (see Chapter 6.1).[48] In addition to tapping into economic potential, data spaces can also create other kinds of significant added value if they are organised in a trustworthy fashion. By integrating necessary precautions into their data infrastructure and governance, data spaces can also help promote and strengthen key elements of digital self-determination – such as understanding and knowledge of data use, decision-making freedom and the ability to take meaningful action.

In order to ensure that individuals, companies and society as a whole are able to exercise digital self-determination, there is a need for data spaces that are not only functional but also trustworthy. *Trustworthy data spaces* are a special category of data space. Its trustworthiness is notably characterised by the ability of members to maintain the necessary level of control over their data and to freely consent to sharing it for economic and social purposes. To create this kind of data space, there are certain fundamental requirements or principles that need to be observed, and these principles should serve to increase trust among all participants. Data spaces should therefore create an ecosystem in which people and organisations can live out the values of digital self-determination. These basic principles are introduced in Chapter 4.

4 Basic principles for trustworthy data spaces

To create trustworthy data spaces and make digital self-determination possible, there are certain technical, legal, economic and social parameters that need to be in place (as outlined in the mandate of the Federal Council above). These requirements can be considered fulfilled when a data space complies with certain requirements concerning its design and functionality, how it assigns rights and obligations, etc. This chapter outlines these requirements, or basic principles: **transparency, control, fairness, responsibility** and **efficiency**. Hence, in terms of this report the aim is not merely the compliance with existing legal obligations, including the FADP, but also to apply a high standard in terms of trustworthiness.

In addition to fulfilling these five principles, trustworthy data spaces should be designed in an ecological and socially responsible way that is compatible with the 2030 Agenda for Sustainable Development and its 17 Sustainable Development Goals (SDGs).[49] More concretely, this means that data spaces should contribute to increasing the common good, reducing the digital divide, sustainably using resources and creating equal opportunities. Sustainability is an important aspect not only for data spaces but for digital society as a whole. Further exploration of the five basic principles makes this clear as well – the principles of fairness and efficiency, for instance, and the corresponding indicators also touch on sustainability themes (see Chapters 4.3 and 4.5).

[48] *European Commission (2018a)*, "Towards a common European Data Space"; *European Commission (2018b)*, "Staff Working Document: Guidance on Sharing Private Sector Data in the European Data Economy".
[49] *UNGA (2015)*, "Transforming our World: The 2030 Agenda for Sustainable Development (A/RES/70/1)".

Since there are a range of possible types and purposes of trustworthy data spaces, it is not possible to establish a rigid typology or one ideal model for this type of data institution. Rather, one must acknowledge the diverse challenges and situations that data spaces can face. This means that the *concrete structure of a trustworthy data space* – i.e., *how the different basic principles and indicators are weighed and ultimately implemented* – will differ depending on the sector.

4.1 Transparency

Transparency is a basic condition for trust and creates both understanding and predictability. Transparency allows users to acquire the necessary knowledge and insight into how a data space operates (*understanding*) and gives them the possibility to clearly conceptualise the expected processes and consequences (*clarity*). Transparency measures should therefore take into account the following indicators: *scope, effectiveness, clarity* and *monitoring*. These indicators are defined below.[50]

Firstly, the **scope** of the available information needs to be sufficient**.** In concrete terms, this means that data space operators (→ data space operator) need to make the necessary information available for users to have a clear understanding of how they can expect their data to be used and processed (e.g., information on the purpose of data processing, access by third parties, rights of the parties involved and the business model of the data space).[51]

Secondly, the information being published should be **effective**. This means that there is a proactive attempt to communicate transparency disclosures before any data is released. This information should be quick and easy to find at any time.[52] Furthermore, in certain situations (e.g., security breaches) it is important to choose a communication method that allows the affected parties to be informed as quickly as possible (e.g., via push notification or SMS).

Thirdly, the information which is presented needs to be **clear**. Users should be able to easily understand the information and quickly identify any risks. In addition to using simple, easy to understand language and ensuring accessibility for users with disabilities, data space operators could also make use of adapted information channels (e.g., low-threshold information for average users and more extensive documentation for experts) and visual aids to communicate with their target audience.

Fourth, a certain degree of **monitoring** should be guaranteed. Users should be able to trust that the information presented is as accurate and true as possible. There are various approaches that can be

[50] See also the explicit consent requirements in Art. 6. para. 6 revFADP as well as the Art. 19, 20, 21, 24 para 4, 25 and 26.
[51] For the data protection requirements, see in particular Art. 19 and 20' revFADP.
[52] See also Art. 19 revFADP.

taken here, such as transparency reports, certifications or independent monitoring organisations. These are to be understood as supplements to the existing mechanisms within the legal framework of data protection.

Edulog, a data federation active in the education sector, serves as a good example of how the aforementioned indicators can be put into practice. Anyone who uses Edulog has access to a dashboard where they can see at any time which information has been shared with which third parties. This fulfils the scope and clarity indicators, and Edulog promotes understanding and predictability regarding where and how data is used.

4.2 Control

The principle of control means that individuals can effectively exercise their rights when they wish to do so.[53] It gives users the option of becoming active if necessary, going beyond the state of merely being informed. Control means having the ability to intervene as well as having the freedom to make decisions in a truly autonomous manner. The following indicators should be taken into account when assessing this principle: *control options, voluntariness and free choice,* and *protection from loss of control*.

First, there should be **control options** in place that allow users to directly decide if and under which circumstances their data can be used, to whom their data can be released, and what kind of data is involved. Wherever possible, the processing of data should be limited (e.g., by having different access or data privacy levels), especially for sensitive data. To guarantee users' freedom to take action, it must always be possible to withdraw decisions on data sharing and they must be limited in duration. This means that users must be able to withdraw their consent and should have the option to periodically renew their consent to general purpose data use.

Second, **free and voluntary choice** must be guaranteed. Participation in data sharing arrangements should be voluntary and without outside pressure. Users should also be able to choose freely between different options, i.e., without having their decision limit their future options or lead to dependencies. This means that users must always have the option of switching and transferring their data to a new provider without encountering any hurdles, as is also provided for in Art. 28 revFADP. True freedom of choice also includes deciding how one's data is managed: this task can also be delegated to third parties, for instance a data custodian (→ data custodian).

Third, there should also be effective **protection from loss of control** in place. It is necessary to have precautionary IT measures and clear risk management processes in place in order to ensure the integrity of the data space and the security of the data. The space also needs to have binding processes and

[53] In terms of legal possibilities, see in particular Art. 28 et seq. CC as well as Art. 25 and 32 revFADP.

contingency measures that protect users in the event of a security breach (e.g., immediately informing users).[54]

An instructive example of the principle of control is the *electronic patient record (EPR)* system, which heavily emphasises control and has already implemented indicators to this end. The EPR gives users the possibility to control who has access to their data and for how long. Users can revoke this access at any time. The EPR also implements the principle of free and voluntary choice: it is up to the individual whether they want to open a record, and afterwards they can freely decide how much access to grant healthcare providers for their treatment.

4.3 Fairness

The principle of fairness guarantees fair treatment to all participants. It does not, however, mean equal treatment within a data space, since differences in roles and forms of governance can mean differences in obligations and/or privileges. Nevertheless, certain minimum standards need to be met regarding data space access and the distribution of privileges to ensure that they are in proportion to the roles that each stakeholder plays. The principle of fairness can be broken down into the following indicators: *proportionality, fair distribution of costs and benefits, non-discrimination,* and *independence*.

First, the data space needs to ensure **proportionality** when it comes to processing data and in designing different roles in the space.[55] When it comes to data processing, one always needs to weigh whether there are alternatives to using certain kinds of data – for instance, replacing personal data with *anonymised data* (→ anonymisation) or *differential privacy* (→ differential privacy) – and whether the principle of privacy by design (→ privacy by design) is being implemented to the best possible degree (i.e., only collecting as much data as is necessary). Also, any difference in treatment between different roles within a data space must always be proportionate (see also freedom from discrimination).

Second, **costs and benefits** should be **distributed fairly**. This means that no one should get the short end of the stick when it comes to accessing data spaces and making use of their benefits. It also involves questions of cost sharing for stakeholders (both individuals as well as companies). For instance, companies can experience added value from developments such as integrated supply chains or efficiency gains on the part of their suppliers. There are possible approaches such as compensating companies that make their data accessible. These approaches can be controversial, however, especially when it comes to compensating individuals or creating financial incentives for them.[56] There

[54] See the minimal requirements according to Art. 24 para. 3 revFADP.
[55] See Art. 6 para. 2 revFADP.
[56] *Collovà P. et al. (2021)*, "Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung", p. 12.

are concerns about the potential for exploiting vulnerable or weak individuals and also about the potential for disappointment since the value of an individual data set can often be much lower than expected. On the other hand, financial incentives may lead to more data being shared, thereby giving companies better access to data that they can use to create personalised products and services.[57]

Third, trustworthy data spaces need to operate in a way that is **non-discriminatory**. This involves issues of data access and of having a representative foundation of data that can be used for making decisions. Data space operators need to ensure that all actors have access to the data they need based on objective and fair criteria. Regarding data quality (→ data quality), insufficient data can lead to skewed digital depictions of individuals where their digital self no longer reflects their real self (→ data bias). This can create discriminatory outcomes in a digital context, where a person is defined solely by the data that has been collected about him or her. Furthermore, it is important to have high-quality data in order to minimise the discriminatory effects of data on marginalised groups. Data space operators need to work to remove inequalities when data is used in situations that are already prone to structural discrimination.[58]

Fourth, data spaces should be operated **independently**, meaning that they are free of conflicts of interest and are protected from abuses of power. Those responsible for the technology and the rule-making must not be unilaterally dependent on certain actors. The governance of a data space needs to be designed in such a way that the operator acts transparently and can potentially be held accountable. There should also be measures in place to ensure that data space operators are not pursuing other interests or aims than those set out in the statutes.[59] The choice of system architecture also plays a role: in some cases, a decentralised or distributed architecture can reduce the potential for abuse considerably. The independence of a data space can also be strengthened by having a system of representation in place for all participants. This applies in particular to stakeholders with little or limited influence (e.g., SMEs or individuals), where simple and transparent representation mechanisms such as advisory bodies can strengthen participatory decision-making.

Switzerland's *national data infrastructure in the energy sector (Datahub-Strom)*[60] and in the *mobility sector (Nationale Datenvernetzungsinfrastruktur Mobilität [NADIM])* serve as examples of how indicators for the principle of fairness can be implemented. Datahub-Strom is intended to provide all participants with non-discriminatory and clearly regulated access to data infrastructure within the energy sector, while NADIM guarantees its independence by being designed as a neutral and independent institution.

4.4 Responsibility

The principle of responsibility creates an avenue for assigning rights and obligations and demanding their enforcement. Clear *governance mechanisms* and *enforcement mechanisms* form the basis of this principle.

[57] See also *BitsaboutMe AG* <https://bitsabout.me/en/> (accessed on 02.01.2022), which allows people to earn money if they share their data with companies or academic institutions for research purposes.
[58] *Findlay M. and Remolina N. (2021)*, "The Paths to Digital Self-Determination: A Foundational Theoretical Framework", p. 27-28.
[59] *Collovà P. et al. (2021)*, "Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung"; *Blankertz A. (2020)*, "Designing Data Trusts: Why We Need to Test Consumer Data Trusts Now"; *Schneider I. (2019)*, "Governance der Datenökonomie: Politökonomische Verfügungsmodelle zwischen Markt, Staat, Gemeinschaft und Treuhand".
[60] *SFOE (2021)*, "Datahub Schweiz: Kern zukünftiger Dateninfrastruktur digitalisierter Strom- und Gasmärkte".

First of all, having clear **governance mechanisms** requires that the data space clearly defines and publishes how it functions as an organisation. There are different forms of governance structures that can be used (see Appendix 2). Regardless of which kind of governance is chosen, the rights and obligations of the different participants in a data space need to be clearly defined. Ideally the basic mechanisms, roles and responsibilities are set out (e.g., in binding statutes, contracts or in specific cases, in guidance documents such as checklists or even via legal requirements).

Secondly, there should be **enforcement mechanisms** that allow participants to demand that the data space adheres to its stated guidelines, even in situations where it is not a matter of non-compliance with applicable laws.[61] This includes making sure that any measures taken by the data space (e.g., when excluding a participant) are clearly and demonstrably justifiable. Furthermore, actors who disagree with a measure should be able to oppose it in order to avoid protracted processes. This can take different forms, from internal procedures to external mediation bodies that are defined in advance. In special cases, for instance if highly sensitive data is involved, establishing an independent complaints office can help create additional trust.

Both the electronic patient record (*EPR*) system and the *Edulog* data federation have responsibility measures in place. The EPR system contains an enforcement mechanism for fining anyone who accesses an electronic patient document in an unauthorised manner (i.e., without having received the necessary access rights from the user) in a non-emergency situation. Edulog sets out contractual rules between participating service providers, thereby creating transparent governance mechanisms that protect the personal data of users.

4.5 Efficiency

The fifth principle relates to efficiency. Data spaces are only efficient if they allow the relevant data to be exchanged and used without problems. The following indicators are used to define the efficiency of a data space: *high data quality, exchangeability, interoperability* and *adaptability*.

[61] See Art. 32, 41 and 49 revFADP.

First, data that is of sufficiently **high quality** should be made available, or the data should at least be graded for its level of accuracy or quality.[62] The data provided should be immediately usable without having to take additional steps to increase its quality. High-quality data means that the data is as complete and intact as possible – both structurally, in terms of the scope of the data, and also from a content perspective, in terms of the information it should contain. Clear quality management procedures and processes are needed to ensure that the necessary level of data quality is reached. Data space operators need to set clear standards, regularly review the necessary procedures and clearly set out responsibilities with regard to data maintenance. It is also possible for the data space itself to increase the quality of its data, for instance via data processing.

Second, data spaces should guarantee the **interoperability** (→ interoperability) of their data between different actors and institutions. To ensure that data can be used efficiently, redundancies and discrepancies within and between systems need to be reduced. Generally, we distinguish between different levels of interoperability (see Chapter 6.3).

Third, trustworthy data spaces need to operate in a way that is **adaptable**. They need to be flexible enough to be able to adapt to quickly changing conditions in a dynamic environment. An increase in the number of participants or the integration of new data sources should not entail compromises on credibility or functionality. Similarly, the governance mechanisms and technical infrastructure need to be future-proofed and designed to accommodate growth. Additionally, one should bear in mind that a data space's risk profile can change due to external influences. As such, operators need to regularly evaluate whether their current measures are appropriate, calling in third-party auditors or other data space operators where necessary.

Switzerland's national data infrastructure network in the mobility sector NADIM illustrates how the principle of efficiency can play out in a real-life data space. As a central infrastructure provider, NADIM opens up access to as much multimodal mobility data as possible. It guarantees interoperability to ensure that all participants, especially companies, can exchange and use data as efficiently as possible. Datahub-Strom, a Swiss data space operating in the energy sector, is similar in this regard and strives for a high level of standardisation.

4.6 Interim conclusion

These five basic principles and the corresponding indicators form the core of the response to the Federal Council's question of what is required for the creation of trustworthy data spaces. They should be understood as guidelines and can serve as inspiration for the operators of trustworthy data spaces when designing their overall architecture, governance and technical parameters. Appendix 3 of this report sets out *recommendations* for each one of the aforementioned indicators. The principles, indicators and recommendations can be used as guidelines for putting ideas into practice and can serve as a foundation for future work on voluntary codes of conduct that govern the establishment and operation of trustworthy data spaces (see Chapter 7.1). They should therefore be understood as a toolkit for future work in this area.

[62] The term 'high quality' depends in large part on the purpose for which the data is being used. For this reason, it is essential to provide information on the quality and accuracy of the data on offer, for instance who generated it or when it was last updated.

5 Data spaces in Switzerland

In Switzerland, data spaces are in the process of being established in a variety of sectors. This chapter will introduce a select handful of data space projects in mobility, energy, finance, healthcare and education. Here it should be mentioned that there are already some data spaces on the federal level such as that for geodata infrastructure.[63]

We will explore how digital self-determination can play a role in building up these sector-specific spaces in Switzerland. It is important to note that the selected examples all have trustworthy data usage models and thus display a certain affinity to the concept of digital self-determination. This is not the case for all data space projects in Switzerland.

5.1 Mobility

Mobility data is indispensable both for ensuring the smooth functioning of the mobility system as a whole and for the development of new mobility services. In this regard, mobility data fulfils two important functions: it acts as a necessary foundation for the functioning of the overall transport system and drives innovations that lead to improvements and efficiency gains. Widely available mobility data allows for improved alignment between different modes of transport, for filling capacity to the best extent possible, and for offering transport options better in line with customers' needs.

As it stands today, around 90% of trips are unimodal, meaning that travellers use only one mode of transport to reach their destination. The average occupancy of public transport is 30%; for cars, the figure is 1.5 persons.[64] By having a suitable foundation of data, free capacity can be used more efficiently, and the combination of different modes of transport (e.g., public transport, motorised personal transport, car/bike/mini-scooter sharing, carpooling, taxis, as well as walking and cycling) can be promoted. Coordinating transport capacity could help achieve various goals in terms of transport, climate and the environment.

The central requirement for networked mobility is that the relevant data and services for different mobility options are easy to find and use. The Federal Council has commissioned DETEC (FOT) with drafting a legal basis for the gradual build-up of a **national data infrastructure network in the mobility sector (NADIM)** that can provide and harness mobility data. NADIM aims to link together mobility data from different providers to create a foundation of data that makes access to overall mobility easier and more efficient for travellers.

NADIM connects mobility service providers and end-customer systems with various relevant sources and collections of data. Use by data suppliers is voluntary. In addition to core data, data suppliers also have the option of providing additional complementary data via NADIM. Those in charge of NADIM act as data space operators (→ data space operator) and should guarantee both the technical operations and the governance structure.

Participants	- Mobility service providers (e.g., public transport and private service providers) - Operators of end-customer systems (e.g., web services and apps)

[63] For further information see <https://www.swisstopo.admin.ch/en/knowledge-facts/geoinformation/spatial-data-infrastructure.html> (accessed on 04.03.2022).
[64] *FOT (2022)*, "Erläuternde Bericht zum Bundesgesetz über die Mobilitätsdateninfrastruktur (MODIG)", p. 6.

	- Public institution that operates NADIM (infrastructure and governance)
Types of data	- Non-personal data: geodata, schedules, availability of vehicles and mobility options, arrival and departure times in real time - Personal data plays a minimal role initially
Purpose of data	- Traffic management (filling capacity and steering users) - Driving innovation and increasing efficiency of mobility services - Promoting multimodal/networked mobility
Infrastructure	- Data infrastructure that allows for standardised data use, mainly by creating interfaces (APIs)
Governance	- NADIM is operated by a public, independent, non-partisan and non-profit federal government institution - Even though the data is generally stored in a decentralised manner, the governance structure is organised centrally via the data space operator

5.2 Energy

Data also has an important role to play in the transformation of Switzerland's energy sector. Climate change and the country's net-zero target require fundamental changes in the electricity and gas sector, in mobility and in heating and construction. A key factor for Switzerland is expanding renewable energy, which will bring about enormous changes in energy generation and consumption. Instead of connecting a handful of centralised energy-generating units to the grid, the future setup will require integrating an increasing number of decentralised providers whose energy will be supplied to various end consumers via the power grid.[65]

Readily available, high-quality data has a tremendously important role to play in a decentralised energy landscape. It allows for improved planning of system operations, for calculating energy flows on a fine-grained level, and for the important aspect of involving the customer, for instance when compiling their energy mix. All of this requires data infrastructure that can facilitate the necessary exchange of energy data and increase transparency in the system. Currently, data is still exchanged bilaterally between distribution grid operators, who are responsible for collecting data and measurements, and third parties. This type of data exchange exists for historical reasons, is not fit for the future and creates huge obstacles for small market players, consumers and academics. This status quo acts as a market, innovation and digitalisation barrier to designing a sustainable energy system. Furthermore, the gas sector and other industries face similar challenges.

The dispatch on the consolidation bill for secure renewable energy supply has laid the foundation for creating a national data infrastructure in Switzerland's energy sector, the backbone of which is a data hub called Datahub-Strom. This hub ensures that data silos in the energy market are connected by acting as a centralised recipient for the specific static data needed to automate power management processes, improve data quality and market transparency, and significantly increase market efficiency. Important measurement data on consumption, production and storage remain decentralised. Access to the data is guaranteed with one standard across Switzerland, and the hub strengthens the rights of consumers in their role as data producers. By using standardised interfaces, market players can directly, consistently and fairly access the data granted to them by customers. From a public interest and transparency perspective, certain aggregated data about the power system could be made available via

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

the data hub. The proposal to establish national data infrastructure in the energy sector sets out the first regulatory guidelines for the future creation of a trustworthy data space in this sector. Something similar could also be created for the gas industry.

Participants	- End customers, consumers - Distribution grid operators (e.g., public utilities operators) - Energy suppliers - Energy service providers and start-ups (e.g., flexibility providers) - Universities and innovators - Data hub operator
Types of data	- Data on energy consumption, production and storage - Data on available flexibilities - Technical data, e.g., on connected loads - Aggregated data on the municipal, cantonal and federal levels
Purpose of data	- Improving forecasting and calculation processes - Energy planning and statistics - Accounting and operational planning - Support for science and innovation - Energy efficiency and other services
Infrastructure	- Data infrastructure that allows for standardised data use, mainly via interfaces (APIs) - Central registries, e.g., user registries, measuring station registries or consumer data registries
Governance	- Independent private consortium of data infrastructure operators (market neutral, Swiss controlled) that is independent from the energy industry - Intention to set out guidelines in the form of an ordinance - Monitoring of compliance and costs by the regulator

5.3 Healthcare

The Swiss healthcare sector is characterised by the need to communicate between and involve a wide range of actors. For this reason, the **electronic patient record (EPR)** system is an important milestone. The record provides important information for treating patients and can be accessed at any time.

The EPR is a virtual, decentralised dossier that contains treatment-related information from a patient's medical history and that can be made available to the medical professionals in charge of their care (e.g., lab data, prescriptions, radiological reports). The patient also has the option of uploading their own data to the record (e.g., information on allergies or emergency contacts) in order to make it available to their healthcare provider.[66] In this way, the EPR connects *medical professionals* and *healthcare institutions* with patients.

Participants	- Patients - Healthcare professionals and the institutions they work at - (Patients') affinity domains (EPR providers), organisational connections between healthcare professionals and their institutions

[66] Art. 2 let. a EPRA.

	- Issuers of identification documents - Platform providers (providing the EPR operating systems) - Providers of primary systems - Certification authorities - Swiss accreditation agencies - Federal government (creating and operating centralised technical components, informing the population, evaluating the EPRA, financial aid for establishing and certifying (patients') affinity domains) - eHealth Suisse (Swiss Competence and Coordination Centre of the Confederation and the Cantons) - Cantons
Types of data	- Personal data requiring special protection (→ personal data requiring special protection): medical information relevant to the patient's treatment
Purpose of data	- Improving the quality of medical treatment - Increasing patient safety - Simplifying the treatment process and increasing the efficiency of the entire healthcare system - Promoting the healthcare knowledge of patients
Infrastructure	- Certified EPR providers offer the technical and organisational infrastructure for the patient records. This infrastructure makes it possible, for instance, to connect the EPR provider with the IT system of the healthcare provider. The federal government also operates central query services that deliver the necessary reference data for communicating between (patients') affinity domains and access portals.
Governance	- The EPR system is provided by decentralised (patients') affinity domains. These organisations receive certification prior to starting operations and are subject to regular monitoring. - The Federal Act on the Electronic Patient Record (EPRA) sets out the framework for establishing and disseminating electronic patient records in Switzerland. - Transnational design via use of internationally recognised standards such as IHE profiles, FHIR, etc.

5.4 Finance

Changing customer needs, new market players and innovative technologies are posing a challenge to established financial institutions, including banks. **Open finance** is poised to make lasting changes to the financial sector.[67] Open finance is based on the principle of exchanging financial data via standardised interfaces with the permission of the customer.[68]

Open finance holds potential for a wide variety of areas. Business and private customers alike can benefit from accessing a full summary of their financial situation by having their different accounts at different providers integrated into one overview. In this way, open finance can provide an improved customer experience thanks to seamless transitions between different financial service options. Banks

[67] *Swiss Bankers Association (2020)*, "Open Banking: An overview for the Swiss financial centre", p. 7.
[68] For more on the great potential of open finance, see <https://www.sif.admin.ch/sif/de/home/dokumentation/fokus/open-finance.html> (accessed on 04.02.2022).

and third-party providers can benefit as well. Thanks to mutual data exchange, banks can make use of third-party data to offer innovative products. Open finance offers third-party providers, such as those in the fintech space, the opportunity to launch their products and services with less technical and regulatory effort.[69]

There are different challenges when it comes to promoting the exchange of financial data of this kind, for instance: the need to standardise interfaces, resistance from established players when it comes to disclosing customer data to potential competitors, or reputational risks connected to failures on the part of third-party providers.

Open finance connects customers with their banks, insurers and other financial institutes via third-party providers. This also holds true vice versa: financial service providers can also offer services from third parties. Third-party providers take on an intermediary function in this context. This in-between position frees customers from the need to individually deal with different banks, insurers and other financial institutes. Rather, they can take care of their personal financial affairs via a single third-party platform or make use of several services via a single bank.

Participants	- Customers - Financial service institutes such as banks and insurance companies - Third-party providers (services & technical infrastructure providers) - Industry associations for setting standards
Types of data	- Personal data: banking data and data connected to insurance policies, investments in securities, mortgages and pension funds, including position and transaction data that may not necessarily be traceable back to an individual
Purpose of data	- Promoting customer control over their financial data - Increasing the competitiveness of the Swiss financial sector, chiefly through connecting different services
Infrastructure	- Established financial institutes, third-party providers and other infrastructure providers are responsible for providing and managing the infrastructure. - The open standardisation of interfaces (APIs) is a key prerequisite for smoothly connecting to third parties and exchanging data in an error-free way.
Governance	- Unlike in the EU, currently in Switzerland there is no legal obligation for financial institutes to exchange data with third-party providers via standardised interfaces. The Federal Council has asked the FDF/SIF to continuously monitor the need for action in connection with promoting and expanding open finance. - The FDF/SIF has worked together with the private sector to develop a common understanding of roles for future cooperation, particularly when it comes to standardising APIs.

[69] *Swiss Bankers Association (2020)*, "Open Banking: An overview for the Swiss financial centre", p. 7-8.

5.5 Education

When it comes to education, self-determination is situated in a special context. In one regard, it helps learners – and therefore society as a whole – deal with data in a responsible way. Digital skills are integrated into curricula at every level. On the other hand, the educational sector itself collects personal data on school-age children and adolescents. They are entitled to special protections of their integrity and to having their development promoted. For this reason, it is important for responsible stakeholders to be educated and competent when it comes to dealing with this kind of sensitive data.

Currently, one of the main challenges to digital self-determination in the education system is clarifying the relationship between private and public actors. This question takes on special relevance in connection with basic infrastructure services such as cloud services. In many cases, a small number of powerful companies effectively exercise control over data thanks to their proprietary ecosystems. An additional challenge is establishing organisational and structural approaches to be applied across Switzerland. These approaches aim at strengthening control over data and putting the necessary prerequisites in place to enable access and exchange in the first place (e.g., data federations, standards for interoperability, nationwide identity solution). Different approaches for tackling these challenges are currently being developed. In addition to establishing a data federation for vocational education[70] that creates the technical parameters for exchanging data between different stakeholders, Switzerland is also working on developing a nationwide data use policy for the educational system.[71] The challenge lies in its applicability to other areas of policy.

Edulog is the most advanced project in the educational sector that implements the concept of digital self-determination. Edulog is a data federation that brings together cantons, communes and schools and issues digital identities for members of their school systems. This allows users to use their digital identity as provided by their canton, commune or school and their pseudonym as provided by Edulog to access and make use of a variety of online services related to the school system and education (learning apps, library access, etc.). In this way, Edulog aims to create a trustworthy space.

Participants	- Cantons, communes or schools that issue and authenticate digital ID for members of their school systems (identity provider) - Private or public providers of online services (e.g., online services from educational publishers, cloud services or learning apps) that can be used in lessons (service providers) - Edulog data federation, which provides users with a pseudonym
Types of data	- Personal data: the digital ID issued by cantons, communes and schools consists of several attributes (e.g., name, date of birth, role, etc.).
Purpose of data	- Simplifying access to online services related to schools and teaching - Increasing 'mobility' within the educational system
Infrastructure	- Edulog's technical operations are managed by a private company (ELCA Informatik AG), meaning that the identity and service providers are connected with one another via a central IT infrastructure. - Edulog acts as a mediator of attributes between the identity and service providers.

[70] Please refer to <https://www.educa.ch/taetigkeiten/datenfoederation-der-berufsbildung> (accessed on 03.01.2022).
[71] Please refer to <https://www.educa.ch/taetigkeiten/fachstelle-datennutzung> (accessed on 03.01.2022); *EDUCA (2021)*, "Digitalisierung in der Bildung: Bericht im Auftrag des SBFI und der EDK im Rahmen des Bildungsmonitorings".

Governance	- Edulog facilitates the controlled, targeted use of data in connection with access to online services. - As a data federation, Edulog does not store any information itself apart from the identity provider's technical identifier and the pseudonym provided by Edulog. All additional information (attributes) remains under the control of the identity provider (canton, commune or school).

5.6 Interim conclusion

When comparing the aforementioned real-world examples of data spaces with the basic principles and indicators outlined in Chapter 4, we reach the following conclusions:

- **Transparency:** While the principle of transparency is present in all of our examples, the emphasis is placed on different aspects. For Edulog and the EPR system, transparency is understood as the user being able to see who has access to their data. For open finance, it means the customer can see what transactions they have made. NADIM and the Swiss Hub for Energy Data (SHED), on the other hand, want to promote the transparency of the entire system in order to match supply and demand in the best way possible. For NADIM, this primarily concerns simplifying travellers' access to mobility options and ensuring optimal capacity utilisation and coordination for different modes of transport (multimodal mobility). For SHED, the emphasis is on transparency regarding energy consumption and production in order to achieve savings and guarantee the energy supply. Placing emphasis on different aspects of transparency is certainly a sensible approach. Our data space examples in healthcare, education and finance deal with services that directly impact individuals and deal with highly sensitive data. In contrast, the mobility and energy data spaces are more focused on overall systems. Transparency plays an important role in all of our examples. What this looks like in concrete terms differs depending on the purpose of the data space and the sensitivity of the data.

- **Control:** A similar tendency can be observed when it comes to the principle of control. This principle is chiefly visible in our examples that deal with sensitive personal data such as electronic health records and open finance. Our examples use various mechanisms to ensure that participants have the freedom and ability to take action. Users in these data spaces can decide who they want to share their data with, which data they want to share, and when and for which purpose they want to share it. This is especially true for the EPR system. The element of control is less defined for NADIM and SHED since their focus is on non-personal data. Another reason is that the primary data providers and beneficiaries are not end customers but rather mobility and energy companies.

- **Fairness and responsibility:** NADIM and SHED stand out as examples of data spaces that emphasise the principles of fairness and responsibility. A neutral and independent institution runs NADIM to guarantee its operations. Institutional independence also plays a central role in the development of SHED. These approaches guarantee non-discriminatory access to data, a proportionate level of data collection, and independence in dealings with stakeholders. NADIM is reviewing the option of an ombudsman's office for this purpose. These focal points were not chosen at random: both in the mobility and energy sectors there are different market players with various roles of systemic importance and a corresponding level of market power. Principles such

as fairness and responsibility take on special importance in this context. This also applies to open finance, where third-party providers such as fintech companies are challenging traditional players. The EPR system and Edulog also attach great importance to fairness and responsibility. They do so mainly by ensuring proportionality, only collecting as much data as is necessary, and appealing to service providers' sense of responsibility – and for EPRs, by fining anyone who accesses records without prior permission.

- **Efficiency:** All of our examples generate and emphasise efficiency gains by making use of standardised interfaces. NADIM deploys interfaces to create a data infrastructure that allows for the use of standardised data. This involves defining a core data set; this is similar to Edulog, which practices standardisation by defining various attributes for each user. Open interface standards are also a central requirement for open finance, as they allow traditional finance companies and third-party providers to dock onto the systems of financial institutions and seamlessly exchange data with them. The EPR system is able to create efficiency gains by directly connecting the EPR provider and the IT system of the healthcare provider.

Our real-world examples show that thus far, when data spaces **implement the principles of digital self-determination, they place their emphasis on different factors**. This is partially explainable due to the different purposes of the spaces, the type and sensitivity of the data, or the relevant market structures in a particular sector.

We can also observe that while the principles of digital self-determination are in some cases mutually dependent, in others they can sometimes come into conflict. Having control over one's data, for instance, requires that there is transparency about which data is going where and for what purpose. On the other hand, an excessive degree of control can obstruct the free flow of data and lead to a loss of efficiency.

Finally, it is evident that our examples are limited to particular sectors (mobility, energy, healthcare, education, finance) and are geographically bound (canton, nation state). This contrasts with the tendency of global platforms to merge increasing amounts of data from various sectors in order to achieve further efficiency gains. For this reason, there is **untapped potential in Switzerland for connecting and creating interoperability between data spaces that span different geographies and sectors**.[72] There are currently efforts underway on the administrative level to fill the gap in this regard. There is already a federal geodata space that ensures the availability of standardised geodata, thereby enabling the increased analysis and use of spatial data. The interoperability platform i14y, which acts as an interface to promote data exchange and connect various parties, also contributes to the potential for data to be used and reused.[73]

Additionally, a national coordination office can help advise interested parties on data spaces, both regarding questions about design/conceptualisation and issues of interoperability. Coordination offices at the national level (data hubs) are in the process of being created in various European countries. This is also the case in Switzerland, where discussions are underway for establishing DataHub4Gov, a coordination office for administrative units and activities.[74] The question remains open as to whether a

[72] The FADP and the Council of Europe's Convention 108+ have to be taken into account in any case. Furthermore, it is important to ensure that the recognition of the Swiss level of data protection by the European Union is not jeopardized.
[73] For additional information, see <www.i14y.admin.ch> (accessed on 04.03.2022).
[74] *Digital public services (2022)*, "Developing and managing the eGovernment architecture for the strategic implementation plan".

national coordination office – a Swiss data hub – should be created for other kinds of stakeholders as well (see Chapter 7.2).

6 International data governance and interoperability

Data often flows across national borders. The reasons for this vary: in some cases, data from different countries is aggregated in order to have more diversified and representative data as a basis for making decisions. In other cases, data is exchanged across borders for processing purposes as part of a value chain, which can be regional or even global in nature. Where the infrastructure is located also plays a role: if there is no local infrastructure (e.g., for cloud systems → cloud), people will turn to service providers abroad, which in turn internationalises the flow of data.

There is enormous potential in data that can be used internationally. Harnessing the power of transnational data is important for Switzerland as a mid-sized, highly networked economy and can help secure Swiss access to international markets as well as the EU's single market. Data spaces should be internationally compatible in order to fully tap into this potential. This means that we need cross-border standards that make shared use possible. The main foundation on which to build upon are the Council of Europe's Convention 108+, Articles 14 et seq. revFADP as well as the criteria from the European Union concerning the recognition of the Swiss level of data protection.

The following chapter discusses the international context, the obstacles to establishing uniform parameters globally, and potential solutions.

6.1 Different approaches to data policy

As geopolitical rivalries have heated up over the past several years, there has been an increase in polarisation along international and multilateral lines. This tendency can be observed in digital and data policy, where different – and sometimes opposing – approaches come into conflict. Just as in other areas, there are different interests and values that are currently standing in the way of the minimum consensus that would be necessary for establishing common international data policy. The currently prevailing data policy approaches can be roughly summarised as follows:

1. Some countries such as the US pursue data policy that is strongly oriented towards the **freedom of businesses to use data**. In this framework, data should be used with the least amount of restrictions from the state in order to boost innovation and competitiveness. Here data is primarily understood as an economic resource that belongs to the entity controlling it. Accordingly, certain data policy measures are given priority, such as protecting intellectual property and business secrets and ensuring the free flow of data across borders. Further regulatory intervention is generally rejected as being a roadblock to innovation.

2. Other countries such as China see access to and control of data in far-reaching areas of life as **the prerogative of the state and an exercise of national sovereignty**. In this framework, data is primarily used as a tool of the state to control society. In an international data policy context, these players are attempting to strengthen the role and influence of the state at the cost of other potential stakeholders.

3. The EU as well as other European and non-European countries have decided to pursue a more **value- and people-oriented approach to data policy**. This approach seeks to strike an appropriate balance between freedom for individuals and companies, achieving a certain level of transparency, and protecting privacy and other basic rights. By actively regulating certain areas, the aim is to strengthen the trust of the population when it comes to data (see box below).

Here the EU is a natural partner for Switzerland in many areas: both advocate for a data-driven society that centres around values and people. Wielding the economic and societal potential of data should only be done while guaranteeing intellectual property rights and protecting and preserving fundamental rights and democratic values. Furthermore, Switzerland's involvement in European data spaces is sensible for both parties because of common economic relationships and strong connections between sectors, for instance due to shared supply chains.[75]

That said, with the concept of digital self-determination Switzerland has developed its own approach, which it can contribute when it comes to the design of European data spaces. While the EU often reacts to data policy challenges with new regulation, Switzerland aims to enter into a dialogue with all stakeholders and use the concept of digital self-determination to achieve a healthy balance between having the freedom to innovate and protecting individual rights. The concept of digital self-determination, along with the basic principles and indicators outlined in this report (see Chapter 4), can make a direct contribution to the development of European data spaces.

Real-world example: the EU

The European Commission's *Data Governance Act* seeks to introduce conditions for data sharing providers (known as data intermediaries → data intermediaries) and for providers who donate data. This includes a registration and supervisory apparatus for data intermediaries and voluntary registration for altruistic data organisations that donate data. The Data Governance Act hopes that by providing this framework, it can promote trust in these institutions.

Similarly, the Commission wants to promote the development and interoperability of European data spaces in certain strategic economic sectors and areas of public interest: industrial production, healthcare, financial data, green deal, mobility, energy, agriculture, public administration and education. Data spaces should be established in these nine sectors to make it easier for public authorities, businesses and the scientific community to use and exchange data of a non-personal nature. In contrast to digital self-determination, which aims to promote the trustworthy use of personal and non-personal data alike, the European Commission is using this first step to focus on creating connections between non-personal data.

6.2 The fragmented global data policy landscape

Due to the different approaches towards data policy, there is currently no international consensus on developing global governance for data and data spaces. Although the norms of international law (such as protecting privacy) apply in both a digital and a physical context, there is currently no agreement on

[75] See also *Federal Council (2020a)*, "Foreign Policy Strategy 2020-23".

the responsibilities and processes of existing international organisations and the task of defining these norms for the digital arena. It is therefore unclear which international bodies would handle which digitalisation issues and to what end.

On top of that, data spaces are often designed and created with a limited geographic scope at their inception due to differences in the legal systems between territories. For this reason, data spaces routinely develop along different political or legal lines. Because data spaces are saddled with these geographical limitations at the time of their founding, the issue of interoperability between international data spaces will not simply resolve itself, but rather will require concerted effort.

The latest examples of regulatory challenges related to policy fragmentation are incompatible data protection requirements and data residency requirements for certain types of data. For instance, a recent ruling from the EU Court of Justice[76] declared the data protection agreement between the US and the EU, known as *Privacy Shield* (→ Privacy Shield), to be invalid. As a result, the Federal Data Protection and Information Commissioner (FDPIC) declared that the equivalent *Swiss-US Privacy Shield* no longer met the requirements for an appropriate level of protection according to Swiss data protection legislation.[77] For this reason, the mismatch between the EU and the US strategy also constitutes a challenge for Switzerland. These developments are not only confined to personal data, however.

In addition to privacy protection measures, calls for data residency requirements – also known as data localisation (→ data localisation) – are growing stronger on a global level. Data localisation refers to mandatory legal and administrative guidelines that stipulate that data must be stored or processed in a certain country.[78] There are various reasons for data localisation measures: security concerns (e.g., cybersecurity, national security) play a role, as does the ability to enforce regulatory and legal requirements. Creating a geopolitical or economic advantage is also a consideration.[79]

While there can certainly be legitimate political reasons for restricting the cross-border flow of data, developments such as data localisation lead to new hurdles and increase the fragmentation of digital policy.[80]

6.3 Interoperability

If we are to bridge the gap between different data policy approaches and the fragmentation that results, there needs to be a model for creating interoperability between international data spaces. The ability of data spaces to communicate and interact with one another despite being founded in different locations or for different sectors is referred to as interoperability. According to the European Interoperability Framework (EIF), interoperability has four different aspects: technical, semantic, organisational and legal.[81] These can also be categorised as **specific interoperability** and **general interoperability.**[82]

[76] *EU Court of Justice (2020)*, "Data Protection Commissioner vs. Facebook Ireland Limited and Maximilian Schrems".
[77] *FDPIC (2020)*, "Policy paper on the transfer of personal data to the USA and other countries lacking an adequate level of data protection within the meaning of Art. 6 para. 1 FADP".
[78] Here there is a distinction to be made between exclusive localisation measures (e.g., where no copies of the data in question can leave the jurisdiction) and non-exclusive localisation measures (e.g., a copy of the data in question must always remain within the jurisdiction).
[79] *Svantesson D. (2020)*, Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines, p. 14.
[80] *Svantesson D. (2020)*, Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines, p. 13.
[81] *European Commission (2017)*, "New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations".
[82] *Goldstein E., Gasser U. and Budish R. (2018*), "Data Commons Version 1.0: A Framework to Build Toward AI for Good – A Roadmap for Data" from the 2018 AI for Good Summit.

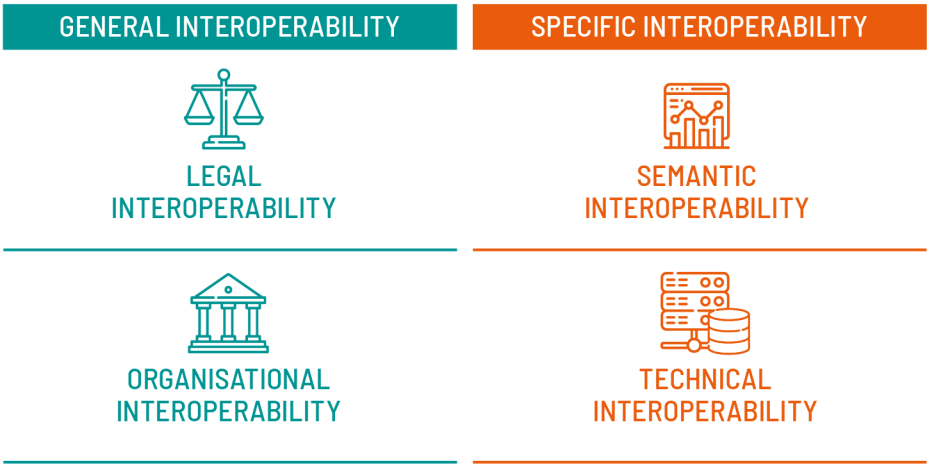

Figure 4: Levels of interoperability[83]

Specific interoperability describes the technical and semantic communication capacity between data spaces. One level of this is compatibility between technical infrastructures. To this end, application systems can be equipped with an appropriate electronic interface (API), for instance, to make data exchange as simple and efficient as possible. Another level is compatibility between data on a semantic level: it needs to be stored and described in such a way as to be readable by other data spaces. In other words, the format and content of the data being exchanged needs to remain intact and interpretable.

Standards are an important aspect of specific interoperability. Standards for data collection, storage, preparation and exchange make it possible for data to be used in different spaces and for different purposes. Uniform metadata standards that correctly record and describe the format and content of data are another relevant aspect for semantic interoperability. One example of this is the i14y interoperability platform,[84] which is part of Switzerland's national data management programme (NaDB). The platform has already integrated aspects of semantic interoperability into its governance, harmonisation processes and planned federal API catalogue. Standards are either developed for a specific project (such as a new data space), which allows for flexibility and specific adaptations, or existing standards are adopted.[85] The major advantage of adopting existing standards is that it guarantees interoperability with all other systems that also use these standards. Adopting existing standards is therefore preferable from an interoperability perspective. There are currently various international bodies dedicated to setting standards: ISO/IEC, IEEE, IETF, ITU and W3C. On a European level, there are CEN and ETSI, and for data spaces in particular, Gaia-X and IDSA.

Interoperability between data spaces is not limited to technical questions, however. There is a need for certain legal and societal conditions as well as interoperability on an organisational level so that data can circulate beyond the borders of any one particular space without too much administrative effort. This aspect is referred to as **general interoperability**.

Technical standards have an important function when it comes to general interoperability: they help implement legal and ethical guidelines and assuming they are adopted on a wider scale, allow for simplified compatibility between different national legal and regulatory systems. Over the past several

[83] Graphic based on *European Commission (2017)*, "New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations".
[84] See also <www.i14y.admin.ch> (accessed on 04.03.2022).
[85] *Collovà P. et al. (2021)*, "Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung", p. 23.

years, challenges have increasingly arisen regarding fundamental differences in regulatory approaches to data policy. This is in addition to legal questions, for instance regarding data protection and intellectual property (see Chapter 6.1). Societal values and geopolitical interests play a central role here. The population needs to be able to trust that data of all kinds is not being misused abroad or that their data is not less protected once it crosses national borders.

Applying a general interoperability approach allows for international data spaces with different structures to be connected. Increased cooperation and coordination between legal systems, in the form of bilateral agreements or other international instruments if necessary, allow for certain challenges to be overcome and for the elimination or minimisation of restrictions on the flow of data. This is possible primarily when dealing with like-minded partners. Major challenges remain on a global level, however. Here, there is a need to develop new approaches that can bring about general interoperability without undermining Switzerland's fundamental principles and values.

6.4 Interim conclusion

International data flows hold enormous potential. Switzerland and many other countries are therefore striving to harness the potential of this data for their societies and economies and to take appropriate steps to strengthen the trust of the population when it comes to dealing with data. Over the past several years, awareness has grown regarding how political and regulatory fragmentation on data issues is hindering this potential. As a result, there are increasing calls for new, effective international frameworks and a functioning governance structure in order to discuss challenges and develop joint solutions to issues surrounding general interoperability.[86]

Various commenters have already pointed out that despite ongoing work being done in international trade (e.g., multilateral negotiations on e-commerce at the WTO) there are still extensive differences in digital governance – both procedurally and in terms of content.[87] Over the medium and longer term, this threatens to lead to ever-increasing fragmentation on data policy questions, thereby creating additional hurdles for cross-border data exchange. With this in mind, making dogmatic demands is not beneficial: neither data localisation nor a completely free flow of data will be able to fulfil different political goals and expectations. What is needed instead are new approaches that strike a balance between the extremes.

By advocating for its vision of digital self-determination, Switzerland can make an important contribution to ongoing discussions about digital governance. Digital self-determination is clearly part of a value- and people-oriented approach, but it can also satisfy other concerns thanks to the fact that it includes not only individuals but also companies and society as a whole. By pursuing a digital self-determination approach, Switzerland is addressing various concerns that are reflected in the three data policy models described above. Even though Switzerland's goals are closest to those of the EU, Switzerland's vision of digital self-determination adds a new dimension to the discussion with the EU as well. In order to help shape digital governance to include the values of digital self-determination, Switzerland can promote this vision beyond its borders and help cement the concept on an international level.

This needs to occur on two levels, both in terms of norms and operationally:

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

1. When it comes to **norms and concepts**, Switzerland wants to explain the relevance and importance of the concept of digital self-determination and work together with like-minded actors to advocate for this idea. The goal is to establish *digital self-determination as a guiding principle for data governance (→ data governance) on an international level*. To this end, Switzerland will continue supporting and developing the relevant bodies and processes for international governance and establishing new ones where necessary. We should use existing synergies in Geneva for these discussions wherever possible. On a substantive level, other organisations should be used in which similar topics are already established (e.g., Council of Europe or OECD).
2. In terms of **operations**, Switzerland would like to join forces with like-minded actors to help realise the principles of digital self-determination and implement trustworthy data spaces. Activities in this area are aimed at practical measures *for establishing interoperable and transnational data spaces*. Drafting international guidelines for data space operators should be useful in this regard. Existing or planned initiatives such as projects connected to the national data management programme (NaDB) should also be taken into consideration. The first step is to identify like-minded partners from all stakeholder groups.

7 Recommendations for action

Digital self-determination can be implemented in different ways. This report focuses on establishing trustworthy data spaces. When observing how these spaces work, one sees that there are two roles in particular that have great influence: the party responsible for operating the technical infrastructure and the institution responsible for the governance.[88] These roles are a crucial starting point for creating trustworthy data spaces and ensuring adherence to the basic principles.

Although there are efforts underway in diverse areas (e.g., mobility, energy) to define appropriate cross-sector parameters for data spaces, these efforts must be intensified in order to promote data usage and counteract certain tendencies (such as the concentration of data in the hands of a few players) while also creating transparency, trust and additional control for users.[89] Without adopting countermeasures, existing challenges will intensify and trust in how data is used will be further eroded.

We should not underestimate the importance of the developments that will take place over the next several years. The data spaces being established now will set the standards for how we as a society make use of data spaces and how we handle the large-scale exchange of data in the future. Measures taken by Switzerland can also point the way forward and help promote the development of data spaces on the basis of the principles outlined in this report.

This raises the question of what role public authorities should play in connection with digital services. Initially, a wide variety of governmental forms of action are conceivable, ranging from the issuance of recommendations (cf. the code of conduct proposed here), through to numerous intermediate stages such as subsidies and strict legal regulation of all aspects. From today's perspective, two approaches are paramount:

[88] These two roles can also be held by the same party, with the same entity that runs the technical infrastructure also bearing responsibility for its governance. This is referred to as a data space operator (see Appendix 2).
[89] *Collovà P. et al. (2021)*, "Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung"; *Jentzsch N. (2017)*, "Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds – Ökonomische Rahmenbedingungen innovativer Lösungen zu Einwilligungen im Datenschutz".

1. **Acting as a service provider:** The public sector can act as a service provider of a public institution and guarantee the necessary services related to trustworthy data spaces. In this case, public authorities would also establish the necessary regulations in the form of legislation through the political process.
2. **Defining an appropriate framework:** The public sector can define a framework for steering developments in a politically desirable direction and preventing unwanted developments. This involves defining principles for how trustworthy data spaces should be organised and operate, and monitoring them for compliance. The initial phases of this process should however emphasise a self-regulatory approach in order not to hinder innovation and development.

Having the **state as a service provider**– meaning that the public sector exclusively runs data spaces for private companies and individuals or competes with private actors in doing so – is neither realistic nor desirable in at least a few sectors. In many cases, a competitive liberal approach is more likely to lead to a range of options that can react with flexibility to different needs. However, there are areas – networked mobility, for instance – where it would be politically opportune and desirable for the public sector to take on a particular role or cover basic needs as a public service. The distribution of competences between the Confederation, cantons and municipalities must be considered, and the necessary legal foundations must be created. The Federal Council is aware of these developments and has commissioned OFCOM with drafting a report on the development of digital public services. The report is scheduled for publication in June 2022.

Academic literature considers it sensible to create or shape **an appropriate framework** through legislation or other, less binding means.[90] Such frameworks are already in place in certain network-dependent sectors such as telecommunications, energy, mobility and the postal service, and establishing similar structures for data spaces would also be necessary. By taking on this role, public authorities can set goals in line with the public interest and promote these goals with the appropriate measures. The Swiss federal government should define the basic parameters for how to organise and operate data spaces and monitor them in this regard. These parameters should maximise the potential of data while also minimising negative trends. One should bear in mind that in certain circumstances, for example depending on the sector or the parties involved, there are limitations to this approach that will need to be accepted. This means that it is important to have ongoing monitoring and evaluation of the parameters to determine if they are still beneficial or if further steps need to be taken. In addition to regulation, the state also has the role of enforcing the rules that it creates. The specific design of enforcement mechanisms should provide for effective means of reporting and responding to violations of legitimate claims by data space operators or data-using organisations.

7.1 Introducing a regulatory framework

Developments in the area of data space are still in their infancy. In some sectors, data spaces are just starting to appear, and not all the challenges are yet known. Even though creating a regulatory framework for data spaces appears sensible at first, having comprehensive horizontal regulation in this context would not be beneficial at this time. This does not mean, however, that particular sectors or subsectors cannot or should not develop any approaches to regulation: this may indeed be appropriate depending on the situation, even today.

[90] *Collovà P. et al. (2021)*, "Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung".

Having a coordinated self-regulatory approach on a national and horizontal level appears to be the most suitable for the current situation, however. Here, the federal government should work together with relevant stakeholders to set out a voluntary framework. This would create a situation where pioneering measures can be introduced without limiting innovation. As a first step, the federal government should coordinate the creation of a voluntary **code of conduct** for trustworthy data spaces in cooperation with the relevant players. The *code of conduct* should also spell out the previously described basic principles for data space operators (see Chapter 4). Here, attention must be paid to the special characteristics and conditions of particular sectors (especially for sectors that have to adhere to certain international standards). There are many elements that can come into play for a *code of conduct*. The recommendations for the basic principles (see Appendix 3) can serve as a guide here. The national Digital Self-Determination Network would be a fitting platform for the project of drafting this code of conduct. It should be possible to monitor whether the code is being adhered to via monitoring and self-reporting mechanisms. It should be clarified whether adherence to the *code of conduct* should be mandatory for the federal government.

The government's next steps will depend on the success of the voluntary *code of conduct*. This means that developments related to the *code of conduct* need to be closely monitored, and the government will need to review whether its key goals are achieved. Furthermore, there should be regular evaluations of whether a self-regulatory approach advances the desired goals or whether other forms of regulation should be considered.

7.2 Establishing a Swiss data hub and promoting interoperability

On a European level, the joint German-French project *Gaia-X* acts as a reference point for establishing cross-sector and cross-border data spaces. Gaia-X is one part data space-focused, one part infrastructure-focused. For the data space part, Gaia-X wants to create common standards, a common register, a common catalogue of services, etc. in order to create the technical conditions for building data spaces on a common foundation of interoperability at their inception. This interoperability should ensure that it is possible to exchange data between different industries and across national borders.

National data hubs should act as central points of contact for a particular country's businesses, research institutes, associations and public authorities who are interested in creating and using data spaces. A comparison with existing national hubs in Europe shows that they have a variety of structures, chiefly regarding the extent of state involvement (ranging from full financing from the government to partial financing from public contributions) and the role of the public authorities (ranging from taking on a national leadership role to simply coordinating contact between interested parties). Most existing hubs share the trait of not having been specifically created for Gaia-X but rather as general points of contact for questions about data spaces.

As described in Chapters 5 and 6, it is also in Switzerland's interest for data spaces to be interoperable across sectors and national borders. The public authorities are already working to bring this about with the DataHub4Gov project and the national data management programme (NaDB).[91] The question still remains, however, whether Switzerland should create a general point of contact for all parties who are interested in how to design and structure a data space. One could be based on existing coordination

[91] *Digital public services (2022)*, "Developing and managing the eGovernment architecture for the strategic implementation plan".

and innovation offices that already deal with individual aspects of data spaces: the Delegate for Digital Transformation and ICT Steering, the Digital Public Services Switzerland Officer, the Data Science Competence Centre (DSCC), the Coordinating Agency for Federal Geographic Information (GCG) and the national Digital Self-Determination Network as well as intercantonal bodies. A national **Swiss data hub** could connect these existing bodies and act as a central point of contact for all stakeholders with questions about data spaces. It could connect relevant stakeholders, provide guidance on drafting a *code of conduct* (see Chapter 7.1), disseminate the code of conduct and in doing so support the establishment of trustworthy data spaces. The Swiss data hub would also ensure that there are connections to international data space projects such as Gaia-X or the international Digital Self-Determination Network.

The hub will need to deal with the question of how to make data spaces currently in the build-up phase compatible with each other, both nationally and internationally. Here, the experience of existing data spaces (e.g., the geodata space) and data spaces under development should be called on, for instance in the mobility and energy sectors. These approaches and insights could be useful for drafting the code of conduct and for guiding the activities of a potential Swiss data hub.

7.3 International measures

The flow of data across borders holds enormous potential and can help the Swiss economy achieve more growth. In accordance with Switzerland's foreign economic policy and its data protection legislation, steps should be taken to ensure that Swiss companies have convenient access to international markets, particularly the EU's single market. Political and regulatory fragmentation in the data policy landscape is a roadblock to this goal, however (see Chapter 6.2). For this reason, Switzerland needs to increase its international involvement in data governance issues. Swiss digital foreign policy constitutes an important first step, but additional concrete measures are needed. More uniformity in international data governance (→ international data governance) is required in order to create general interoperability between data spaces. Switzerland has a clear vision here – digital self-determination – and will need to advocate for this vision more strongly, also on an international level. Digital self-determination can then serve as a basis for concrete solutions to data policy challenges. To this end, Switzerland needs to identify suitable partners and to support and develop relevant processes and bodies, or create new ones where required. Wherever possible, Switzerland should consider International Geneva as a platform for global data and digital policy. Furthermore, Switzerland has started working on establishing an international digital self-determination network as a corollary to the domestic organisation. The current participants are from academia, with plans to include participants from the public and private sectors as well. The international network is currently employing concrete *use cases* in various sectors to test and develop the concept of digital self-determination on an international level.

International standards are an important aspect of interoperability. In addition to governance issues, it is essential to make progress on questions of standards. Ongoing projects related to strengthening standards and norms should address the importance of data spaces (see also the review of the EAER (SECO) together with the FDFA, the FDF (FOBL) and DETEC (OFCOM) on efforts to promote international norms organisations). Furthermore, we should promote the development of standards for trustworthy data spaces in cooperation with existing organisations for norms and standardisation.

Over the longer term, it will be necessary to establish international guidelines for trustworthy data spaces and digital self-determination in order to create legal certainty on an international level. This is in Switzerland's interest as a mid-sized, highly networked economy. The first step is to identify like-minded partners. Switzerland should aim to have the principles of digital self-determination and the national code of conduct reflected as much as possible in the global guidelines it creates with these partners.

8 Glossary

This glossary consists of working definitions taken from various sources that have not been individually cited.

Algorithm	A clear rule for action to solve a problem that consists of a finite number of clearly defined individual steps, allowing it to be executed by a computer programme.
Anonymisation	Process in which → *data* is changed to make it untraceable back to an identifiable natural person or a natural person who could potentially be identified, or a process in which → *personal data* is processed in such a way as to make the person in question unidentifiable or only identifiable with a disproportionate amount of effort or legally forbidden means.
Application Programme Interface (API)	Programming interface that connects one software system to another. See also → *interfaces*
Closed data	→ *Data* that is only accessible under strict lock and key by a limited circle of users within a company or administrative organisation. Only data controllers have access.
Cloud	Model of data processing in which a shared pool of configurable computing resources (e.g., networks, servers, storage systems, applications and services) can be accessed at any time, from anywhere and whenever needed via a network. Clouds can be made available quickly and with a minimum amount of administrative effort or interaction with the service provider.
Collective data use	Once → *data* is collected, it can be used for other purposes or by other people or organisations. See also: → *data sharing*.
Data	In an IT and data processing context, data is understood to be information, usually represented in a digital format, that can be read and processed (by a machine).
Data bias	Phenomenon in which skewed data leads to a gap between a person's real and digital selves.
Data as a commodity	→ *Data* used for business/economic purposes.
Data as infrastructure	The totality of → *data* that comprehensively depicts a sector or subsector (e.g., mobility or electromobility). This data is mandatory for the functioning of a system (e.g., mobility system in Switzerland).
Data as a public good	→ *Data* that is made available to the general public because it is considered to be part of the common good. Because of its accessibility, data of this kind is necessarily considered to be → *open data*. It is always non-personal in nature.
Data sharing	→ *Shared data*
Data provider	→ *Data supplier*

Data processing	Every action taken with → *data* (both → *personal data* as well as → *non-personal data*), regardless of the tools or processes used, particularly acquiring, saving, storing, using, changing, publishing, archiving, deleting or destroying data.
Data governance	The establishment, design and strengthening of institutional systems, sets of rules and mechanisms within the data community. See also → *international data governance*.
Data infrastructure	The necessary technical and organisational systems and structures for exchanging → *data* or making it useable.
Data supplier	Legal or natural persons who offer or provide → *data* via → *data infrastructure.*
Data localisation	Mandatory legal and administrative guidelines that stipulate that data must be stored or processed in a certain country.
Data intermediaries	Providers or services for shared data use. A type of → *intermediary* or 'middleman' that works exclusively with data.
Data network effect	See → *network effect*
Data user	Legal or natural persons who use→ *data* for a specific purpose.
Data set	A collection of → *data* that belongs to a particular object and that is stored in a file.
Data producer	Natural or legal persons who generate and record → *data*.
Data quality	Evaluation of → *data* regarding its suitability to fulfil a certain purpose. Criteria include correctness, relevance and reliability as well as consistency and availability on different systems.
Data space	Technical and organisational structure that facilitates and governs the availability, exchange and collection of → *data* from various sources and actors. Often specific to a certain sector and defined by its purpose, clear rules and → *standards*. Run by a → *data space operator*.
Data space operator	Responsible for a → *data space.* The term only applies if the same organisation is responsible both for the technical infrastructure as well as the governance of the data space.
Data custodian	A data custodian can be entrusted with the task of developing and implementing standardised access to → *data* for approved entities. Additionally, data custodians have an advisory role towards users and offer various services depending on their focus, e.g., managing data in the interests of users. Data custodians can also assert the interests and decision-making rights of a variety of consumers when it comes to data privacy.
Data cycle	Lifecycle of → *data*, from availability and accessibility to processing, exchange and reuse to deletion, freezing or archiving.
Differential privacy	Disguising → *data* so that identifying a specific person would only be possible with a certain defined probability, even if using third-party data.
Digital divide	Describes inequalities in accessing and using digital technologies.
Digital value chain	Three elements make up the value chain: → *data,* → *information*, → *knowledge*. At every step along the chain – as data transitions into

	information and as information becomes knowledge – more value is created, both socially and economically.
Dynamic data	→ *Data sets* that change as soon as new information is available (the temporal aspect of data). In contrast with → *static data.*
Governance	Efficient mechanisms that set out common rules (including the regulation of responsibilities and risks) for accessing, exchanging or using data. See also → *data governance* and → *international data governance*.
Information	The result of linking → *data* together. Data that takes on meaning by being decoded or interpreted.
Informational autonomy	The right and/or possibility and ability of a person to fundamentally decide on their own about revealing, collecting and using → *personal information/data* as well as having control over their 'digital double'. Basic entitlement of every person to have their personal data protected from abuse (from Art. 13 para. 2 Cst.).
Interfaces	Part of a software system that facilitates communication with other systems or other parts of a system. Usually involves functions that return an extract of data in a standardised format in response to a parameterised query.
Intermediary	Institutions that act as 'middlemen' who facilitate access to → *data* and broker its flow from its source to other users. Intermediaries are the uppermost category and include institutions with trustee and/or marketplace functions as well as other methods of brokering data.
International data governance	Development of an institutional and regulatory system alongside international cooperation mechanisms with the aim of overcoming global problems and cross-border issues. Venues include the UN system, international organisations, IGOs and NGOs and regional organisations.
Interoperability (general and specific)	The ability of different systems, technologies or organisations to work together, usually based on common → *standards*. Sales and distribution systems, for instance, are interoperable if they can be connected to each other via → *standardised interfaces* that make it possible for one system to acquire products from another participating system. *Specific* interoperability describes the technical ability of → *data spaces* to communicate with each other. *General* interoperability includes legal and societal parameters that allow → *data* to circulate beyond the borders of any one particular data space without too much administrative effort.
Knowledge	Result of analysing → *information* or → *data* based on a framework, theory or certain perspective. It is only by applying a particular perspective that data or information becomes an intelligible basis for action.
Multi-sided markets	A company that is active in a multi-sided market usually serves at least two different groups of customers (who constitute the different 'sides' of the market). Furthermore, the definition often requires there to be indirect → *network effects* between these various groups of customers.

Network effect	Describes the phenomenon by which a product or service becomes more valuable or beneficial the more users it has. In a → *data* context, the → *data network effect* describes the phenomenon that when data is used for innovation, it in turn generates more data that can improve the product or service.
Non-personal data	→ *Data* that is not personal in nature and that is therefore not covered by data protection law.
Open data	Freely accessible → *data* that can be used for any purpose, including commercial purposes, and that can also be modified and made available to third parties. Open data is provided for free or at a minimal charge.
Open government data	Administrative data provided by the public sector in the form of → *open data*.
Personal data	Details, → *information* and statements that refer to a particular person or person who could be identified from said information. A legal definition is included in Art.3 let. a FADP.
Personal data requiring special protection	Data requiring special protecting due to elevated risk of violating a person's privacy, e.g., health data. A legal definition is included in Art. 3 let. c FADP.
Platforms	A specific model of data use in which a single company collects, collates and performs in-house analysis of→ *data* which has been generated on a platform (usually international in nature). This is then used to offer services to customers on different marketplaces. The services are based on the collection and analysis of data on all three marketplaces. A platform can also be a → *data space* but does not have to be.
Profiling	Every type of automated processing of → *personal data* that involves evaluating, analysing or predicting factors related to an individual person such as their performance, financial situation, health, personal preferences, interests, reliability, behaviour, and location or location changes. A legal definition will be spelled out in Article 5 let. f revFADP.
Privacy by design	Overarching principle and starting point. In essence, responsible parties should consider early on how they can comply with data protection requirements during the entire → *data life cycle.*
Privacy Shield	The Privacy Shield is a legal framework for sending personal data from Switzerland to the US (Swiss-US Privacy Shield) or from the EU to the US (EU-US Privacy Shield).
Privacy paradox	Commonly observed phenomenon where people's actual behaviour regarding revealing their personal → *data* is not in line with the intrinsic preferences that they express when they are faced with an immediate situation online.
Pseudonymisation	Processing → *personal data* in such a way that it cannot be traced to a specific person without drawing on additional information, as long as this additional information is stored separately and subject to technical and organisational measures that ensure that it cannot be connected with a particular natural person or identifiable natural person. One example is replacing names with ID numbers and outsourcing the table that assigns numbers to names.
Shared data	→ *Data* that is prepared for certain groups or only under certain conditions.

Standards	Consistent, established and documented agreement on the structure and format of shared → *data*, → *interfaces* and processes.
Standardisation	Development of → *standards*.
Static data	→ *Data* in a fixed → *data set*, i.e., data that remains unchanged after it is generated and recorded (the temporal aspect of data). In contrast with → *dynamic data.*
Vertical integration	Describes the up- or downstream integration of value-adding steps in a company that were previously provided by other market players.

9 List of abbreviations

AI	Artificial intelligence
API	Application Programme Interface
Art.	Article
CC	Swiss Civil Code (SR 210)
CEN	European Committee for Standardization
CO	Federal Act on the Amendment of the Swiss Civil Code (Part Five: Code of Obligations) (SR 220)
Cst.	Federal Constitution of the Swiss Confederation (SR 101)
DDPS	Federal Department of Defence, Civil Protection and Sport
DETEC	Federal Department of the Environment, Transport, Energy and Communications
DIL	Directorate of International Law
DPPE	Swiss Conference of Directors of Public Works, Planning and Environmental Protection
DSCC	Data Science Competence Centre
EAER	Federal Department of Economic Affairs, Education and Research
ECHR	European Convention on Human Rights (SR 0.101)
EDK	Swiss Conference of Cantonal Ministers of Education
EIF	European Interoperability Framework
EPR	Electronic Patient Record
EPRA	Federal Act on the Electronic Patient Record (SR 816.1)
ETSI	European Telecommunications Standards Institute
EU	European Union
FADP	Federal Act on Data Protection (SR 235.1)
revFADP	revised Federal Act on Data Protection
FDF	Federal Department of Finance
FDFA	Federal Department of Foreign Affairs
FDPIC	Federal Data Protection and Information Commissioner
FHIR	Fast Healthcare Interoperability Resources
Fintech	Financial technology
FOBL	Federal Office for Buildings and Logistics
FOT	Federal Office of Transport
GCG	Coordinating Agency for Federal Geographic Information
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and communications technology
IDSA	International Data Spaces Association
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
IPI	Swiss Federal Institute of Intellectual Property
ISO	International Standards Organisation
IT	Information technology
ITU	International Telecommunication Union

let.	Letter
MODIG	Federal Act on Mobility Data Infrastructure
MRI data	Magnetic resonance imaging data
NADIM	National data infrastructure in the mobility sector
OECD	Organisation for Economic Cooperation and Development
OFCOM	Federal Office of Communications
p.	Page
para.	Paragraph
SATW	Swiss Academy of Engineering Sciences
SERI	State Secretariat for Education, Research and Innovation
SDA	Swiss Data Alliance
SECO	State Secretariat for Economic Affairs
SFOE	Swiss Federal Office of Energy
SHED	Swiss Hub for Energy Data
SIF	Secretariat for International Financial Matters
SME	Small or medium-sized enterprise
UNCTAD	United Nations Conference on Trade and Development
UNGA	United Nations General Assembly
US	United States
W3C	World Wide Web Consortium
WTO	World Trade Organization

10 List of sources

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

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

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

Collovà P. et al. (2021), "Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung", Bern University of Applied Sciences

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

Digital public services (2022), "Developing and managing the eGovernment architecture for the strategic implementation plan", <https://www.digital-public-services-switzerland.ch/en/implementation/egovernment-implementation-plan/developing-and-managing-the-egovernment-architecture-for-the-strategic-implementation-plan> (accessed on 04.03.2022)

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

EU Court of Justice (2020), "Data Protection Commissioner vs. Facebook Ireland Limited and Maximilian Schrems", <https://curia.europa.eu/juris/liste.jsf?num=C-311/18> (accessed on 03.01.2022)

European Commission (2016), "Study on Data Sharing between Companies", <http://publications.europa.eu/resource/cellar/2d6d436e-4832-11e8-be1d-01aa75ed71a1.0002.01/DOC_1> (accessed on 03.01.2022)

European Commission (2017), "New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations", <https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf> (accessed on 01.02.2022)

European Commission (2018a), "Towards a common European Data Space", <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0232&from=EN> (accessed on 03.01.2022)

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

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

FDPIC (2020), "Policy paper on the transfer of personal data to the USA and other countries lacking an adequate level of data protection within the meaning of Art. 6 para. 1 FADP", <https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/Positionspapier_PS_%20ED%C3%96B_EN.pdf.download.pdf/Positionspapier_PS_%20ED%C3%96B_EN.pdf> (accessed on 03.01.2022)

Federal Council (2019), "Health policy strategy 2020-30", <https://www.bag.admin.ch/bag/en/home/strategie-und-politik/gesundheit-2030/gesundheitspolitische-strategie-2030.html> (accessed on 03.01.2022)

Federal Council and DPPE (2020), "Strategie Geoinformation Schweiz", <https://www.geo.admin.ch/de/ueber-geo-admin/leistungsauftrag/strategie-und-umsetzung.html> (accessed on 03.03.2022)

Federal Council (2020a), "Foreign Policy Strategy 2020-23", <https://www.eda.admin.ch/content/dam/eda/en/documents/publications/SchweizerischeAussenpolitik/Aussenpolitische-Strategie-2020-23_EN.pdf> (accessed on 03.01.2022)

Federal Council (2020b), "Strategy Digital Switzerland", <https://www.digitaldialog.swiss/en/> (accessed on 03.01.2022).

Federal Council (2020c), "Digital Foreign Policy Strategy 2021-24", <https://www.eda.admin.ch/content/dam/eda/en/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_EN.pdf> (accessed on 03.01.2022)

Federal Council (2021), "Botschaft zum Bundesgesetz über eine sichere Stromversorgung mit erneuerbaren Energien vom 18. Juni 2021", Federal Gazette 2021, 1666 et seq.

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

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

FOT (2022), "Erläuternde Bericht zum Bundesgesetz über die Mobilitätsdateninfrastruktur (MODIG)", <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2022/2/cons_1/doc_5/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2022-2-cons_1-doc_5-de-pdf-a.pdf> (accessed on 03.02.2022)

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

Ghielmini S. et al. (2021), "Grund- und Menschenrechte in einer digitalen Welt", Swiss Centre of Expertise in Human Rights, <https://www.skmr.ch/cms/upload/pdf/2021/210518_Grund_und_Menschenrechte_in_einer_digitalen_Welt.pdf> (accessed on 03.01.2022)

Goldstein E., Gasser U. and Budish R. (2018), "Data Commons Version 1.0: A Framework to Build Toward AI for Good – A Roadmap for Data from the 2018 AI for Good Summit", Berkman Klein Center, <https://medium.com/berkman-klein-center/data-commons-version-1-0-a-framework-to-build-toward-ai-for-good-73414d7e72be> (accessed on 01.02.2022)

Häfelin U. et al. (2020), "Schweizerisches Bundesstaatsrecht", Schulthess, Zurich/Basel/Geneva

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

IPI (2021), "Zugang zu Sachdaten in der Privatwirtschaft", <https://www.ige.ch/fileadmin/user_upload/recht/gesellschaft/d/20210301_Bericht_IPI_Zugang_zu_Sachdaten_in_der_Privatwirtschaft.pdf> (accessed on 03.01.2022)

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

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

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

OFCOM, FDFA, SDA & SATW (2020), "Discussion paper on digital self-determination", <https://digitale-selbstbestimmung.swiss/home/245-2/> (accessed on 03.01.2022)

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

Schneider I. (2019), "Governance der Datenökonomie: Politökonomische Verfügungsmodelle zwischen Markt, Staat, Gemeinschaft und Treuhand"; Ochs C. et al. (pub.), "Die Zukunft der Datenökonomie: Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz", Springer VS, Wiesbaden, p. 143-180

SID (2022), "Digital Finance: Handlungsfelder 2022+", <https://www.newsd.admin.ch/newsd/message/attachments/70095.pdf> (accessed on 02.02.2022)

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

Swiss Bankers Association (2020), "Open Banking: An overview for the Swiss financial centre", <https://www.swissbanking.ch/_Resources/Persistent/8/8/2/8/88286724aa4fdc3dd8bb8ecd9b9c0d7af659a803/SBA_Overview_OpenBanking_en.pdf> (accessed on 03.02.2022)

Swiss Economics (2021), "Vertrauenswürdige Digitale Datenräume: Schlussbericht Konzeptualisierung und Anforderungen" (available to author team)

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

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

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

Appendix 1: Overview of relevant reports

Topic	Title	Responsible federal office	Date
Data policy in general	Bericht Auslegeordnung Datenpolitik (*Report: Overview of data policy*)	OFCOM	June 2016
	Eckwerte einer Datenpolitik (*Cornerstones of data policy*)	OFCOM	May 2018
	Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit (*Expert report on the future of data processing and security*)	Expert group	September 2018
	Zugang zu Sachdaten in der Privatwirtschaft (*Access to non-personal data in the private sector*)	IPI	February 2021
Data policy by sector	Daten in der Bildung – Daten für die Bildung: Grundlagen und Ansätze zur Entwicklung einer Datennutzungspolitik für den Bildungsraum Schweiz (*Data in education, data for education: foundations and approaches to developing a data use policy for the educational sector in Switzerland*)	Educa, commissioned by SERI and EDK	May 2019
	Strategie Geoinformation Schweiz (*Geoinformation strategy for Switzerland*)	Federal Council and DPPE	December 2020
	Data Hub Schweiz – Kern zukünftiger Dateninfrastrukturen digitalisierter Strom- und Gasmärkte (*Data hub Switzerland – the core of future data infrastructure for digitalised energy and gas markets*)	SFOE	August 2021
	Digital Finance: Handlungsfelder 2022+ (*Digital finance: Areas of action 2022+*)	SID	February 2022
	Bericht zum Bundesgesetz über die Mobilitätsdateninfrastruktur (*Report on the Federal Act on Mobility Data Infrastructure*)	FOT	February 2022
Digital policy	Bericht Intermediäre und Kommunikationsplattformen (*Report on intermediaries and communication platforms*)	OFCOM	November 2021
	Bericht Digitaler Service Public (*Report on digital public services*)	OFCOM	Q3 2022
Digital infrastructure	Bedarfsabklärung Swisscloud (*Swisscloud needs analysis*)	FITSU	December 2020
	Prüfaufträge Swisscloud (*Swisscloud audits*)	FDFA	June 2021
AI	Bericht der interdepartementalen Arbeitsgruppe Künstliche Intelligenz (*Report by the interdepartmental*	SERI	December 2019

	working group for artificial intelligence)		
	Leitlinien Künstliche Intelligenz für die Bundesverwaltung (*Guidelines on artificial intelligence for the Federal Administration*)	OFCOM	November 2020
	KI und Völkerrecht (*AI and international law*)	FDFA	Q2 2022

Appendix 2: Components of a data space

How a data space is operationalised and how it makes use of data depends on various components. Within a data space, various participants identify themselves, take on different roles and use different types of data for specific purposes. Furthermore, data spaces are based on different types of data infrastructure and governance forms. We will look at these components in closer detail in the following pages.[92]

1. Participants and roles in a data space

Within a data space, various participants identify themselves and take on different roles. The most important of these roles is operating and organising the data space. **Infrastructure operators** are responsible for making sure the technical infrastructure of the data space is functional. They can also offer services in connection with the data space, for instance analysis and additional processing for data sets (→ data set). In many data spaces, there is an additional role when it comes to **ensuring the governance** of the space – i.e., enforcing the rules and conditions for making use of the data.[93] We use the term **data space operator** if the same organisation is responsible both for the technical infrastructure as well as the governance. The types of governance (i.e., the rules of engagement for the data space) can also be defined by an overriding **trusteeship** – private or public – responsible for defining the functions of the data space operators.

In addition to operational and organisational roles, there are also other roles that can be identified which differ in whether they are on the **data supply** or the **data demand** side. Here the same participants can occupy several of the following roles:

Supply		Demand	
Data producer	Natural or legal persons who generate and record data.	**Data user/collector**	Natural or legal persons who use or obtain data from a data space.
Data provider (also: data supplier)	Natural or legal persons who provide data via a data space.		

These roles depend on the goals and purposes of the different parties participating in a data space. One actor can take on various roles. For instance, a hospital or patient can generate data from examinations, treatments and operations (→ data producer) and then make this data available for research purposes via a data space (→ data provider). At the same time, the hospital can use other data from the space in order to improve its systems (→ data user).

2. Types of data

The types of data can generally be distinguished based on various criteria. The report primarily focuses on the legal distinction between **personal and non-personal data**, on **static and dynamic data** (temporal aspect), and on **data in relation to its accessibility and the scope for which it is used**.

[92] For a graphical depiction of a data space model, please refer to Chapter 3.3.1.
[93] Data communities with collective governance are an exception to this principle.

An important distinction relates to the question of whether data has any *reference to individuals*, making it subject to data privacy legislation. **Personal data** is therefore any information that refers to a certain person or identifiable natural person (Art. 5 let. a, revised FADP). This type of data is explicitly protected by data privacy law. In contrast, **non-personal data** does *not* relate to specific individuals or identifiable natural persons. Unlike personal data, non-personal data is not regulated per se. It is important to mention that in reality it can sometimes be difficult to differentiate between personal data and non-personal data.[94] The reason is that it is often possible to trace data back to specific individuals when various sources of non-personal data or sets of non-personal data are combined. This development is accelerating due to the ever-increasing availability of data sets. For this reason, **anonymised** or **pseudonymised data** (→ pseudonymisation) is increasingly being used, the major advantage of which is that under circumstances it is possible to gain key insights without violating the privacy of individuals. However, it should be noted that anonymisation generally offers better protection than pseudonymisation with regard to possible re-identification. Mechanisms such as *differential privacy* pursue similar aims. In this approach, algorithms (→ algorithm) calculate statistically relevant information from a data set in such a way that it would be impossible to determine whether the data of a specific individual was in the original data set.

The *temporal aspect* of data is also growing in importance, with a distinction being made between **static** and **dynamic data** (→ static data; → dynamic data). Static data refers to data in a fixed data set, i.e., data that remains unchanged after it is generated and recorded. Dynamic data refers to data sets that change as soon as new information is available. This helps maintain the integrity of the data. It is noticeable, however, that there is a growing preference for dynamic data: this is due to its accuracy and because it offers the possibility to provide services that are personalised, individualised or otherwise tailored to the circumstances.

Furthermore, data can be broken down into different categories based on how accessible it is. Here a distinction is made between *closed data, shared data* and *open data* (→ closed data; → shared data; → open data). **Closed data** refers to personal and non-personal data that is only accessible under strict lock and key by a limited circle of users within an organisation (e.g., a company's market-related data). **Shared data** refers to personal and non-personal data that can be shared with other actors or organisations under certain circumstances (e.g., for payment, within a particular governance framework). **Open data** refers to data that does not contain any information in need of protection and that is made available to the public to freely use. This category includes **open government data** (→ open government data) – i.e., public sector data that is made freely accessible.

Another distinction regards the scope for which data is used. This distinction is closely connected to the issue of data governance. Here we can distinguish between data as a *public good, data as infrastructure* and *data as a commodity* (→ data as a public good; → data as infrastructure; → data as a commodity). **Data as a public good** is data that is made available to the general public because it is considered to be part of the common good. This kind of data is always classified as *open data* and always concerns non-personal data. *Open government data* is one example of data in this category. **Data as infrastructure** is data that is considered essential for the guaranteed functioning of societally relevant systems (e.g., the mobility system in Switzerland). The distinction between *data as a public good* and *data as infrastructure* is not always clear cut. In some areas, *data as infrastructure* can also be

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

categorised as *data as a public good* and *open data* and be available to the public. *Data as infrastructure* can also be made available to a limited circle of users as *shared data*, especially if the data is sensitive in nature. **Data as a commodity** describes data that is used for business/economic purposes.

Distinction	Description		
Reference to individuals	Personal data	Non-personal data	
Temporal aspect	Dynamic data	Static data	
Level of accessibility	Open data	Shared data	Closed data
Scope for use	Data as a public good	Data as infrastructure	Data as a commodity

3. Purpose of data

Data is not valuable in and of itself but only becomes valuable when a specific purpose is identified (primary use). The first step is to identify this purpose: examples include using data to help develop healthcare solutions, to fight climate change or to improve mobility. By having a shared purpose of this kind, players within a certain sector can create incentives for shared data use, thereby opening up new opportunities.

In addition to this primary use – where data is harnessed for a specific aim – there is also great potential in making data available beyond its original purpose. This is referred to as secondary use, and it enables various actors in different sectors to make use of data at the same time for different purposes. This allows for innovation in areas that may not have even been considered previously. For instance, analysing a patient's MRI data can help develop a tailored approach to their treatment (primary use). Analysing a large amount of MRI data can yield general further insights for the healthcare sector and may even aid the development of new preventative therapies and treatments (secondary use).

Our example of MRI data, the various roles that can be held by participants in a data space, and the different types of data make it clear that data flows as part of a data cycle (→ data cycle). Data is generated and made available and accessible, and it is used, kept, re-used and exchanged for a specific purpose.

Where personal data are processed, the data protection law principle of purpose limitation must be observed.[95] In the case of data processing by state authorities, the processing purposes must be provided for in the applicable law. In the case of data processing by private individuals, they must be covered by the relevant justification (Art. 31 revFADP), notably by consent of the data subject.

4. Data infrastructure

Data spaces always require data infrastructure (→ data infrastructure). Depending on the distribution strategy, the infrastructure can be centralised or decentralised. This means that data is exchanged and stored (and potentially also processed) either via a special dedicated centralised structure, or this is done in a decentralised fashion directly between data providers and data users. Hybrid formats can also increasingly be observed, where parts of a space are decentralised (e.g., for certain data sets that can

[95] Art. 6 para. 3 revFADP: "Personal data may only be collected for a specific purpose which is evident to the data subject; personal data may only be processed in a way that is compatible with such purpose".

or must be maintained directly by the data provider) and other parts are centrally administered by the space operator (e.g., mostly for data sets that require additional preparation or that are subject to certain criteria for sharing).

5. Types of governance

Data spaces can be organised in various ways. This is why we see very different types of data spaces in practice (see Chapter 5). Each data space is organised according to specific parameters and rules that are defined and enforced by the governance of the data space. There is an important distinction to be made between data spaces that are open to everyone and data spaces that are exclusive to a few particular participants (see also *open data* and *shared data* above). In principle, however, different forms of governance can be applied to open data spaces as well as exclusive data spaces. It is difficult to categorise the types of governance in a uniform way because they are structured so differently and also use terms in different ways.[96] As a general rule, however, the approaches to governance can be broken down as follows:

Data cooperative	Organisation where members have equal say and control. Parameters, rules and enforcement are defined by all members, and compliance is reviewed in a transparent manner.
Data club	Organisation in which members have different levels of influence depending on their role and participation. Parameters, rules and enforcement are defined according to the roles.
Data community	Organisation in which data is mutually shared without the need for an operating organisation. Conditions of use are defined and enforced by the collective.

In addition to these forms of governance, there are also data spaces that place the concept of individual control right at their heart and are geared towards the needs of the individual. This mainly includes data custodians and personal data storage providers. They can also be integrated into larger data spaces, thereby strengthening the overall level of control.

Data custodian	Organisation that administers data in its capacity as an independent custodian (e.g., non-partisan, prudent, transparent and loyal) in the interests of the affected person. Acts as a representative of this individual and asserts their preferences directly in dealings with service providers or data spaces.
Personal data storage	Organisation that offers secure, independent data storage for an individual. Third parties can only access this data if explicitly allowed by the individual in question.

[96] *Collovà P. et al. (2021)*, "Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung", p. 27.

Appendix 3: Recommendations regarding basic principles for data spaces

Transparency

Recommendations on transparency

Scope

- The scope of the information provided should contain a certain minimum level of content (depending on the sector).
- Sufficient information on the business model of the data space operator and data usage should be made available so that participants are aware of the purpose for which their data is being processed.
- Information about which actors have access to which information should also be made known.

Clarity

- Information should be presented as clearly as possible and should be adapted to the target audience.
- Users should have access to processes and mechanisms that help them understand how their data is processed.
- Wherever possible, additional material should be provided (e.g., visual or audio-visual aids) in order to convey information in a low-threshold way.
- Potential risks should be communicated explicitly.

Effectiveness

- The information provided should be communicated in a proactive way and should be easy to find.
- The types and channels of communication should be adapted to the situation.

Monitoring

- Trustworthy data spaces should be public knowledge and should openly disclose their activities.
- Third parties should be able to assess the reliability and trustworthiness of data spaces and their operators.

Control

Recommendations on control

Control options

- Users should be able to decide which data they disclose, to whom they disclose it and when.
- Users should be able to limit the processing of their data wherever possible, especially for sensitive data.
- It should be possible to reverse any decisions to release data.
- Any consent given for using data should be limited in time and scope.

Free and voluntary choice

- Users should be able to choose their providers freely and to switch them without facing barriers.
- Participants should not face disadvantages or a worsening of their position on the basis of their decision.
- Users should also have the option of delegating the control and use of their data to third parties and to grant them the required powers.

Protection from loss of control

- There should be clear precautions and processes in place for recognising, controlling and mitigating security risks to the data space and its stakeholders.
- There should be a binding process in case the security of the data provided is compromised.

Fairness

Recommendations on fairness

Proportionality

- Data should always be processed according to the principle of proportionality.

Fair distribution of costs and benefits

- The costs and benefits of collecting, preparing and saving data should be fairly distributed.
- Participation in a trustworthy data space should yield specific added value for data producers and data users alike.

Freedom from discrimination

- Data spaces should be designed in a non-discriminatory fashion.

Independence

- The operations of a data space should be free of any conflicts of interest.
- There should be simple, transparent procedures for representing the interests of stakeholders who have limited influence and a lack of market power (mainly individuals).

Responsibility

Recommendations on responsibility

Governance mechanisms

- There should be clear rules and structures for responsibilities, actions and decision-making when it comes to running the data space.

Enforcement mechanisms

- There should be mechanisms in place that allow claims to be enforced in the event of a violation.
- Measures taken within a data space must be clearly justified.

Efficiency

Recommendations on efficiency

High data quality

- Data should be available at a sufficient level of quality thanks to a comprehensive quality management system.

Interoperability (general and specific)

- Thanks to clear shared standards and formats and open interfaces, technical infrastructure and data formats should be compatible within and between data spaces (specific interoperability).
- The basic principles of a data space, along with its practical and normative structure, should be compatible with other data spaces (general interoperability).

Adaptability

- A data space should be flexible enough to be able to adapt to changing circumstances without violating its basic principles.