Code of
CONDUCT

for operating trustworthy data spaces
based on digital self-determination

approved by the Federal Council on 8 December 2023

1. Introduction

On 30 March 2022 the Federal Council took note of the report 'Creating trustworthy data spaces based on digital self-determination'.[1] The report emphasises the importance of data and the potential of its use for Switzerland, and recommends actively promoting the creation and operation of trustworthy and interoperable data spaces.

Data spaces are organisational and technical structures that connect data users and data providers, allowing data to be used multiple times. Data spaces create a direct link between different actors involved in data supply and demand. A data space usually has a thematic focus (e.g. health, mobility, finance), generally comprises a broad range of data (e.g. data types including the personal data of individuals, data of legal entities and other non-personal data,[2] as well as dynamic and/or static data) and is subject to a governance framework that defines the conditions for accessing and using the data.

The term 'data space governance authority' is used to describe the role of the bodies that determine a data space's structure, organisation and governance, based on its legal, organisational and practical characteristics. This role can be shared by several actors. Other roles relevant to data spaces are described in greater detail in Annex 1. This code of conduct provides a guiding framework for all these roles with regard to the design and governance of trustworthy data spaces.

The development of trustworthy and interoperable data spaces is still in its infancy, but their importance is growing in an increasingly digitalised society. They open the door to broad data exchanges, create the basis for shared data usage that is more versatile and extensive, and enable the development of synergies. They also facilitate innovation, the efficient and sustainable use of existing resources, and the fulfilment of social and economic needs. In order to harness the potential of existing data, new governance mechanisms and standards need to be defined that set out how and under what conditions we as a society will use data in the future.

2. Objective and purpose of the code of conduct

The development of data spaces is taking place in a complex technological environment, with increasing volumes of data stored in proprietary silos and growing questions about data control. The code of conduct addresses these challenges by providing specific guidance on the design of trustworthy data spaces. By establishing processes in a data space that promote trust-building behaviours, actors can actively contribute to confidence in the responsible use of data as a whole. In the interests of digital self-determination, the code of conduct contains tools for the trustworthy design and governance of data spaces as well as for the secure and controlled sharing and use of data by all actors.

The code of conduct defines four basic principles for the trustworthy design of data spaces (see Section 7) and sets them out in detail in the form of recommendations alongside possible measures for implementing them. The latter are structured based on the roles that the various actors assume within the data space (see Annex 1). Decisions regarding which recommendations should apply to which actors in a given data space must be made based on the applicable legal framework, the characteristics of the data space, and the legitimate interests of all parties involved. It will not always make sense to implement every recommendation, especially when their objectives clash and one recommendation must be prioritised over another.

1. *Report on Creating trustworthy data spaces based on digital self-determination (DE), OFCOM, FDFA, March 2022.*
2. *Es ist zu beachten, dass aufgrund der Möglichkeit der Verknüpfung von Daten in Datenräumen eine trennscharfe Unterscheidung zwischen Personen- und Sachdaten künftig vermehrt erschwert wird. Die Unterscheidung von Personen- und Sachdaten fällt den verantwortlichen Akteuren innerhalb eines Datenraumes zu.*

3. Target groups of the code of conduct

The code of conduct is targeted at all private and public actors who participate in a data space. These actors assume one or more of the following four roles: data space governance authority, data intermediary, data provider and data user (see Annex 1). The following recommendations and the possible measures for implementing them are provided in reference to these four roles. The code of conduct can also serve as a guide for any future data space participants or other interested parties.

4. Added value of the code of conduct

The code of conduct is intended to promote a basic understanding of trust-building behaviour in data spaces so that individuals, companies and public bodies use these spaces and consider them secure. It thus shows how the autonomous and trustworthy handling of data can be promoted and how the utilisation potential of data can be better exploited.

Compliance with the code of conduct brings the following added value from a social and economic perspective:

1. Greater trust in the handling of data allows it to be used in a more versatile and comprehensive manner, providing scope for innovation and new business models, as well as optimised and personalised services. This also helps to ensure that challenges facing society as a whole, such as climate change, can increasingly be tackled using data-based methods.
2. The code of conduct allows actors using a trustworthy data space to play a pioneering role in new and digital business models.
3. Creating trust and acceptance in a service offered and in the technologies used has a positive effect on the experience of the actors concerned as well as on commercial success.
4. The actors using the data spaces help to shape the application and further development of the code of conduct.
5. The result is a community of practice that can share their experience of operating trustworthy data spaces.
6. Ultimately, the code of conduct supports a harmonised vision of trustworthy data spaces shared by the Confederation, the private sector and civil society.

5. Legal classification of the code of conduct

Depending on the context and the actors involved, data spaces must take a range of challenges into account in their various functions and areas of focus. The weighting and application of the different conduct recommendations and implementing measures must therefore be structured and prioritised based on the area of application and the sensitivity of the data. This voluntary code of conduct sets out legally non-binding conduct recommendations and thus serves as a guide for private and public actors to create or participate in data spaces in their respective context and legal framework.

However, it should be noted that certain requirements of the code of conduct overlap with existing statutory and specialised legal requirements (e.g. in the Data Protection Act). Here and in all other areas, the code of conduct assumes full and comprehensive compliance with the existing legal framework. Implementation of this code of conduct is not a substitute for a comprehensive review of compliance with relevant laws or sector-specific standards.

Because trust requires more than just compliance with the law, however, the code of conduct is designed to be broader than the existing legal principles in areas such as data protection. As an instrument of self-regulation, the code of conduct complements the existing legal framework by promoting voluntary and wider-ranging behavioural practices to create trustworthy data spaces based on digital self-determination. And while the code of conduct is not legally binding, it does have a certain normative intent. It is assumed that all actors have an interest in trustworthy data spaces and therefore an incentive to comply with the code of conduct by taking it seriously and carefully considering the implementation of the conduct recommendations relevant to their context.

6. Development of the code of conduct

The following recommendations, as well as the accompanying implementing measures in Annex 2, were developed as a coordinated framework for self-regulation. This was done under the direction of the Confederation as part of an inclusive process involving various actors from the private sector, academia, civil society and the public administration. If necessary, the code of conduct can be further developed and supplemented under the same approach (see Section 10). It is possible that the code of conduct will be supplemented or replaced by new legislation, as proposed by the Science, Education and Culture Committee of the Council of States in its motion 22.3890 of 22 August 2022, necessitating a shift in focus.

7. Basic principles

The following conduct recommendations show how the basic principles can be implemented within a data space. They are further explained in Annex 2 and attributed as possible implementing measures to the different roles in the data space (see Section 3 and Annex 1).

Transparency

The basic principle of transparency aims to ensure simple and transparent access to key information.

1. **Documentation**: Necessary information is documented and made accessible in such a way that all actors in the data space have a clear understanding of how data is used (especially with regard to its content, collection, storage, retention, utilisation, modification, disclosure, transfer, archiving, deletion or destruction). The same applies to the purposes for which the data is used.
2. **Organisation**: The business model, format and organisation of the data space are transparent.
3. **Clarity**: Information and data relating to the data space are made easily accessible and are presented in a way that is both clear and appropriate for the target group.
4. **Traceability**: The origin of the data provided is traceable and, particularly in the case of personal data, it is possible to anticipate how and to what end the data will be used.
5. **Access**: Data space actors have easy and barrier-free access to data and metadata. This means that data and metadata can be accessed promptly and in machine-readable form.

Control

The basic principle of control ensures that all actors have the ability to manage their data and access it in line with their roles.

6. **Monitoring tools:** All actors within a trustworthy data space have the monitoring tools required by their role for secure data use, especially with regard to personal data.
7. **Transfer**: If a data space provides for the transfer of data beyond that data space, control of such transfers must be guaranteed. This applies in particular to personal data.
8. **Freedom of choice:** Where there are no legal obligations, participation in a data space is voluntary. Participation is subject to the data space's own conditions.
9. **Security:** There are clear processes in a data space to identify and, if necessary, minimise security risks for the data space and actors involved.

Fairness

All actors in the data space must be treated fairly.

10. **Proportionality:** The exchange, use and reuse of data within a data space is based on the principle of proportionality.
11. **Freedom from discrimination:** The conditions and operation of the data space must be non-discriminatory and actors must be guaranteed the chance to participate based on objective criteria.
12. **Balance of interests:** The interests of the data space's actors are properly balanced.
13. **Data quality:** All actors within a data space strive for high data quality. Data has a direct impact on the design of products and services, and low-quality data sets can in turn lead to discrimination and unequal treatment.
14. **Special protection for children and young people:** Due to their limited experience, children and young people must be given special protection when participating in data spaces.

Effectiveness

The basic principle of effectiveness helps to maximise the usefulness and sustainability of data spaces.

15. **Implementation:** The data space's governance framework is effectively applied and implemented.
16. **Interoperability:** All actors promote the interoperability of data spaces wherever possible and relevant.
17. **Agility:** Data spaces are constantly evolving and can adapt quickly and flexibly to changing circumstances.
18. **Sustainability:** All actors are committed to the environmental, social and economic sustainability of the data space.

8. Exchange of practices

In order to promote broad and effective application of the code of conduct (comparable results in comparable situations), as well as its further development, it is suggested that data space governance authorities regularly share best practice, with a multi-stakeholder approach emphasising the interdisciplinary nature of the exchange of practices. Data space governance authorities establish corresponding activities to allow these exchanges of practices to take place. This promotes best practices, ensures the participation of a range of actors and builds capacity. The data space governance authorities report publicly on the content and format of the exchange of practices.

9. Implementation

The signatory organisations and units publish a report on their implementation of the conduct recommendations and measures at regular intervals. For the purposes of comparability, the report follows a standardised structure. In addition, the signatories are free to take further measures (e.g. mutual peer review, establishment of data assemblies).

10. Relationship to other federal projects

In addition to this 'Code of conduct for trustworthy data spaces', there is also the Federal Statistical Office's 'Code of conduct for human-centred and trustworthy data science'. This contains trustworthy behavioural practices for federal data science projects that can be used to obtain data-based insights and solve problems. Both codes of conduct pursue the same objectives, promoting the use of data under trustworthy conditions in their respective areas of application.

Motion 22.3890 WBK-S of 22.08.2022 Framework Act for the Secondary Use of Data instructed the Federal Council to create a framework act containing the necessary basis for quickly initiating and developing specific infrastructure for the secondary use of data in strategically relevant areas. The code of conduct can provide important insights in this area.

Annex 1: Roles in a data space

Data spaces are organisational and technical structures that connect data users and data providers and facilitate exchanges and the multiple use of data. Data spaces thus create a direct link between different actors on the supply and demand side of data. A data space usually has a thematic focus and a governance framework that defines the conditions for accessing and using data within the data space. Wherever possible, the structure, organisation and governance of a data space are determined in an inclusive process by the data space governance authority in consultation with the other data space actors. A total of four roles can be identified within a data space based on the functions and responsibilities assumed. An actor can take on different roles and participation is not limited to a single data space. A given role can also be allocated to several actors.[3] The roles of data space governance authority, data intermediary, data provider and data user are particularly important in the proper functioning of the data space. Figure 1 provides a simplified overview of these roles:

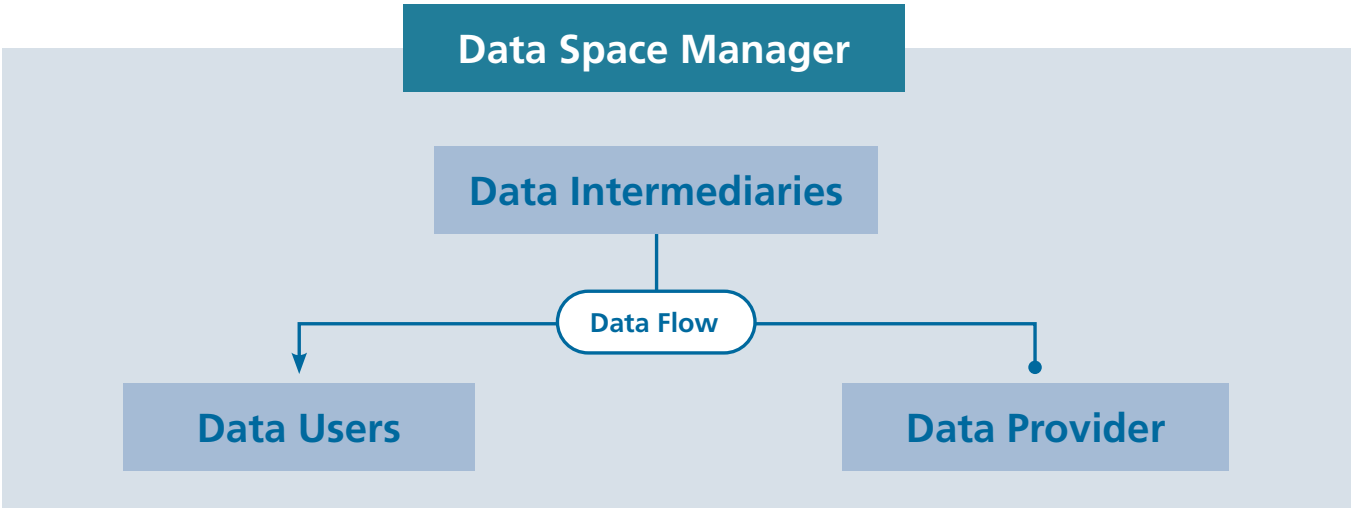

Figure 1: Overview of roles in the data space

3. *This applies in particular when state bodies perform the tasks of the governance authority. This is because, according to the constitutional principle of the separation of powers, the determination, application and enforcement of rules must in principle be shared among various state bodies.*

A. Role and responsibility / function

Role	Responsibility / function
Data space governance authority	The role of the data space governance authority encompasses all functions relating to the governance framework for the data space in question. In concrete terms, this means establishing, designing, anchoring and, if necessary, applying the conditions and associated implementation systems of the data space in its specialist context. In this sense, the data space governance authority uses the governance framework to guarantee the trustworthiness and interoperability of the data space, thus contributing significantly to a culture of trust.
Data intermediaries	Data intermediaries provide services for shared data use. They ensure the exchange of data between the supply and demand sides. Data intermediaries can be organisations or operators of data exchange infrastructure (e.g. software, physical infrastructure), as well as providers of subsidiary services such as identification or authentication. The services can be offered for a specific data space or as a general service for different applications.
Data users	Data users use the data space's data and/or data-related services. Depending on the design of the data space, they can be either organisations or natural persons.
Data providers	Data providers have the power to decide whether to grant or revoke access or usage rights to specific data. They can also make data available within a data space. Depending on the data space, data providers can be either organisations or natural persons. Under data protection law, data subjects are natural persons about whom personal data is processed.[4] Data subjects can themselves act as data providers within a given data space, for example when they enter their own data into the data space. However, data providers can also be third parties, in particular companies providing the data of legal entities, other non-personal data, and data about their customers or other persons. The code of conduct only sets out behavioural recommendations for data provision/data exchange scenarios that occur within a data space. The existing legal framework – in particular data protection law – applies in all cases, even if a data subject has no direct relationship with the data space. This in turn means that the roles required by the Data Protection Act (e.g. controller, processor, etc.) must be designated within all data spaces.

4. *See Art. 5 let. b FADP.*

B. Roles and actors

In certain circumstances, the role of data space governance authority can be filled by a committee of representatives from one or more organisations. At least in the state context, however, it is divided up into several sub-roles that are fulfilled by a number of bodies (see Annex 1. A).

Due to the tasks they perform, data intermediaries are usually legal entities under private and/or public law or public bodies entrusted with public-sector tasks.

The role of data user and data provider can be performed by natural and legal persons under private and/or public law, as well as by public bodies entrusted with public-sector tasks.

If a legal entity under public law or a public body (especially federal and cantonal bodies entrusted with public-sector tasks of the Confederation or the cantons) assumes one of the four roles of the data space, the principle of legality applies as set out in Article 5 paragraph 1 of the Swiss Federal Constitution and a legal basis is required. The code of conduct can be used as a guide for establishing the legal basis for state action. It can be used in a similar vein with private actors as a guide for determining the contractual basis or establishing internal organisational rules.

Annex 2: Possible implementing measures

This annex details the recommendations along with possible measures for implementing them. The implementing measures are organised based on the roles that actors can assume within a data space. It is necessary to consider the characteristics of the data space, the legitimate interests of all parties involved, and the applicable legal framework when deciding which recommendations and implementing measures are appropriate for a given stakeholder and data space. Although it will not always make sense to implement every recommendation and measure, implementing them as consistently as possible nonetheless promotes the trustworthiness of data spaces.

To support the practical application of the implementing measures, the annex refers at various points to existing legal obligations that are, to varying extents, connected to the measure in question. Here and in all other areas, the code of conduct assumes full and comprehensive compliance with the existing legal framework. The references are not exhaustive. The term 'data' is understood in a broad sense throughout the code of conduct (this includes, for example, the personal data of natural persons as well as the data of legal entities, non-personal data, dynamic and/or static data, etc.). Where a specific data type is explicitly meant (e.g. personal data), this is noted or referenced accordingly.

TRANSPARENCY

Recommendation 1: Documentation

Necessary information is documented and made accessible in such a way that all actors in the data space have a clear understanding of how data is used (especially with regard to its content, collection, storage, retention, utilisation, modification, disclosure, transfer, archiving, deletion or destruction). The same applies to the purposes for which the data is used.

Possible implementing measures for Recommendation 1

Data space governance authorities	Data intermediaries	Data users	Data providers
1.1.1 Data space governance authorities provide other actors with relevant and transparent information on the general data use process applicable in the data space.	1.2.1 Data intermediaries support data space governance authorities by providing relevant information about the general data use process applicable in the data space.	1.3.1 Data users provide information on the exact manner in which data is used to data space governance authorities, data intermediaries and data providers. If the data is reused, the data users in question inform the other actors about the new purposes it might be used for.[5] This implementing measure is not appropriate in an open government data context.	1.4.1 Data providers are transparent about the sources of the data offered and what it may be used for.[6]
1.1.2 Data space governance authorities ensure that transparent information and controls are in place with regard to access rights by external parties. Information is also available regarding how these access rights are controlled and secured.	1.2.2 Data intermediaries monitor data access by external parties. If required, they ensure transfers to external parties are authorised.[7]		1.4.2 Data providers make transparent to affected data space actors when and under what conditions they pass on data to external parties. In the case of personal data, they are also transparent about who they have forwarded the data to.[8]
	1.2.3 Data intermediaries provide information on the technical and organisational measures they take to identify and authorise actors in a data space.[9]		

5. *With regard to personal data within the meaning of Art. 5 let. a FADP, see in particular Art. 12, 19-20 FADP.*
6. *With regard to personal data within the meaning of Art. 5 let. a FADP, see in particular Art. 25-27 FADP on the right to receive information.*
7. *With regard to personal data within the meaning of Art. 5 let. a FADP, see in particular Art. 9, para. 3 FADP.*
8. *With regard to personal data within the meaning of Art. 5 let. a FADP, see in particular Art. 19 FADP.*
9. *With regard to personal data within the meaning of Art. 5 let. a FADP, see in particular Art. 8 and Art. 9 para. 2 FADP.*

1.1.4 Data space governance authorities ensure transparent information is provided on the data space's conditions for data transfers abroad.	1.2.4 Data intermediaries ensure an appropriate level of data protection when transferring data abroad, particularly in the case of sensitive data (i.e. sensitive personal data or valuable non-personal data). With regard to personal data, they provide information on the efforts made to ensure protection in line with the conditions applicable in Switzerland.[10]		1.4.4 Data providers ensure an appropriate level of data protection when transferring data abroad, particularly in the case of sensitive data (i.e. sensitive personal data or valuable non-personal data). With regard to personal data, they provide information on the efforts made to ensure protection in line with the conditions applicable in Switzerland.[11]

10. With regard to personal data within the meaning of Art. 5 let. a FADP, see in particular Art. 16-18 FADP.
11. Ibid.

Recommendation 2: Organisation
The business model, format and organisation of the data space are transparent.

Possible implementing measures for Recommendation 2

Data space governance authorities	Data intermediaries	Data users	Data providers
2.1.1 Data space governance authorities provide transparent information about the conditions that apply in the data space and about the actors involved, their roles and their positions in the decision-making process.	2.2.1 Data intermediaries provide information about the infrastructure and technical services of the data space.		
2.1.2 Data space governance authorities ensure there is transparent information about the data space's structure and how it functions legally and financially.			
2.1.3 Data space governance authorities clarify and regulate the rights and obligations of the various actors in the most binding form possible (e.g. by means of checklists, model contracts or by law and regulation). Feedback mechanisms are established to adapt and improve the roles.			
2.1.4 Data space governance authorities take security measures to ensure the performance of key tasks and required decision-making processes, and to minimise the risk of cyberattacks.			

Recommendation 3: Clarity
Information and data relating to the data space are made easily accessible and are presented in a way that is both clear and appropriate for the target group.

Possible implementing measures for Recommendation 3

Data space governance authorities	Data intermediaries	Data users	Data providers
3.1.1 Data space governance authorities ensure that the information and data are appropriate, legible and correct. The language and communication methods are adapted to the addressees to improve understanding.	3.2.1 Where appropriate, all information about the function and structure of the data space must be accessible in a machine-readable format for greater ease of use.		
	3.2.2 Data intermediaries ensure that the information is easy to understand, e.g. through visual or audio-visual aids such as data-protection icons, explanatory videos or podcasts that present complex topics clearly.		
	3.2.3 When sensitive data (i.e. sensitive personal data or valuable non-personal data) is collected and consent for further use is obtained, the data is given a special label.		
3.1.4 Data space governance authorities provide a point of contact for specific questions.			

Recommendation 4: Traceability
The origin of the data provided is traceable and, particularly in the case of personal data, it is possible to anticipate how and to what end the data will be used.

Possible implementing measures for Recommendation 4			
Data space governance authorities	**Data intermediaries**	**Data users**	**Data providers**
	4.2.1 Data intermediaries provide access logs so that data providers can track who has accessed their data, which data has been accessed, and when this took place.[12]		4.4.1 Data providers indicate the source of the data so that its origin can be fully traced (lineage).
4.1.2 Data space governance authorities inform data providers about the potential general risks of providing data.	4.2.2 Data intermediaries inform data providers about the potential general risks of providing data.	4.3.2 Data users inform data providers about the potential specific risks of providing data.[13]	4.4.2 Data providers are informed about the potential risks of providing their data.[14]
	4.2.3 Data intermediaries create error logs and inform all affected parties about them.		

12. *With regard to personal data within the meaning of Art. 5 let. a FADP, see in particular Art. 12 FADP and Art. 4 para. DPO.*
13. *With regard to personal data within the meaning of Art. 5 let. a FADP, see in particular Art. 22-24 FADP.*
14. *With regard to personal data within the meaning of Art. 5 let. a FADP, see in particular Art. 24 para. 3 and Art. 25 -26 FADP.*

Recommendation 5: Access
Data space actors have easy and barrier-free access to data and metadata. This means that data and metadata can be accessed promptly and in machine-readable form.

Possible implementing measures for Recommendation 5

Data space governance authorities	Data intermediaries	Data users	Data providers
5.1.1 Data space governance authorities ensure the provision of a standardised metadata catalogue and data models allowing data to be found rapidly.	5.2.1 Data intermediaries create a standardised metadata catalogue and data models.	5.3.1 A metadata catalogue is made available to data users.	5.4.1 Data providers record their metadata in accordance with the metadata catalogue provided.
5.1.2 Data space authorities ensure that the mechanisms for exercising access rights are harmonised and easily accessible to data providers.	5.2.2 Data intermediaries harmonise the mechanisms for exercising access rights and ensure data providers have easy access to these mechanisms.	5.3.2 The mechanisms for exercising access rights are harmonised and easily accessible to data users.	5.4.2 The mechanisms for exercising access rights are harmonised and easily accessible to data providers.

CONTROL

Recommendation 6: Monitoring tools

All actors within a trustworthy data space have the monitoring tools required for secure data use, especially with regard to personal data.

Possible implementing measures for Recommendation 6

Data space governance authorities	Data intermediaries	Data users	Data providers
6.1.1 Data space governance authorities ensure that all data users, data intermediaries and data providers in a data space have the necessary monitoring tools for data use.	6.2.1 Data intermediaries provide information about the existing monitoring tools for data use. They also obtain informed consent for the processing of data wherever necessary.[15] In addition, data intermediaries ensure that data use is restricted in terms of time and content, i.e. consent cannot be given in the form of a blanket authorisation.		6.4.1 Where no legal obligations exist, data providers can consent to the use of their data for a specific purpose and withdraw this consent at any time. This explicit consent must represent an expression of the provider's wishes that is free, specific and informed, and made in the form of a clear statement or affirmative act.[16]
6.1.2. Data space governance authorities ensure that data access and confidentiality levels vary in line with the type of data and risk level.	6.2.2. Data intermediaries ensure there are simple registration and data use processes that employ common identification methods (e.g. E-ID, TrustID, SwissID, etc.).		6.4.2 Data providers have access to existing data collections relating to their profile/person and to information on the risks of merging data in data collections, e.g. profiling activities. [17]
6.1.3 Data space governance authorities enable data providers to easily grant or withdraw consent to the use of data at any time.	6.2.3 Data intermediaries ensure that data providers always provide consent for data use.[18]	6.3.3 Data users ensure that data providers always provide consent for data use.[19]	

15. *With regard to sensitive personal data within the meaning of Art. 5 let. c FADP and high-risk profiling within the meaning of Art. 5 let. g FADP, see Art. 6 para. 7 FADP. See in particular also Art. 31 and, concerning data processing by federal bodies, see in particular Art. 33 ff. FADP.*
16. *Ibid.*
17. *Regarding personal data within the meaning of Art. 5 let. a FADP, see in particular Art. 12, Art. 24 para. 4 FADP as well as Art. 6 para. 7 FADP and Art. 15 DPO regarding profiling.*
18. *With regard to sensitive personal data within the meaning of Art. 5 let. c FADP and high-risk profiling within the meaning of Art. 5 let. g FADP, see Art. 6 para. 7 FADP.*
19. *Ibid.*

Recommendation 7: Transfer
If a data space provides for the transfer of data beyond that data space, control of such transfers must be guaranteed. This applies in particular to personal data.

Possible implementing measures for Recommendation 7

Data space governance authorities	Data intermediaries	Data users	Data providers
7.1.1 Data space governance authorities ensure that data sharing in general or for specific purposes can be stopped at any time. This means they must give data providers the option to withdraw their consent, thereby prohibiting further use of the data.[20]	7.2.1 Data intermediaries ensure the necessary infrastructure is in place to allow data sharing to be stopped at any time.		
7.1.2 Data space governance authorities ensure existing data can be easily deleted or destroyed and thus rendered unusable. Personal data that is no longer required for processing purposes must be destroyed or anonymised.[21]	7.2.2 At the request of the data space governance authorities or data providers, data intermediaries must delete and/or destroy the data concerned and ensure it is not forwarded to third parties.[22]	7.3.2 At the request of the data space governance authorities, data intermediaries or data providers, data users must delete and/or destroy the data concerned by the request and ensure it is no longer used.[23]	

20. *This only applies if there are no legal obligations to share the data concerned. Regarding the consent required for processing personal data, see in particular Art. 6 para. 7 FADP.*
21. *See Art. 6 para. 4 FADP*
22. *In line with Art. 6 para. 4 FADP, personal data within the meaning of Art. 5 let. a FADP must be destroyed or anonymised when it is no longer needed for processing purposes, even if a request has not yet been made.*
23. *Ibid.*

Recommendation 8: Freedom of choice

Where there are no legal obligations, participation in a data space is voluntary.

Possible implementing measures for Recommendation 8

Data space governance authorities	Data intermediaries	Data users	Data providers
8.1.1 Data space governance authorities take technical or organisational measures to minimise lock-in effects.	8.2.1 Data intermediaries facilitate data portability.[24]	8.3.1 Data users are free to choose which data space they use, and whether to use one at all.	8.4.1 Data providers are free to choose which data space they provide data in, and whether to provide it at all.
8.1.2 Data space governance authorities take measures to avoid systematic and unjustified dependence on dominant actors (be they external service providers, data providers or data users), as this dependence would make data exchange more difficult or even impossible.			
		8.3.3 Data users can easily transfer their data.[25]	8.4.3 Data providers can easily transfer their data.[26]
8.1.4 Data space governance authorities ensure that the conclusion of contracts or the provision of services and products (e.g. by data intermediaries or other service providers relevant to the data space) is not based on the unjustified provision or use of data.			

24. With regard to personal data within the meaning of Art. 5 let. a FADP and data portability, see in particular Art. 28-29 FADP.
25. Ibid.
26. Ibid.

Recommendation 9: Security

There are clear processes in a data space to identify and, if necessary, minimise security risks for the data space and actors involved.

Possible implementing measures for Recommendation 9

Data space governance authorities	Data intermediaries	Data users	Data providers
9.1.1 Data space governance authorities regularly carry out risk evaluations. These evaluations are supplemented with measures to reduce the risks identified.			
9.1.2 In the case of sensitive data (i.e. sensitive personal data or valuable non-personal data), data space governance authorities ensure regular external risk assessments are carried out. These should cover a range of security aspects.[27]			
9.1.3 Datenraumträgerschaften definieren genaue Prozesse, wie vorzugehen ist, falls die bereitgestellten Daten kompromittiert werden sollten. Die Anweisungen umfassen einen definierten Plan für Notfallmassnahmen im Falle von Datenverlust oder Sicherheitslücken.	9.2.3 Data intermediaries comply with the emergency measures applicable in the data space in the event of data loss or security breaches.	9.3.3 Data users comply with the emergency measures applicable in the data space in the event of data loss or security breaches.	9.4.3 Data providers comply with the emergency measures applicable in the data space in the event of data loss or security breaches.
	9.2.4 If data loss or a security breach is detected, data intermediaries inform the affected parties immediately so that the latter can take appropriate protective measures.[28]	9.3.4 If data loss or a security breach is detected, data users inform the affected parties immediately and in sufficient detail so that the latter can take appropriate protective measures.[29]	9.4.4 If data loss or a security breach is detected, data providers inform the affected parties immediately so that the latter can take appropriate protective measures.[30]
9.1.5 Wherever possible, data space governance authorities encourage the use of automated systems to identify data copies and patterns of misuse. The results and information produced by these systems are made available to all affected actors.			

FAIRNESS

Recommendation 10: Proportionality

The exchange, use and reuse of data within a data space is based on the principle of proportionality.

Possible implementing measures for Recommendation 10

Data space governance authorities	Data intermediaries	Data users	Data providers
10.1.1 Data space governance authorities determine the conditions for participation in a data space and generally know the purpose of data use.	10.2.1 Data intermediaries promote the implementation of privacy preserving data use methods such as anonymisation, pseudonymisation and differential privacy.[31]	10.3.1 Data users ensure that data use within the data space is reasonable, appropriate and necessary for the respective purpose, and is compatible with the conditions of the data space.	10.4.1 Where appropriate, data providers observe the principle of data minimisation when collecting data.[32]

27. *With regard to personal data within the meaning of Art. 5 let. a FADP, there is an obligation under Art. 22 FADP to carry out a data protection impact assessment if processing might entail a high risk to the personality or fundamental rights of the data subjects.*
28. *Regarding the duty to report security breaches affecting personal data to the FDPIC, the person responsible or the data subject, see in particular Art. 24 FADP and Art. 15 DPO.*
29. *Ibid.*
30. *Ibid.*
31. *With regard to personal data within the meaning of Art. 5 let. a FADP, see in particular Art. 7 FADP.*
32. *Ibid.*

Recommendation 11: Freedom from discrimination
The conditions and operation of the data space must be non-discriminatory and actors must be guaranteed the chance to participate based on objective criteria.

Possible implementing measures for Recommendation 11

Data space governance authorities	Data intermediaries	Data users	Data providers
11.1.1 Data space governance authorities ensure that there is no unjustified unequal treatment of actors with regard to data space access or within the data space itself.			
11.1.2 Data space governance authorities identify obstacles of an administrative, economic, technical and linguistic nature at an early stage and take appropriate measures to address them.	11.2.2 Data intermediaries ensure non-discriminatory access to the data space for all actors.		
11.1.3 Data space governance authorities define objective criteria for any unequal treatment of actors. They communicate them clearly and explain to all actors why these criteria justify unequal treatment.		11.3.3 Data users can request information on the criteria for any unequal treatment from data space governance authorities.	11.4.3 Data providers can request information on the criteria for any unequal treatment from data space governance authorities.

Recommendation 12: Balance of interests
The interests of the data space's actors are properly balanced.

Possible implementing measures for Recommendation 12

Data space governance authorities	Data intermediaries	Data users	Data providers
12.1.1 Wherever possible, data space governance authorities cooperate with the actors in an inclusive process to determine how, and to what extent, a balance of interests is envisaged within the data space.	12.2.1 Data intermediaries facilitate a balance of interests between data users and data providers (e.g. monetisation, compensation on the part of data users) ('fair exchange in terms of individual interest'), if provided for in the agreed conditions of the data space.	12.3.1 If provided for in the agreed terms and conditions of the data space, data users must compensate data providers.	12.4.1 If provided for in the agreed terms and conditions, data providers must receive compensation that is proportionate to the data offered.
12.1.2 Data space governance authorities safeguard the balance of interests – especially those of individuals – by enabling transparent representation mechanisms or other effective processes for taking into account the interests of all actors. They also ensure there are sufficient resources in place to achieve this.		12.3.2 Wherever possible, data users must make the knowledge gained from data use generally available in a standardised form ('fair exchange in the public interest').	12.4.2 Data providers may submit comments to the data space governance authorities or request they provide information on the criteria for the balance of interests.

Recommendation 13: Data quality:
All actors within a data space strive for high-quality data. Data has a direct impact on the design of products and services, and low-quality data sets can in turn lead to discrimination and unequal treatment.

Possible implementing measures for Recommendation 13

Data space governance authorities	Data intermediaries	Data users	Data providers
13.1.1 Data space governance authorities (or, if applicable, data intermediaries) define clear guidelines on the necessary quality requirements for data provided as well as regarding transparency and information, should data quality be reduced.	13.2.1 Data intermediaries (or, if applicable, data space governance authorities) define clear guidelines on the necessary quality requirements for data provided as well as regarding transparency and information, should data quality be reduced.	13.3.1 Data users inform data space governance authorities and data intermediaries about possible improvements to the guidelines from the perspective of the data users.	13.4.1 Data providers consistently implement the data space's quality requirements with regard to data provided.
13.1.2 Data space governance authorities ensure all actors within the data space understand the importance of high-quality data.	13.2.2 Data intermediaries enable data users and data providers to exchange information on data quality and to report any inadequacies.	13.3.2 Data users must inform data providers (or, if this is not possible, the data intermediaries) if they identify undeclared inadequacies or quality deficiencies within a dataset. There are legal obligations regarding the accuracy of personal data.[33]	13.4.2 Data providers clearly and transparently declare quality deficiencies, unrepresentative data sets and any resulting data distortions. Where possible, they make the necessary efforts to rectify such issues. There are legal obligations regarding the accuracy of personal data.[34]
13.1.3 Data space governance authorities identify and implement appropriate processes to ensure data is representative and of high quality.			13.4.3 Data providers respond promptly to reports of inadequate data sets. Where possible, they improve the data set in question. Otherwise, they declare the shortcomings clearly and transparently.
13.1.4 Data space governance authorities (or, if applicable, the data intermediaries) conclude clear data maintenance agreements with data providers which are binding for the latter.	13.2.4 Data intermediaries (or, if applicable, the data space governance authorities) conclude clear data maintenance agreements with data providers which are binding for the latter.		13.4.4 Data providers have a clear understanding of their data maintenance obligations.

33. *With regard to personal data within the meaning of Art. 5 let. a FADP, see Art. 6 para. 5 FADP, and in particular also Art. 32 and Art. 41 FADP.*

34. *Ibid.*

Recommendation 14: Special protection for children and young people Due to their limited experience, children and young people must be given special protection when participating in data spaces			
Possible implementing measures for Recommendation 14			
Data space governance authorities	**Data intermediaries**	**Data users**	**Data providers**
14.1.1 Data space governance authorities define special protective measures for the participation of children and young people in the data space. These must take into account the following circumstances in particular: the age of the child, their ability to make judgements, the type of data processed, the purpose of the processing and the specific risks of processing the personal data of children and young people.	14.2.1 Data intermediaries must ensure compliance with special protective measures for children and young people.		

EFFECTIVENESS

Recommendation 15: Implementation

The governance framework applicable in a data space is effectively applied and implemented.

Possible implementing measures for Recommendation 15

Data space governance authorities	Data intermediaries	Data users	Data providers
15.1.1 Data space governance authorities define and communicate clear measures with regard to non-compliance with the agreed responsibilities.	15.2.1 Data intermediaries implement the measures defined by the data space governance authorities in the event of non-compliance with the agreed responsibilities.	15.3.1 Data users implement the measures defined by the data space governance authorities in the event of non-compliance with the agreed responsibilities.	15.4.1 Data providers implement the measures defined by the data space governance authorities in the event of non-compliance with the agreed responsibilities.
15.1.2 Data space governance authorities establish or identify complaints bodies to which actors can turn in the event of a conflict. These complaints bodies provide procedural safeguards to ensure due process and procedural fairness.			
15.1.3 Data space governance authorities inform the actors concerned of the relevant legal remedies.			
15.1.4 Data space governance authorities ensure all involved actors in the data space have access to evaluation mechanisms for regularly assessing the effectiveness of the existing governance.			

Recommendation 16: Interoperability
All actors promote the interoperability of data spaces.

Possible implementing measures for Recommendation 16

Data space governance authorities	Data intermediaries	Data users	Data providers
16.1.1 Data space governance authorities ensure the interoperability of the data space from a legal and organisational perspective.	16.2.1 Data intermediaries ensure the interoperability of the data space in technical and semantic terms.	16.3.1 Data users comply with the interoperability requirements of data space governance authorities and data intermediaries.	16.4.1 Data providers comply with the interoperability requirements of data space governance authorities and data intermediaries.
16.1.2 Data space governance authorities determine relevant standards carefully and in consultation with all actors involved. These standards are defined in clear guidelines and are easy to access and understand.	16.2.2 Data intermediaries determine relevant standards carefully and in consultation with all actors involved. These standards are defined in clear guidelines and are easy to access and understand.	16.3.2 Data users apply the guidelines provided and adhere to the standards applicable in the data space.	16.4.2 Data providers apply the guidelines provided and adhere to the standards applicable in the data space.
16.1.3 Data space governance authorities check whether existing open standards are suitable and adopt them whenever possible in order to increase compatibility with other data spaces.	16.2.3 Data intermediaries check whether existing open standards are suitable and adopt them whenever possible in order to increase compatibility with other data spaces.		
16.1.4 Data space governance authorities promote open and common standards, especially within a specific sector.	16.2.4 Data intermediaries promote open and common standards, especially within a specific sector.		

Recommendation 17: Agility
Data spaces are constantly evolving and can adapt quickly and flexibly to changing circumstances.

Possible implementing measures for Recommendation 17

Data space governance authorities	Data intermediaries	Data users	Data providers
17.1.1 Data space governance authorities select the infrastructure, form and business model of the data space carefully and with an eye to future developments.			
17.1.2 Data space governance authorities design organisational and governance structures that remain functional even in rapidly changing circumstances and can be adapted promptly. Feedback mechanisms are established for this purpose.	17.2.2 Data intermediaries contribute to the development process of the data space as effectively as possible via feedback mechanisms.	17.3.2 Data users contribute to the development process of the data space as effectively as possible via feedback mechanisms.	17.4.2 Data providers contribute to the development process of the data space as effectively as possible via feedback mechanisms.

Recommendation 18: Sustainability
All actors are committed to the environmental, social and economic sustainability of the data space.

Possible implementing measures for Recommendation 18

Data space governance authorities	Data intermediaries	Data users	Data providers
18.1.1 Data space governance authorities conduct regular impact assessments regarding the sustainability of the data space.			
18.1.2 Based on these impact assessments, data space governance authorities identify risks and develop specific measures to reduce and minimise them.	18.2.2 Data intermediaries implement risk reduction measures to the best of their ability.	18.3.2 Data users implement risk reduction measures to the best of their ability.	18.4.2 Data providers implement risk reduction measures to the best of their ability.