Rulebook for a Fair Data Economy

Rulebook Template for Data Networks

Version 1.3 en

30 June 2021

The Rulebook Template is created by the Rulebook Workgroup in Sitra's IHAN program. The Rulebook Template has been actively contributed by Olli Pitkänen (1001 Lakes Oy), Jyrki Suokas (Sitra), Sami Jokela (1001 Lakes Oy), Marko Turpeinen (1001 Lakes Oy), Jorma Yli-Jaakkola (Borenius Attorneys Ltd and Lexia Attorneys Ltd), Jani Koskinen (University of Turku), Jussi Mäkinen (Technology Industries of Finland), Kai Kuohuva (TietoEVRY Oyj), Kari Hiekkanen (Aalto University), Saara Malkamäki (Sitra), Antti Kettunen (TietoEVRY Oyj), Petri Laine (Hybrida), Kari Uusitalo (Business Finland), Pekka Mäkelä (University of Helsinki), Meri Valtiala (The Human Colossus Foundation), Anna-Mari Rusanen (Ministry of Finance), Sari Isokorpi (Medifilm Oy), and Otto Lindholm (Dottir Attorneys Ltd).

Rulebook Template for Data Networks

Inquiries: ihan@sitra.fi
www.sitra.fi

1 Rulebook template for Data Networks

This Rulebook template is produced in Sitra's IHAN programme by the Rulebook workgroup. It is openly available under Creative Commons 4.0 CC-BY terms and conditions

Table of Contents

2 General Part

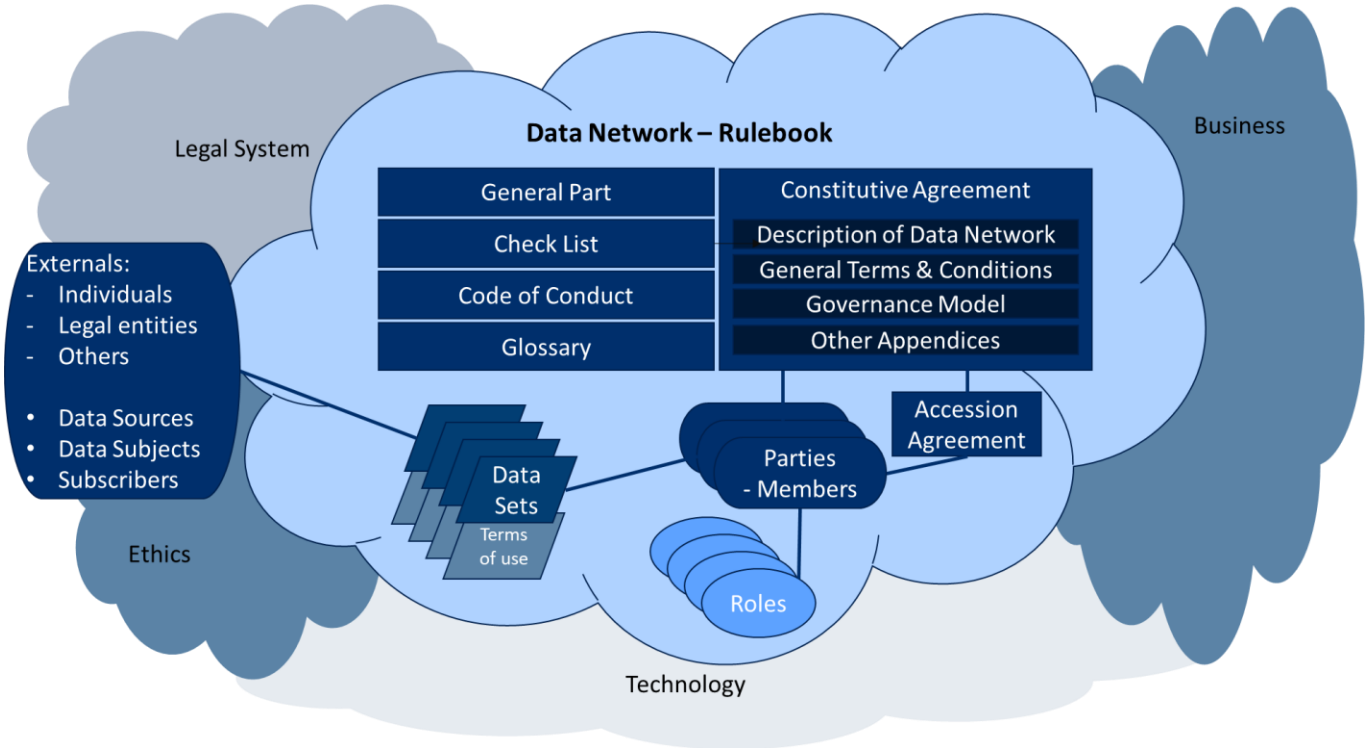
2.1 Introduction

The purpose of this Rulebook Template is to provide an easily accessible manual on how to establish a data network and to set out general terms and conditions for data sharing agreements. This Rulebook Template will help organisations to form new data networks, implement rulebooks for those data networks, and promote the fair data economy in general. With the aid of a rulebook, parties can establish a data network based on mutual trust that shares a common mission, vision and values. A rulebook also helps data providers and data users to assess any requirements imposed by applicable legislation and contracts appropriately in addition to guiding them in adopting practices that promote the use of data and management of risks. However, despite the Rulebook Template, the parties still need to check themselves that all the relevant legislation, especially on the national and subnational levels, as well as specific legislation regulating the data in question is considered.

There are many benefits to sharing data. It may allow data users to access data for research purposes or for the development of their products and services. Sharing data may also allow data providers to improve their products or services and supporting the development of added value or services by third parties. The existence of rich ecosystems that create new products and services may become very attractive to users. An increase in the number of service users, in turn, encourages new product and service developers and users to join the data ecosystem. This network effect may increase the value of a specific service and even the entire ecosystem. Furthermore, sharing data may lower the transaction costs of gathering data and allow data providers to combine their databases with minimal organisational changes.

Data networks that adopt the Rulebook Template must be fair, balanced and lawful in their processing of data. They must also be just and impartial toward their members and ensure that the rights of third parties are not infringed. Personal data must be processed in accordance with European and applicable national data protection regulations. Data networks identify and manage risks associated with the sharing and processing of data while ensuring the exploitation of new possibilities that data offers. This includes also ensuring compliance with relevant competition legislation and that the data network will not have a negative impact on market competition and consumers. Provisions restricting access to the network are especially important to take into account in this kind of assessment.

The following picture illustrates the relations between the different parts of a rulebook implemented from this Template.



It is possible to significantly improve commercial businesses and public services by better availing data. Sharing data across organization borders multiplies these opportunities. However, there are lots of obstacles that prevent cross-organizational data sharing. They include

- the lack of technical and semantic interoperability;
- inability to adequately identify different actors;
- the lack of data quality;
- cultural and attitudinal problems; difficulties in understanding the benefits from data sharing;
- risks related to losing control of data and trade secrets, infringing others' rights, and data protection; inability to coordinate data ecosystems and get all entities excited and involved;
- inability to define success and show value for all entities in a data ecosystem;
- inability to create a common vision, mission, purpose and values;
- inability to identify roles for each entity.

The Rulebook Template aims at helping to remove these obstacles. It enables and improves fairer, easier and more secure data sharing within data networks. A rulebook based on this Template describes legal, business, technical, and governance models that the members of the data network use when sharing data with each other. It takes with the greatest importance into consideration ethical principles and especially the requirements that arouse from individuals' privacy and data protection.

The General Terms of the Rulebook Template as well as most of Glossary, Code of Conduct, and Control Questions in Check Lists (see Appendix) are the same for all the data networks that use this IHAN Fair Data Economy model. Only the Specific Terms are written case by case. Therefore, it is easier and more cost-effective to create data networks and ecosystems, if the rulebooks of different data networks have substantially similar basis. It simplifies collaboration and data sharing even between data networks and makes it easier for an organization to participate in several data networks. The similar Rulebooks ensure fair, sustainable and ethical business within the data ecosystems, which in turn enables increasing know-how, trust and common market practises.

In order to be able to use its own and others' data, the organization needs to understand broadly the business, legal, technical, and ethical perspectives of data sharing. It should especially recognize in which roles it acts in the data network, which data processing and refining capabilities it needs to have, and what are the minimum requirements to participate in the data network. The four main roles of the actors within a data network are:

1. **Data Provider**: one or several sources that provide the network with data.[1]
2. **Service Provider**: one or several data refiners that combine data streams, refine data, and provide them further. Provides services to End-Users or as a subcontractor to other Service Providers.
3. **End-User**: one or several individuals or organizations for which a Service Provider has developed its services. Consumes, utilizes and accesses the value that is created in the data ecosystem.
4. **Infrastructure Operator**: one or several actors that provide identity management, consent management, logging, or service management services for the data network.

As recognized in the Proposal for a Regulation on European data governance (Data Governance Act), providers of data sharing services (data intermediaries) are expected to play a key role in the data economy, as a tool to facilitate the aggregation and exchange of substantial amounts of relevant data. Data intermediaries offering services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing. Specialised data intermediaries that are independent from both Data Providers and End-Users can have a facilitating role in the emergence of new data-driven ecosystems independent from any player with a significant degree of market power.[2] To comply with the Data Governance Act, its provisions will be considered, when they will become available, while this Rulebook Template is developed further. However, it is essential to realize that each of the members of the data network can operate in several roles and they may change continuously. Service Providers and Infrastructure Operators are natural candidates for independent data intermediaries in accordance with the Data Governance Act. Nonetheless, it should be noted that they are not always independent, but Data Providers and End-Users may occasionally also provide services or operate the infrastructure. Also, note that in a wider context, even Data Providers may get data from external sources and there can be external parties, **Subscribers,** that receive data from the data network in accordance with the Data Sets' Terms of Use although they are not Parties of the Constitutive Agreement. The starting point is that the rulebook is open and public, which is required by the transparency principle and the data protection legislation. However, the network-specific parts of a rulebook contain also confidential rules that are not disclosed outside the data network.

[1] Note: in earlier versions of the Rulebook Template for Data Networks, the term "Data Source" is used instead of Data Provider.

[2] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM(2020) 767 final.

2.2 Quick Start Guide

How to Start?

If you want to initiate a rulebook-based data network, follow these steps:

1. Go through the control questions in the Rulebook Template's Check List (see Appendix) to see, how mature the network is, what are your capabilities, and how your version of the Rulebook should be implemented.

2. Based on your answers to the Check List's control questions, fill in the Description of the Network, both the Business Part and the Technology Part. Check if you want to add more terms into the Glossary or change the existing definitions.

3. Read carefully all the Contractual parts and decide, how you want to complete them, and which terms and conditions need to be changed in your case.

4. Ask the Founding Members to sign the Constitutive Agreement and start sharing data. New members may join the data network by signing an accession agreement. The data network is governed in accordance with the Governance Model.

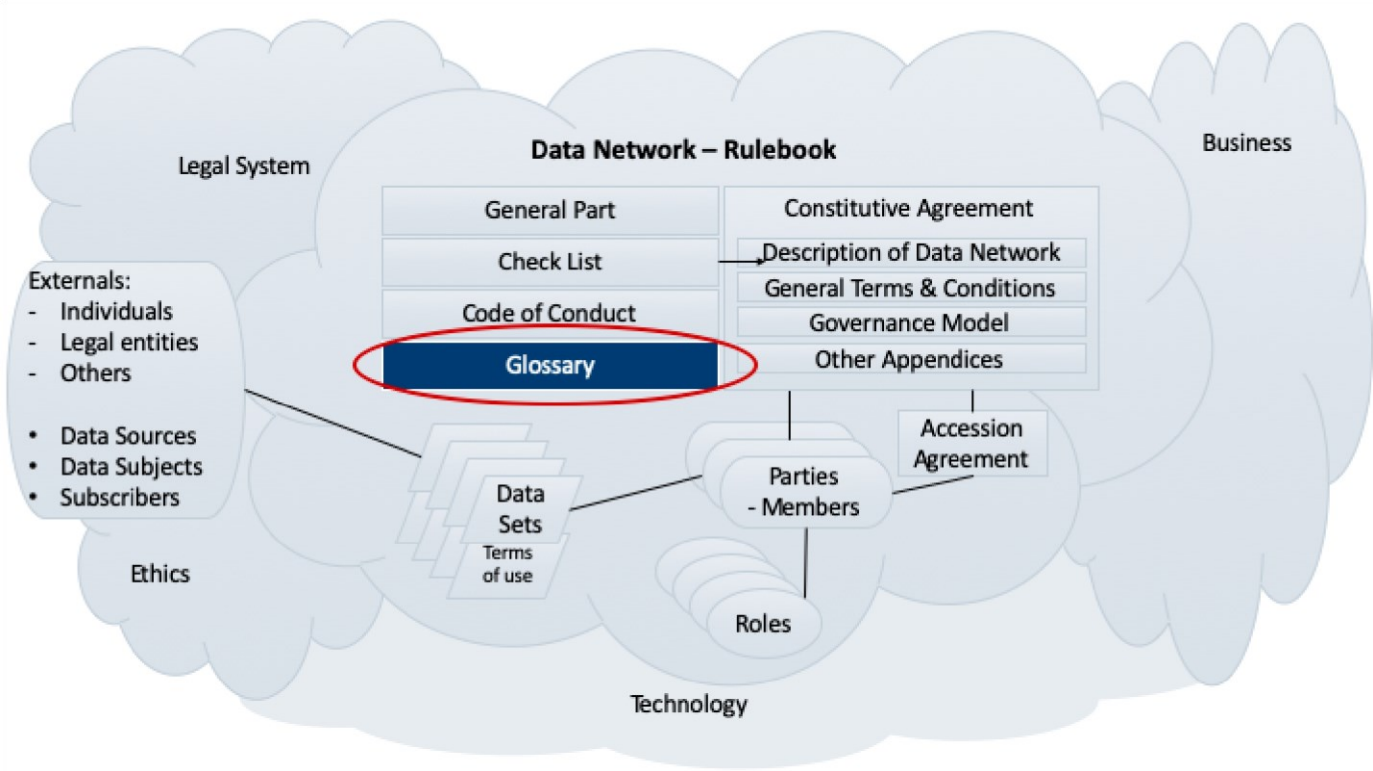
5. Give feedback to us on what kind of changes and amendments you made to the Rulebook and how we could improve the Templates.

2.3 What is new in this version?

In this version 1.3, both the business part and the technology part of the description of the data network have been enhanced based on the feedback and increasing experiences we have gathered. The checklists have been respectively improved. The contractual models have been revised based on the feedback we have received. Our intention is to make the Rulebook more approachable. Therefore, we are in process of simplifying the structure of the Rulebook and the contractual models. This version is a step in that process. We will continue the work and hope to get more feedback from you. Please send your comments to Juhani Luoma-Kyyny < juhani.luoma-kyyny@sitra.fi> and Olli Pitkänen <olli.pitkanen@1001lakes.com>.

3 Glossary

This Glossary explains some of the key concepts in the rulebook. Please note that the Constitutive Agreement of this rulebook includes legally binding definitions of some terms that are used in the agreement. If this Glossary and the definitions in the Constitutive Document are in conflict, the definitions in the agreement prevail legally. The following picture illustrates the Glossary's position within the entirety of the Rulebook. The data network may add and adapt concepts and their explanations in this Glossary as necessary.



TERM	DESCRIPTION
Data Ecosystem	A system of interrelated Data Networks.
Data Intermediary	A provider of data sharing services as defined in the Regulation on European data governance (Data Governance Act) or its current draft.
Data Network	A group of organizations and/or individuals that build data sharing solutions. / A group of companies and other organizations or even individuals that share data in accordance with a rulebook or other contractual arrangement.
Data Provider	Any natural person or an organisation that provides data for the parties to use via a Data Network. Note that in earlier versions of Sitra's Rulebook Template for a Fair Data Economy, the term "Data Source" is used instead of Data Provider.
Data source	Any source system for data. For example, weather APIs (application programming interfaces), internal systems and databases, IoT devices. Note that in earlier versions of Sitra's Rulebook Template for a Fair Data Economy, the term "Data Source" refers to a Data Provider.

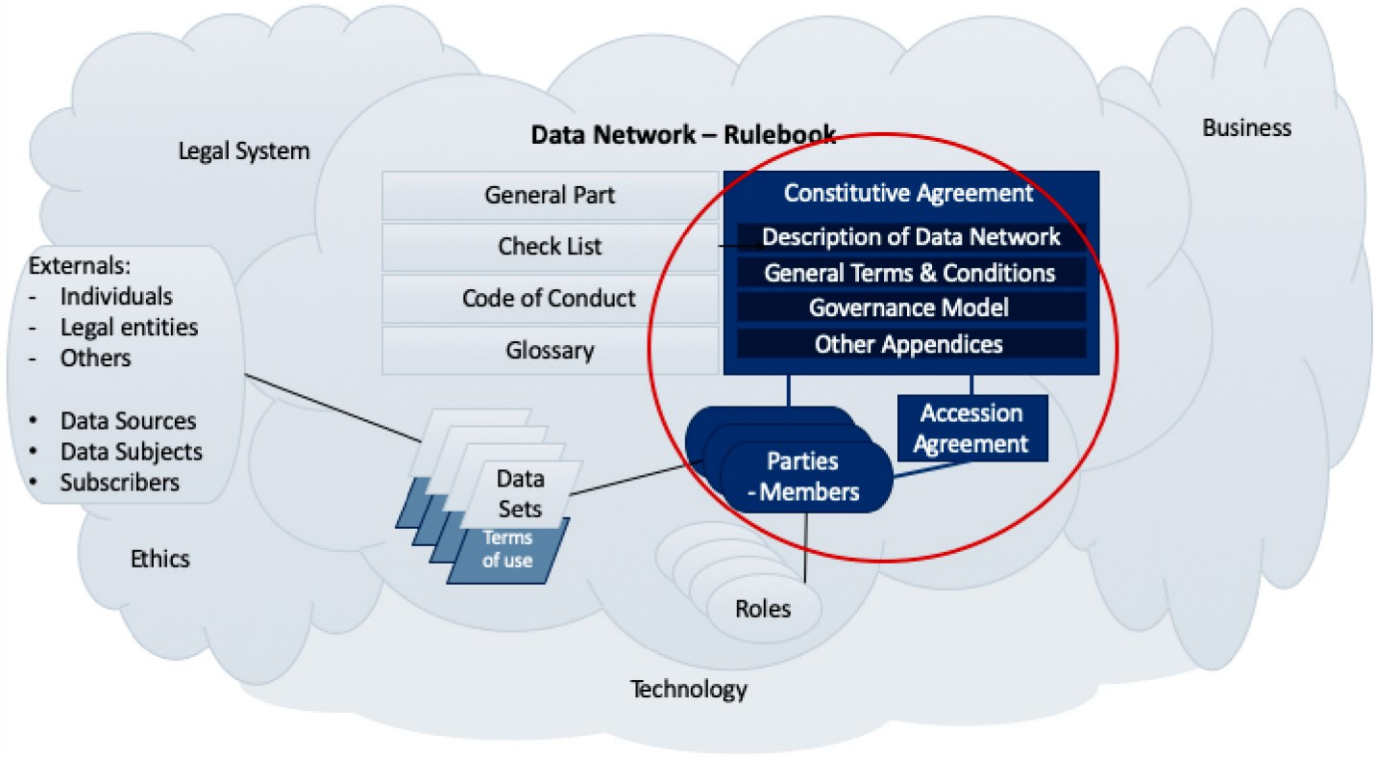
Description of the Network	The part of the Rulebook that describes the Data Network by summarizing the answers to the control questions of the Check Lists as found appropriate by the founding members of the data Network. It has a business part, including a Data Ecosystem Canvas that presents the business design for the data network, as well as a technical part that collects the technical decisions raised via the rulebook checklist document and otherwise during the infrastructure and system design for the data ecosystem.
Fair Data Economy	A fair data economy accommodates the interests of all types of participants while also providing for a high level of overall data usage. In a fair data economy: • Individuals know how their data is being used, can freely give and revoke required permission for the use of their data and mandate its sharing with third parties. They gain a share of the benefit from their data, typically not in monetary form but in terms of better services. • Service providers include for instance social media, banks, utilities, hospitals and retailers. They share control of their users' data, often investing significant resources to co-produce them. They are able to share personal data with third parties based on a range of legally valid reasons, including consent. They may need to provide their customers with portability rights, but also be able to build innovative services on users' data. A fair data economy is not a form of data collectivisation: it does not require service providers to give up and share their aggregate Data Products as such, only individual data through portability. • Data re-users are able to access a customer's personal data hosted by the service provider to provide them or others with new services. Data should not constitute an excessive barrier to entry. And researchers and innovators should be able to make the best out of the data. Data re-users include for instance third-party payment providers or independent businesses that directly compete with the service provider, but also other parties, such as data analytics companies or researchers, that are in different lines of business and can innovate by re-using the data. Both service providers and data re-users are accountable for misusing personal data. (Sitra: A Roadmap for a Fair Data Economy, https://media.sitra.fi/2019/04/09132843/a-roadmap-for-a-fair-data-economy.pdf)
GDPR	General Data Protection Regulation, i.e. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. https://eur-lex.europa.eu/eli/reg/2016/679/oj
IDS	International Data Space is a peer-to-peer network, a virtual data space that supports the secure exchange and the simple linking of data in business ecosystems on the basis of standards and by means of common governance models. https://www.internationaldataspaces.org/
IHAN	Sitra's IHAN® project aims to build the foundation for a fair and functioning data economy. The main objectives are to create a method for data exchange and to set up European level rules and guidelines for ethical use of data. https://www.sitra.fi/en/topics/ fair-data-economy/
IPR	Intellectual Property Rights including copyright and its neighbouring or related rights, patents, trademarks, and other legal rights that protect intangible, intellectual property.

4 Contractual Framework

The Contractual Framework of the Rulebook consists of the following parts:

- Constitutive Agreement
  - General Terms and Conditions
  - Governance Model
  - Accession Agreement
  - Dataset Terms of Use
- Description of the Data Network
  - Business Part
  - Technology Part

The members of the Data Network are parties to the Constitutive Agreement either directly (the Founding Members) or through an Accession Agreement. The following picture illustrates the Contractual Framework's position in the entirety of the Rulebook.



These templates that will enable corporations to establish contractual frameworks for their Data Networks have been prepared to support corporations in defining the legal relations within their Networks. During the development of these templates, it was kept in mind that Data Networks will differ from one another materially in several respects and that it is not feasible to establish general templates for a contractual framework that would be complete and ready to use as-is for all Data Networks across the board. As such, the Founding Members must plan, design and document each Data Network carefully by amending and supplementing the templates in a manner that best serves the purposes of the contractual framework they require. In this regard, the templates provided herein should be considered to constitute a baseline that serves as a generic structure for Data Networks.

The templates for the contractual framework include

- the **General Terms and Conditions**;
- a template for the **Constitutive Agreement**;
- a template for the **Accession Agreement**;
- a template for the **Dataset Terms of Use**; and
- a template for the **Governance Model**.

Data Networks are established under the Constitutive Agreement, which is concluded by and between the Founding Members of the relevant Data Network. The General Terms and Conditions are included as an Appendix to the Constitutive Agreement.

Although the intention behind the General Terms and Conditions is to have them serve as a one size fits all baseline solution for various Data Networks, the reality is that each Data Network will require specific modifications to be made to the General Terms and Conditions. For this purpose, the template Constitutive Agreement includes a designated section for derogations from the General Terms and Conditions, which the Founding Members should review and amend in order to ensure that the contractual framework suits their Data Network. As such, the final contents of different Data Networks' Constitutive Agreements and their Appendices are expected to differ to a material degree. We recommend that the Founding Members do not amend the General Terms and Conditions document itself but rather

include any relevant amendments as derogations from the Constitutive Agreement. This will enable the Members to easily identify which amendments have been made without the need to compare the original General Terms and Conditions document to the amended version.

The Founding Members may allow new Members to join the Data Network under an Accession Agreement. Where the Data Network is established to allow for this kind of open access, the Founding Members should describe the applicable accession criteria for new Members in the Constitutive Agreement. Furthermore, the Founding Members should consider whether they should define the criteria and process for accepting new Members to the Data Network in the Governance Model Appendix, together with other governance framework related matters that must be taken into consideration during the life cycle of the Data Network. The Governance Model Appendix assumes that each Member nominates a representative to serve on the Steering Committee. The Steering Committee's mandate has been defined in a relatively broad manner in order to facilitate collaboration between the Parties and to organise the administration of the Data Network appropriately on a strategic level. This includes e.g., a mandate to amend the Constitutive Agreement by a qualified majority of the Steering Committee representatives.

The purpose of the General Terms and Conditions is to serve as a tool during the operational phase of a Data Network. On the one hand, establishing a Data Network may involve material joint project investments by the Founding Members, while on the other hand, establishing a Data Network could require the Members to carry out individual actions. Any such potential project agreement by and between the Founding Members must be concluded separately and, where the Founding Members are open to welcoming new Members to the Data Network at a later stage, their contribution to cover the project costs should be agreed in the Constitutive Agreement and in any Accession Agreements. In addition, the Members should also define any fixed term commitments for sharing the Data within the Data Network, e.g., where the Members seek to recover any investments, they have made for the purposes of establishing the Network or, alternatively, where they require reciprocity while sharing the Data.

The purpose of the template Dataset Terms of Use is to provide a template for the Data Providers to define the detailed terms and conditions that apply to the Dataset(s) that the respective Data Provider makes available within the Data Network. Where the Data Provider allows redistribution of the Data to any Third Parties, the Data Provider should also define any applicable Dataset specific terms and conditions in the Dataset Terms of Use that the Members should include in their agreement with such Third Parties regarding the redistribution of the Data thereto.

By using the General Terms and Conditions, the parties undertake to comply with them, unless the parties expressly decide to derogate from the General Terms and Conditions in the Constitutive Agreement. The Dataset Terms of Use, on the other hand, are supposed to be defined separately for each Dataset by the relevant Data Provider that makes the Data available to the Data Network.

The roles identified under the General Terms and Conditions for the Members of the Data Network include:

- **Data Provider** (makes data available within the Network);
- **Service Provider** (processes Data to provide related services and redistributes the Data, such as anomymisation, pseudonymisation or combination of Data);
- **End User** (uses the Data in its business); and
- **Operator** (provides services to facilitate the operation of the Network, such as provision of APIs, management of identities, connections and/or contracts).

In addition, **Third Party End User** has been identified as a role for any Third Parties who receive Data from Service Providers where the respective Data Provider has permitted such transmission of the Data.

It should be noted that individual parties may assume several roles within a specific Data Network and that, on the other hand, Data Networks may not necessarily require all roles. For example, the roles of Operator or even Service Provider may not be relevant if the parties exchange Data among themselves and use the Data in their respective businesses. On the other hand, the Data may pass through several Service Providers in certain Data Networks before End Users or Third Party End Users receive and use it.

Key Principles for the Data

Both the Data exchanged in various Data Networks and the terms and conditions that apply to the Data may vary significantly. It was not feasible for the Working Group to define a library of terms and conditions that would cover various scenarios while establishing the template contractual framework. The Working Group has decided to define a simple set of principle-based terms and conditions in the template contractual framework.

The principle-based terms and conditions for Data are based on the following assumptions:

- the Data Provider may decide, separately for each Dataset, the Parties who are granted access to the Data;
- unless otherwise defined by the Data Provider in the Dataset Terms of Use or agreed by the Members, the Data Provider grants the right to use the Data free of charge;
- the provision of Data within the Data Network does not constitute a transfer of Intellectual Property Rights;
- the Data can be redistributed only to the Members of the Network, but Data Providers may allow redistribution of the Data to Third Party End Users under the applicable Dataset Terms of Use;
- the Parties are entitled to redistribute Derived Materials to third Parties, subject to additional requirements related to Intellectual Property Rights, Confidential Information and Personal Data;
- where the Data involves Personal Data, the default approach assumes that the data recipient becomes a data controller;
- the Data Provider indemnifies other Parties against claims that its Data, which is subject to any fees, infringes Intellectual Property Rights or Confidential Information in the country of the Data Provider;

- the Members are entitled to use the Data after the termination of the Constitutive Agreement, in which case the Constitutive Agreement survives the termination, except for where the Constitutive Agreement is terminated as a result of Party's material breach; and
- the Data Provider is entitled to carry out audits related to its Data.

Process-wise, the Members need to carefully analyse their needs and objectives against the assumptions above. If needed, the Members of the relevant Data Network may wish to amend these principles on a case-by-case basis either at the level of the Data Network by indicating any necessary derogations from the General Terms and Conditions in the Constitutive Agreement and/or by defining a more detailed template for the Data Network specific Dataset Terms of Use. In addition, each Data Provider should define, within the framework established for their respective Data Network, the terms and conditions that apply to their Data. Furthermore, more detailed conditions may be added in order to accommodate for different and more multi-faceted business models and e.g., framework for processing of Personal Data. The Members of the Data Network may also need to add a mechanism that facilitates transfer of data also to third parties.

4.1 General Terms and conditions

1 APPLICABILITY, SCOPE AND GOVERNANCE

1.1 The Data Network is established by the Constitutive Agreement, which is signed by the Founding Members of the Network.

1.2 The provisions of these General Terms and Conditions will become applicable to and legally binding on the data sharing agreements of the Parties to the Data Network upon the execution of the Constitutive Agreement and any further Accession Agreements, as applicable.

1.3 In the event that a discrepancy arises between any of the terms and conditions established in the Constitutive Agreement, any Accession Agreements and these General Terms and Conditions, including any of their appendices or schedules, any such discrepancy will be resolved in accordance with the following order of priority:

(i) the clauses of the Constitutive Agreement;

(ii) the clauses of any Accession Agreement(s);

(iii) Dataset Terms of Use and related Schedules;

(iv) these General Terms and Conditions; and

(v) other Appendices to the Constitutive Agreement in numerical order.

1.4 Any amendments to or derogations from these General Terms and Conditions must be agreed upon in the Constitutive Agreement in order to be valid.

2 DEFINITIONS

2.1 In these General Terms and Conditions, the following capitalised terms and expressions have the following meanings, and the singular (where appropriate) includes the plural and vice versa:

"**Accession Agreement**" means the agreement that governs the admission of parties to the Constitutive Agreement and the Data Network after the execution of the Constitutive Agreement.

"**Affiliate**" means any individual, company, corporation, partnership or other entity that, directly or indirectly, controls, is controlled by, or is under shared control with Party.

"**Appendix**" means any appendix to the Constitutive Agreement.

"**Confidential Information**" refers to trade secrets as defined in the EU Directive 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, point (1) of Article 2.

"**Constitutive Agreement**" means the agreement under which the Data Network is established and any of its appendices.

"**Data**" means any information that Data Providers have distributed, transmitted, shared or otherwise made available to the Data Network based on the Constitutive Agreement and during its period of validity as further defined in the respective Dataset Terms of Use.

"**Data Processing Agreement**" means a written contract concluded between a controller and a processor that processes Personal Data on behalf of the controller, which sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of data subjects, and the obligations and rights of the controller.

"**Data Provider**" means any natural person or an organisation that provides Data for the Parties to use via the Data Network.

"**Dataset**" means a collection of Data whose use the Data Provider authorises via the Data Network. Datasets and their related terms and conditions are defined more in more detail in the respective Dataset Terms of Use.

"**Dataset Terms of Use**" means the terms under which the Data Provider grants a right to use the Data included in the Dataset to the Service Providers and/or End Users.

"**Derived Material**" means information derived from Data or information that is created as a result of the combination, refining and/or processing of Data with other data, provided that (i) the Data cannot be readily converted, reverted or implied from the Derived Material to recreate the Data; (ii) the Derived Material cannot be used as a substitute for the Data; (iii) individual Data Providers of the Data cannot be identified from the Derived Material; and (iv) the Derived Material does not contain any Data Provider's Confidential Information.

"**End User**" means any of the Parties to which Service Providers provide Data and/or services or to which the Data Provider provides Data, and which do not redistribute the Data further.

"**Founding Members**" are the initial Parties that execute the Constitutive Agreement.

"**Governance Model**" means an appendix to the Constitutive Agreement that includes a network-specific description of the rules and procedures of accession (i.e., who may be admitted to the Network and how), applicable decision-making mechanisms, and further governance provisions regarding the administration of the Network.

"**Intellectual Property Rights**" means patents, trademarks, trade and business names, design rights, utility models, copyrights (including copyrights in computer software), and database rights, in each case registered or unregistered and including any similar rights to any of these rights in any jurisdiction and any pending applications or rights to apply for the registration of any of these rights.

"**List of Members**" means a list of Parties which is included as an appendix to the Constitutive Agreement and which is updated upon the accession of new Parties and the termination of incumbent Parties.

"**Operator**" means any Party that provides data system or any other infrastructure services for the Data Network that are related e.g., to identity or consent management, logging or service management.

"**Operator Service Agreement**" means any service level agreements governing the services provided by any of the Operators to the Data Network or to its Members.

"**Party**" or "**Member**" means a party to the Constitutive Agreement and/or to an Accession Agreement and a member of the Data Network.

"**Personal Data**" has the meaning set forth in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation) ("**GDPR**").

"**Schedule**" means any schedule to the Dataset Terms of Use.

"**Service Provider**" means any of the Parties that combines, refines and processes data and provides the processed Data and/or a service, which is based on the Data, to the use of End Users, other Service Providers or Third Party End Users.

"**Third Party**" means a party other than a Party.

"**Third Party End User**" means any Third Party that receives any Data directly or indirectly from any of the Service Providers.

3 ROLE-SPECIFIC RESPONSIBILITIES

3.1 The potential roles defined under these General Terms and Conditions for the Parties to the Constitutive Agreement are (1) the Data Provider, (2) the Service Provider, (3) the End User and (4) the Operator. A Party may simultaneously occupy multiple roles. In such case, the relevant Party must comply with all applicable obligations related to each role and relevant Data. In addition, Third Party End User is a role recognised under these General Terms and Conditions as applying to any stakeholders who are not a Party to the Constitutive Agreement but who receive Data.

3.2 A more specific description of the roles and the determination of role-specific responsibilities may be included in the Constitutive Agreement.

1.1 Data Provider

3.3 The Data Provider will be responsible for defining the Dataset Terms of Use for any Data that the Data Provider makes available within the Network. This includes, the right to define the purposes for which relevant Data can be processed, the right to allow the redistribution of Data to End Users and, where applicable, to Third Party End Users, and the right to prohibit the unauthorised use of Data and the right to refrain from sharing Data within the Network. The Data Provider must notify the Parties to whom the Data Provider makes the Dataset available of any new Dataset Terms of Use, after which the Dataset Terms of Use will bind the other Parties. Unless otherwise defined in the applicable Dataset Terms of Use, any changes introduced by the Data Provider to the applicable Dataset Terms of Use will become effective within thirty (30) days from the relevant Parties to the Network being sent a notification of such change. changes to the Dataset Terms of Use must not have retroactive effect.

3.4 The Data Provider shall provide Data for the use of the Network in a machine-readable form and by a method as defined by the Data Provider in the applicable Dataset Terms of Use (e.g., application programming interface, downloadable package or other method).

3.5 As an exception to the above clause 3.3, the Data Provider may undertake to grant the right to use certain specific Datasets or types of data to the Network for a fixed period, , in order to protect investments made in the Network by other Parties in good faith.

3.2 Service Provider

3.6 The Service Provider will be responsible for processing Data in accordance with the Constitutive Agreement and the applicable Dataset Terms of Use.

3.7 The Service Provider must keep records of its processing activities and deliver, on request, reasonably detailed reports on usage, processing and redistribution of Data to the relevant Data Provider(s).

3.3 End User

3.8 The End User must use Data in accordance with the Constitutive Agreement and the applicable Dataset Terms of Use.

3.4 Operator

3.9 The Network may involve one or several Operators. The Operator(s) are responsible for providing the Network with services that facilitate the operations of the relevant Data Network, such as authentication, identification, and identity/consent management services or for ensuring data security or providing technical data protection solutions for the Network and as further defined in the applicable Operator Service Agreement.

3.10 Any Operator Service Agreement(s) concluded with the Party/Parties and the Operator(s) may be included as an Appendix to the Constitutive Agreement.

3.11 Operator shall adhere to any regulatory requirements such as notifications required by applicable legislation.

4 REDISTRIBUTION OF DATA

4.1 Service Providers can redistribute Data to Third Party End Users only if permitted under the applicable Dataset Terms of Use. The Parties are entitled to redistribute Derived Materials to any Third Party End Users, unless specifically prohibited in the applicable Dataset Terms of Use and provided that the Data Provider's Intellectual Property Rights do not restrict such redistribution. However, the redistribution of any Personal Data or Derived Materials created on the basis of any Personal Data is always subject to the more detailed requirements disclosed in the applicable Dataset Terms of Use and applicable data protection laws.

4.2 Where the Data Provider permits the redistribution of Data to Third Party End Users, the Data Provider is responsible for defining further the applicable terms and conditions for the redistribution of Data in the respective Dataset Terms of Use. Service Providers are obliged to include such terms and conditions in any agreements they conclude with their Third Party End Users with regard to the redistribution of Data.

4.3 Notwithstanding the above, the Parties are entitled to redistribute any Data to their Affiliates, unless such redistribution is specifically prohibited in the applicable Dataset Terms of Use. Each Party will be responsible for ensuring that its respective Affiliates comply with the terms and conditions of the Constitutive Agreement.

5 GENERAL RESPONSIBILITIES

5.1 Data security, protection and management

5.1 Each Party must designate a contact person for data security matters, who is responsible for the relevant Party's data systems that are connected to the Network and for the implementation of the Party's security policy.

5.2 Each Party to the Data Network must have, sufficient capabilities to process Data securely and in accordance with the relevant data security standards and data protection legislation. The Parties must implement and maintain suitable technical, organisational and physical measures that are in line with good market practice, by taking into account the nature of the Data processed by the Party. Each Party must have the capability to properly perform its obligations under the Constitutive Agreement and applicable Dataset Terms of Use and, where necessary, to cease processing activities without undue delay for any relevant reason.

5.3 The aforementioned capabilities include e.g., the capability to control Data and its processing by being aware of

(i) the origins of the Data (specifically whether the origin is the Party itself, another Party or Third Party);

(ii) the basis for processing Data;

(iii) the restrictions and limitations that apply to processing Data; and

(iv) the rights and restrictions that apply to redistributing or refining Data.

5.4 Parties must also be capable of recognising Data and removing or returning it if the basis for the processing of Data expires. the obligation to remove or return Data is not applicable to Derived Materials.

5.5 Any identified data security breaches must be duly documented, rectified and reported to the affected Parties without undue delay. All involved Parties have a mutual responsibility to contribute reasonably to the investigation of any data security breaches within the Network.

5.2 Subcontractors

5.6 The Parties will have the right to employ subcontractors to perform their obligations under the Constitutive Agreement. Where and to the extent that the outsourced functions require it, the Parties may allow their subcontractors to access Data. The Parties will be responsible for the subcontracted performance as for their own.

6 FEES AND COSTS

6.1 Data is shared within the Network free of charge, unless otherwise defined in the applicable Dataset Terms of Use.

6.2 Each Party will bear their own costs related to accessing the Network and operating as a Member of the Network.

6.3 Unless otherwise agreed by Parties, the joint costs incurred for the maintenance and administration of the Network will be allocated in equal shares between the Parties. For the avoidance of doubt, the maintenance and administration of the Network does not include the costs of Data where applicable and as defined in the Dataset Terms of Use in question.

7 CONFIDENTIALITY

7.1 The Parties must use any Confidential Information they receive in connection with the operation of the Data Network and/or regarding the Data Network only for the purposes for which such Confidential Information has been provided. The Parties must not unlawfully use or disclose to Third Parties any such Confidential Information they have become aware of in the course of the operation of the Data Network.

7.2 At the expiration or termination of the Constitutive Agreement, the Parties must cease to use Confidential Information and, upon request by any Party, verifiably return or destroy any copies thereof. Notwithstanding the above, the Parties are entitled to continue to use the Data subject to clause 10.2. In addition, the Parties may retain copies of Confidential Information as required by the applicable law or competent authorities.

7.3 If a Party is, under the applicable law or an order issued by a competent authority, obliged to disclose another Party's Confidential Information to the authorities or Third Parties, the obliged Party must promptly notify the affected Party whose Confidential Information will be disclosed of such disclosure if so permitted under the applicable law or the competent authority's order.

7.4 The confidentiality obligations established in the General Terms and Conditions will survive the termination of the Constitutive Agreement.

8 INTELLECTUAL PROPERTY RIGHTS

8.1 The Intellectual Property Rights of the Parties must be respected and protected in connection with the operation of the Data Network.

8.2 Signing the Constitutive Agreement and sharing any Data within the Network does not result in the transfer of any Intellectual Property Rights. More specific provisions, if any, concerning the Intellectual Property Rights that relate to specific Datasets are included in the applicable Dataset Terms of Use. For the avoidance of doubt, any new Intellectual Property Rights created by a Party will vest in the creating Party as further defined in the applicable legislation governing Intellectual Property Rights.

8.3 Where the Data Provider charges the other Parties a fee for its Data, the Data Provider indemnifies the paying Parties against claims that the Data subject to any such fees infringes Intellectual Property Rights in the country of the Data Provider, provided that the Data Provider is notified of these claims in writing without undue delay.

8.4 The Parties are entitled to utilise software robots or other forms and applications of robotic process automation or machine learning or artificial intelligence when processing Data, provided that they respect the confidentiality obligations set out in clause 7 and the data protection obligations set out in clause 9. In accordance with the aforementioned and the applicable Dataset Terms of Use, the Parties have the right to learn from Data and to use any professional skills and experience acquired when processing Data.

9 DATA PROTECTION

9.1 Any Personal Data processed within the Data Network must be processed in accordance with the applicable data protection laws and regulations.

9.2 Terms that are not defined here, have the meaning stated in the GDPR or other applicable data protection laws.

9.3 For the purposes of processing Personal Data within the Network, any Parties disclosing or receiving Data are, individually and separately, assumed to be controllers under the provisions of the GDPR. The said Parties are also assumed to be processing Data on their own behalf unless the Parties have concluded a written Data Processing Agreement that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of data subjects and the obligations and rights of the controller and the processer. Where any such Data Processing Agreement is applicable in general to certain Dataset(s) or services provided under the Constitutive Agreement, it must be included as an Appendix to the Constitutive Agreement.

9.4 The Parties must prevent the unauthorised and unlawful processing of Personal Data by employing appropriate technical and organisational measures. The Parties must ensure that persons allowed to process Personal Data have committed to keeping such data confidential or are bound by an appropriate statutory obligation of confidentiality.

9.5 Personal Data that is shared within the Network can be transferred within the European Union and the European Economic Area (EEA). This kind of Personal Data can also be transferred outside the EU and the EEA in compliance with the data protection regulations, unless otherwise prescribed by the applicable Dataset Terms of Use.

10 TERMINATION AND VALIDITY

10.1 If the Constitutive Agreement is concluded for a fixed period, it will expire without separate notice at the end of the applicable fixed period. If the Constitutive Agreement is concluded for an indefinite period, it will expire upon termination by the Parties.

10.2 The Parties are entitled to continue to use any Data received through the Network prior to the termination of the Constitutive Agreement, unless otherwise determined in the applicable Dataset Terms of Use or agreed by the Parties in the Constitutive Agreement. In such case, the clauses governing use of Data in these General Terms and Conditions, Dataset Terms of Use and/or in the Constitutive Agreement, remain in force according to the Clause 17.1.

10.3 Any Party may choose to terminate the Constitutive Agreement as defined in the Constitutive Agreement. Notice of termination must be provided in writing to the Parties of Constitutive Agreement. In the event that there are more than two Parties to the Constitutive Agreement, the Constitutive Agreement will remain in force for the remaining Parties following the termination thereof by one Party.

10.4 Where the Parties have agreed on a process for amending the Constitutive Agreement otherwise than by the written consent of all Parties, any Party that objects to such an amendment in writing after having become aware of it will be entitled to terminate the Constitutive Agreement by notifying the other Parties thereof. The termination will become effective after the objecting Party has submitted the aforementioned notice to the other Parties, after which the amendment will enter into force unless the agreeing Parties have agreed on a later date.

10.5 In the event that there are only two Parties to the Constitutive Agreement and one Party commits a material breach of the provisions of the Constitutive Agreement, the other Party will have the unilateral right to terminate the Constitutive Agreement with immediate effect by providing the other Party with a written notice.

10.6 In the event that there are more than two Parties to the Constitutive Agreement and one Party commits a material breach of the provisions of the Constitutive Agreement, the other Parties together and unanimously will have the right to terminate the Constitutive Agreement with the breaching Party with

immediate effect. Such a termination may either concern the contractual relationship between the breaching Party and other Parties or the entire Constitutive Agreement. if the material breach is of substantial importance only to certain non-breaching Parties, such Parties are individually and separately entitled to terminate the Constitutive Agreement unilaterally with the breaching Party. Notice of any such termination must be provided in writing to all Parties.

10.7 If the breach can be rectified, the non-breaching Party/Parties may resolve to suspend the performance of their obligations under the Constitutive Agreement until the breaching Party has rectified the breach.

11 LIABILITY

11.1 The Parties will only be liable for direct damages that result from a breach of the provisions of the Constitutive Agreement as defined hereinafter and where applicable, in the Constitutive Agreement. Any other liabilities are hereby excluded, unless otherwise specifically defined in the Constitutive Agreement. Parties are not liable for loss of profits or damage that is due to a decrease or interruption in production or turnover, or other indirect or consequential damages.[3]

11.2 The Parties will not be liable for any losses, damages, costs, claims or expenses howsoever arising from a mechanical or electrical breakdown or a power failure or any other cause beyond the reasonable control of the Party; and

11.3 the Parties must fully compensate any damages resulting from an intentional or grossly negligent breach of the provisions set out in the Constitutive Agreement.

11.4 The Data Provider must indemnify paying Parties against claims that its Data infringes Intellectual Property Rights in accordance with clause 8.3.

11.5 Each Party, severally and not jointly, will be liable for any infringements of personal data obligations set out in the GDPR in accordance with Article 82 of the GDPR.

12 FORCE MAJEURE

12.1 No Party will be liable for injuries or damage that arise from events or circumstances that could not be reasonably expected beforehand and are beyond its control (*force majeure*).

12.2 A Party that is unable to perform its obligations due to an event of force majeure must inform other Parties of any such impediment without undue delay. These grounds for non-performance will expire at the moment that the force majeure event passes. This clause is subject to a long-stop date: where performance is prevented for a continuous period of one hundred and eighty (180) days or more, the Parties are entitled to terminate the Constitutive Agreement as set forth in clause 10.5 or 10.6, as applicable.

13 AUDIT

13.1 A Data Provider will be entitled to audit the Parties processing the Data made available by the Data Provider at its own expense, including also material and reasonable direct costs of the audited Party. The purpose and the scope of the audit is limited to verifying compliance with the material requirements of the Constitutive Agreement, the applicable Dataset Terms of Use, and applicable legislation.

13.2 The obligations of the audited Party as set out herein will apply to all of its Affiliates and subcontractors that process the respective Data Provider's Data. The Parties represent and warrant that the same auditing obligations as set out herein will be imposed on their Affiliates and subcontractors, where reasonably available and where limited, and the Parties will act in good faith to ensure that the objectives of the Data Provider's audit rights materialise.

[3] Parties may wish to note that the concept of indirect or consequential damage varies between different jurisdictions.

13.3 The auditing Party must notify the audited Party of the audit in writing at least thirty (30) days prior to the audit. The written notice must disclose the scope and duration of the audit and include a list of requested materials and access rights.

13.4 The audited Party is entitled to require that the audit is conducted by a mutually acceptable and/or certified independent Third Party.

13.5 The Parties are required to retain and provide to the auditing Party and/or the Third Party auditor, for the purposes of the audit, all records and documents as well as access to all necessary data systems and premises and to interview personnel that are of significant importance for the audit. Records and documents thus retained must span to the previous audit or to the accession of the audited Party to the Network, whichever is later.

13.6 The auditing Party and/or Third Party auditor may only request such records and documents and such access to data systems and premises and to interview personnel that are of significant importance to the audit.

13.7 All records, documents and information collected and disclosed in the course of the audit constitute Confidential Information. The auditing Party and/or Third Party auditor may not unlawfully utilise or disclose Confidential Information that it has become aware of in the course of the audit. The auditing Party represents and warrants that any Third Party auditor, where applicable, complies with the applicable confidentiality obligations. The audited Party is entitled to require that the auditing Party and/or Third Party auditor or any other persons participating in the audit sign a personal non-disclosure agreement provided that the terms and conditions of such a non-disclosure agreement are reasonable.

13.8 The results, findings and recommendations of the audit must be presented in an audit report. The audited Party is entitled to review any Third Party auditor's audit report in advance (and prior to it being provided to the relevant Data Provider(s) by the Third Party auditor). The audited Party is entitled to require the Third Party auditor to make any such changes to the audit report that are considered reasonable while taking into account the audited Party's Confidential Information and the applicable Data Provider's business interests in the Data. The audited Party must provide its response to the audit report within thirty (30) days. If no response is provided, the audited Party is considered to have accepted the contents of the report.

13.9 If the auditing Party justifiably believes the audited Party to be in material breach of the obligations imposed thereupon in the Constitutive Agreement, an additional audit may be conducted.

13.10 In the event that the audit reveals a material breach of the obligations imposed in the Constitutive Agreement or the applicable Dataset Terms of Use, the audited Party will be liable for reasonable and verifiable direct expenses incurred as a result of the audit.

14 APPLICABLE LAWS AND DISPUTE RESOLUTION

14.1 The agreement incorporating these General Terms and Conditions is governed by and construed in accordance with the laws of Finland without regard to its principles of private international law and conflict of laws rules.

14.2 Any dispute, controversy or claim arising out of or in relation to the agreements based on the General Terms and Conditions, or the breach, termination or validity thereof, shall be finally settled by arbitration in accordance with the Arbitration Rules of the Finland Chamber of Commerce. The number of arbitrators shall be one, the seat of arbitration shall be Helsinki, Finland and the language of the arbitration shall be English.

15 OTHER PROVISIONS

15.1 Unless otherwise agreed by the Parties, any amendments to the Constitutive Agreement and its Appendices must be made in writing and signed by all Parties.

15.2 No Party may assign the Constitutive Agreement, either wholly or in part, without a written consent of the other Party/Parties. Notwithstanding the previous, no consent shall be required where the assignee is a company that belongs to the same group of companies as the Party pursuant to the provisions of the Finnish Accounting Act.

15.3 If any provision of the Constitutive Agreement or any applicable Dataset Terms of Use is found to be invalid by a court of law or other competent authority, the invalidity of that provision will not affect the validity of the other provisions established in the Constitutive Agreement.

15.4 Each party represents and warrants that it is validly existing and in good standing under the applicable laws of the state of its incorporation or registration. Each Party also represents and warrants that it has all required power and authority to execute, deliver, and perform its obligations under the Constitutive Agreement and, where applicable, to bind its Affiliates.

15.5 The Parties intend to create a Data Network that is subject to a single set of contractual terms, and nothing contained in the Constitutive Agreement may be construed to imply that they are partners or parties to a joint venture or the other Parties' principals, agents or employees. No Party will have any right, power, or authority, express or implied, to bind any other Party.

15.6 No delay or omission by any Party hereto to exercise any right or power hereunder will impair such right or power, nor may it be construed to be a waiver thereof. A waiver by any of the Parties of any of the covenants to be performed by the other Parties or any breach thereof may not be construed to be a waiver of any succeeding breach thereof or of any other covenant.

16 NOTICES

16.1 All notices relating to these General Terms and Conditions and the Constitutive Agreement must be sent in a written or electronic form (including post or email) or delivered in person to the contact person and/or address specified by the respective Party in the Constitutive Agreement or in the applicable Accession Agreement. Each Party will be responsible for ensuring that their contact details are up-to-date. Notices will be deemed to have been received three (3) days after being sent or on proof of delivery.

17 SURVIVAL

17.1 Clauses 1, 2, 3, 4, 5, 8, 9, 11, 14, 16 and 17 of these General Terms and Conditions will survive the termination of the Constitutive Agreement in its entirety together with any clauses of the Constitutive Agreement that logically ought to survive the termination.

17.2 Clause 13 of these General Terms and Conditions will survive for a period of three (3) years following the termination of the Constitutive Agreement in its entirety.

17.3 Clause 7 of these General Terms and Conditions will survive for a period of five (5) years following the termination of the Constitutive Agreement in its entirety.

4.2 Constitutive Agreement [Template]

PARTIES

(1) [Founding Member no. 1]

(2) [Founding Member no. 2]

(3) […][4]

(Together the "**Parties**" or "**Founding Members**".)

Appendix	Description
1	Description of the Data Network[5]
2	General Terms and Conditions
3	List of Members and Contact Details[6]
4	Governance Model
[5] [7]	[Any other Appendices]
[●]	[Code of Conduct][8]

BACKGROUND AND PURPOSE

The Parties are contemplating the establishment of a Data Network in order to [●][9].

DEFINITIONS

As used in this Agreement, including the preamble and the Appendices hereof, unless expressly otherwise stated or evident in the context, the following terms and expressions have the following meanings, the singular (where appropriate) includes the plural and vice versa, and references to Appendices and Sections mean the Appendices and Sections of this Agreement:

"Chair"	has the meaning set forth in Appendix 4.
"Qualified Majority"	has the meaning set forth in Appendix 4.

[4] **Note**: Please fill in the corporate details of the Founding Members.

[5] **Note**: Please append, where appropriate, any Business or Technical documentation prepared as a result of completing the Checklist for the Rulebook as an Appendix.

[6] **Note**: This Appendix should include a list of Members and necessary contact details.

[7] **Note**: Please list all Appendices, such as a Technical appendix describing e.g. APIs (to the extent not included in Appendix 1), Operator Service Agreement, Data Provider Service Level Agreement, and fixed term commitments or reciprocity of Data Provider(s) to share Data (where applicable) as well as any technical or data security specifications. Where the Network involves an Operator, the Members should consider whether the Operator should be a Member of the Network. This could provide benefits with regard to governance and the effective management of contractual relations.

[8] **Note**: As the Code of Conduct includes principles regarding the Data Network, the Founding Members may consider appending the Code of Conduct as an Appendix to the Constitutive Agreement, in which case it is recommended that it be placed after the more detailed and/or technical Appendices in the order of precedence.

[9] **Note**: The background and purpose of the Data Network should be described herein.

"Representatives"	has the meaning set forth in Appendix 4.
"Secretary"	has the meaning set forth in Appendix 4.
"[defined term]"[10]	means [definition]

Other terms and expressions have the meanings defined in **Appendix 2** (General Terms and Conditions).

THE NETWORK

The undersigned hereby establish a Data Network that is further described in **Appendix 1** (Description of the Data Network).

[The Parties agree that new Members may join the Data Network subject to the following conditions:.][11] **Appendix 3** (The List of Members) will be updated upon the accession of new Parties, the termination of incumbent Parties or any changes in the representatives or their contact details.

[The ethical principles that apply to the Networks are laid down in Appendix [5] (Code of Conduct). The Parties agree to comply with these ethical principles in good faith in connection with their conduct within the Network.][12]

The Data Network is subject to the following provisions:[13]

NO EXCLUSIVITY[14]

Nothing in this Agreement prevents or restricts the Parties from participating in any other data networks, platforms, ecosystems or any other cooperation or from using any services provided by Third Parties. Furthermore, sharing any of the Data within the Network does not prevent or restrict the respective Data Provider from sharing such Data with Third Parties at its own discretion.

GOVERNANCE OF THE NETWORK

The governance framework that applies to the Network is defined in further detail in **Appendix 4**[15].

The Parties agree to appoint necessary representatives to the governing bodies as defined in **Appendix 4**, and the Parties represent and warrant that their representatives are duly authorised to represent the relevant Party in the governing bodies. Furthermore, the Parties acknowledge any decisions made by the governing bodies as legally effective and binding upon the Parties under this Agreement.

---

[10] **Note**: Please list herein, where applicable, any definitions introduced in the Constitutive Agreement or its Appendices (other than General Terms and Conditions).

[11] **Note**: Please consider whether and to which extent new Members may join the Data Network and if any further accession criteria should apply to such new Members. Please consider also, if the Founding Members want to define role-specific preconditions for accession.

[12] **Note:** This is relevant only where the Conduct of Conduct is appended to the Constitutive Agreement.

[13] **Note**: It should be noted that the General Terms and Conditions focus mainly on governing the Data within the Network and the Parties should agree under this clause on Network specific matters and its Members in further detail. The Members' rights and obligations regarding the Network during its life cycle should be described herein in further detail. This should include the Members' Data and/or service delivery obligations but also, where applicable, their payment obligations. The Parties should consider entering into a separate project agreement if the establishment of the Network requires material investments and carrying out a project, and in such case, the Parties may consider attaching the project agreement to this Agreement and/or agree in this Agreement on sharing the project costs with new Members.

[14] **Note**: A lack of exclusivity has been adopted as the baseline, but this should not prevent the Founding Members from requiring exclusivity where it is deemed necessary. The Founding Members should carefully assess the need for exclusivity, as it may e.g. result in the need to carry out further competition law analysis.

[15] **Note**: The wording of the template for the Governance Model is relatively general as the governance requirements for different types of Data Networks may vary significantly. As a result, the Members should consider amending the Governance Model template to meet the requirements of the respective Data Network and its life cycle.

DEROGATIONS TO THE GENERAL TERMS AND CONDITIONS

The Parties have agreed to replace the following clauses of the General Terms and Conditions as follows:[16]

[**Examples**:

(i) Clause 4.1: "The Service Providers are entitled to redistribute any Data made available to the Network and any Derived Materials to Third Party End Users without limitations."; and

(ii) Clause 17.3: "Clause 7 of these General Terms and Conditions will survive for a period of three (3) years following the termination of the Constitutive Agreement in its entirety."]

TERMINATION AND VALIDITY[17]

This Agreement is concluded [for a fixed period of [●] [months/years]] from the Effective Date after which it remains in force for an indefinite period and is subject to a termination period of [●] months.

NOTICES

Any notices provided under this Agreement must be submitted in writing to the Representatives listed in the Appendix 3.[18]

Any change in contact persons or relevant contact details must be disclosed immediately by the respective Party to [the secretary of the Steering Committee].[19]

LIMITATION OF LIABILITY

[The annual total liability of any Party[20] under this Agreement must not exceed the greater of (i) [●] euro; or (ii) [●] per cent of the aggregate fees payable to the breaching party under this Agreement in the [twelve-month (12 months) period preceding the cause of action giving rise to claim under this clause, whichever is greater.]

Notwithstanding any limitations of liability, General Data Protection Regulation (GDPR), Article 82 is applied to damages related to personal data. The above-mentioned limitation of liability does not limit the controller's right to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage in accordance with the GDPR Art. 82.

OTHER TERMS[21]

ENTRY INTO FORCE AND APPLICATION

This Agreement will enter into force when [executed (signed) by all Parties OR on _____ 20___].

---

[16] **Note**: Any amendments to or derogations from the General Terms and Conditions should be disclosed herein, e.g. in line with the example.

[17] **Note**: Please fill in the necessary details for the term and termination.

[18] **Note**: The Members may want to name a different contact person for formal notices and operational notices in Appendix 3.

[19] **Note**: Appendix 4 – Governance Model describes the duties of the secretary of the Steering Committee.

[20] **Note**: Please consider whether liability caps should be defined separately and differently for various roles.

[21] Note: Please consider any other terms that could be relevant to the Network, such as non-solicitation, marketing and promotional activities.

APPLICABLE LAWS AND DISPUTE RESOLUTION

This Agreement is governed by and construed in accordance with the laws of Finland without regard to its principles of private international law and/or conflict of laws rules.

Any dispute, controversy or claim arising out of or in relation to the agreements based on the General Terms and Conditions, or the breach, termination or validity thereof, shall be finally settled by arbitration in accordance with the Arbitration Rules of the Finland Chamber of Commerce. The number of arbitrators shall be one, the seat of arbitration shall be Helsinki, Finland and the language of the arbitration shall be English.

COUNTERPARTS

This agreement has been executed in [ ] identical counterparts, one for each Party [and one for the Steering Committee].

In _____, on _____ 20

[Signatures on the next page]

[PARTY 1]

_____

Name: [Name]
Title: [Title]

[PARTY 2]

_____

Name: [Name]
Title: [Title]

[PARTY 1]

_____

Name: [Name]
Title: [Title]

[PARTY 2]

_____

Name: [Name]
Title: [Title]

4.3 Accession Agreement [Template]

ACCEDING PARTY

(1) [Acceding Party][22]

APPENDICES

Appendix	Description
1	Constitutive Agreement
1.1	Description of the Data Network
1.2	General Terms and Conditions
1.3	List of Members and Contact Details
1.4	Governance Model
1.5	Code of Conduct
1.6	[Any other Appendices to the Constitutive Agreement][23]

BACKGROUND

The Acceding Party has expressed its interest to accede to the Constitutive Agreement regarding [●] that was signed on [●].[24]

The Constitutive Agreement allows new [Parties][25] to accede the Data Network [provided that [●].[26]

DEFINITIONS

As used in this Agreement, including the preamble and the Appendices hereof, unless expressly otherwise stated or evident in the context, the following terms and expressions have the following meanings, the singular (where appropriate) includes the plural and vice versa, and references to Appendices and Sections mean the Appendices and Sections of this Agreement:

"Acceding Party"	means the entity defined under section Acceding Party.
"Accession Agreement"	means this Agreement.
"Constitutive Agreement"	means the Constitutive Agreement regarding Data Network on [●], dated [●].
"[defined term]"	means [definition].

[22] **Note:** Please insert the Acceding Party's details herein.

[23] **Note**: Please include the full list of Appendices herein.

[24] **Note**: Please insert a reference to the Data Network herein.

[25] **Note**: The Founding Members may consider it relevant to define role-specific preconditions for accession, and it may be necessary to detail herein the role(s) as which the Acceding Party joins the Network.

[26] **Note**: Please include, where applicable, a reference to the conditions for new Members of the Data Network herein.

ACCESSION TO THE CONSTITUTIVE AGREEMENT

The Acceding Party has expressed its interest in acceding to the Constitutive Agreement, and the Constitutive Agreement allows new Parties to accede to the Data Network [, subject to [●]].[27]

As the Acceding Party fulfils such requirements, the Acceding Party accedes to the Constitutive Agreement and to the Data Network under this Accession Agreement.

ENTRY INTO FORCE AND APPLICATION

This Accession Agreement will enter into force as of its execution by the Acceding Party and after it has been duly approved by the Data Network's Steering Committee.

APPLICABLE LAWS AND DISPUTE RESOLUTION

This Agreement is governed by and construed in accordance with the laws of Finland, without regard to its principles of private international law and conflict of laws rules.

Any dispute, controversy or claim arising out of or in relation to the agreements based on the General Terms and Conditions, or the breach, termination or validity thereof, shall be finally settled by arbitration in accordance with the Arbitration Rules of the Finland Chamber of Commerce. The number of arbitrators shall be one, the seat of arbitration shall be Helsinki, Finland and the language of the arbitration shall be English.

COUNTERPARTS

This agreement has been executed in [●][28] identical counterparts, one for [each Party/Acceding Party and one for the Steering Committee].

In _____, on _____ 20

[Signatures on the next page]

[27] **Note**: Please include, where applicable and as defined in the Constitutive Agreement, the conditions for new Members of the Data Network herein.

[28] **Note**: Please note that this information is subject to the accession process and its governance (e.g. whether the Steering Committee has the authority to approve new Members or whether the Accession Agreement should be signed by each incumbent Member).

[PARTY 1]

_____

Name: [Name]
Title: [Title]

[PARTY 2]

_____

Name: [Name]
Title: [Title]

[PARTY 1]

_____

Name: [Name]
Title: [Title]

[PARTY 2]

_____

Name: [Name]
Title: [Title]

4.4 Dataset Terms of Use [Template]

DATA PROVIDER

_____ acts as the Data Provider.

SCHEDULES

Schedule	Description
1	Dataset Description [no. 1][29]
2	

BACKGROUND

The purpose of this Dataset Terms of Use is to define, the Data that the Data Provider makes available through the Network and to set out the terms and conditions for the use of such Data.

DEFINITIONS

As used in this Dataset Terms of Use, including the Schedules hereof, unless expressly otherwise stated or evident in the context, the following terms and expressions have the following meanings, the singular (where appropriate) includes the plural and vice versa, and references to Schedules and Sections mean the Schedules and Sections of this Dataset Terms of Use:

”Data Provider”	means the entity defined under section “Data Provider” above.
”User”	means any End User, Service Provider, Operator or Third Party End User who processes any Data that is made available by the Data Provider under these Dataset Terms of Use. [Otetaan kontrollilistaan kysymys siitä, että miten eri skenaarioissa mm. datan edelleen jakelu ja siihen liittyvät ehdot on määriteltävä]
"[defined term]"[30]	means [definition]

Other terms and expressions have the meanings defined in the General Terms and Conditions.

APPLICABILITY AND SCOPE

These Dataset Terms of Use apply to the Dataset(s) provided by the Data Provider under the Constitutive Agreement [dated [●] [●] 202[●] / as acceded by the Data Provider under the Accession Agreement dated [●] [●] 202[●]][31] and as further defined in **Schedule 1**.

By using any such Data, the User undertakes to use the Data in compliance with these Dataset Terms of Use.

[29] **Note**: Where the Data Provider provides several Datasets under the Dataset Terms of Use, the Data Provider may prefer to include individual Dataset Descriptions as separate Schedules herein. It should be noted that, where the terms and conditions for different Datasets are different, the Data Provider must define separate Dataset Terms of Use for any such Datasets.

[30] **Note**: Please list herein, where applicable, any definitions introduced in these Dataset Terms of Use.

[31] **Note:** Please edit based on the date on which the Data Provider has become a party to the Constitutive Agreement.

In the event that a discrepancy arises between the Constitutive Agreement or any of its appendices and these Dataset Terms of Use, these Dataset Terms of Use and its Schedules will prevail. Furthermore, in the event that a discrepancy arises between these Dataset Terms of Use and any of its Schedules, these Dataset Terms of Use will prevail.

DATA

The Data as well as its location and method of distribution are defined in the Dataset Description(s) (**Schedule 1[- ●]**[32]).

The Data Provider represents and warrants that it has the right to make the Data available and that the data recipients are entitled to use the Data as further defined in the Constitutive Agreement and these Dataset Terms of Use.

RIGHT TO USE THE DATA

Subject to these Data Set Terms of Use, the Data Provider hereby grants the User a non-exclusive right to the Data to[33]

(1) receive, process and reproduce[34];

(2) refine and modify; and

(3) [redistribute][35] the Data to Third Party End Users provided that the Service Provider includes in its agreement with any Third Party End User the terms and conditions of this Dataset Terms of Use / clauses […][36] of this Dataset Terms of Use

in [Finland/the European Union and the European Economic Area/globally].

The User is entitled to utilise software robots or other forms and applications of robotic process automation or machine learning or artificial intelligence when processing Data provided that the applicable confidentiality obligations are respected. In accordance with the aforementioned, the User has the right to learn from the Data and to use any professional skills and experience acquired when processing the Data.

RESTRICTIONS ON THE PROCESSING OF DATA

The Data may not be processed for [●].[37]

FEES AND PAYMENT TERMS

The use of Data is subject to fees and charges, as further defined in **Schedule 1**.[38]

---

[32] **Note**: Where applicable, please add references to additional Schedules.

[33] **Note**: The list hereinafter provides an example of the matters to be included in this clause with regard to the right to use the Data. The Data Provider and/or the Members of the Network may want to consider preparing a more specific Network specific template(s) for the Dataset Terms of Use to reflect the business context of the Network.

[34] **Note**: Please note that Derived Materials can be distributed to Third Parties without restrictions. Thus, it is important that the Data Provider considers on a case-by-case basis whether

[35] **Note**: Please note that, in accordance with the General Terms and Conditions (clause 4), Data can be redistributed to Third Party End Users only if permitted under the applicable Dataset Terms of Use. As such, please remove the redistribution right where it does not apply to a specific Dataset(s).

[36] **Note**: Alternatively, the Members or the Data Provider may want to prepare a separate Schedule, including any terms and conditions that must be included in any redistribution agreements.

[37] **Note**: Please describe herein any specific restrictions that apply to the Dataset(s).

[38] **Note**: Where applicable, any fees or charges related to the Data should be defined and referred to herein as the default option under clause 6.1 of the General Terms and Conditions is that the Data is provided free of charge.

REPORTING

The use of Data is subject to the following specific reporting obligations: [●].[39]

AUDIT

The use of Data is subject to the following specific audit obligations: [●].[40]

DATA SECURITY

The use of Data is subject to the following specific data security obligation: [●].[41]

CONFIDENTIAL INFORMATION

The Parties acknowledge that the Dataset, as defined in **Schedule [1]**, includes Confidential Information and that its use and processing is subject to: [●].[42]

DATA PROTECTION

The Data includes personal data, and its reception and processing is subject to the following: [●].[43]

INTELLECTUAL PROPERTY RIGHTS

[●][44]

DISCLAIMER AND LIMITATION OF LIABILITY

[**Example**: Unless otherwise expressed in these Terms, the Data Provider offers the data "as is" and "as available" with no warranty of any kind. The risk inherent in the suitability of the data for the User's purposes remains solely with the User. Notwithstanding the above, this does not limit the Data Provider's liability under clauses 11.3–11.5 of the General Terms and Conditions [and clause(s) of the Constitutive Agreement]].[45]

EFFECTS OF TERMINATION

[**Example**: Where a Member's membership in the Network is terminated as a consequence of the Member's material breach of the Constitutive Agreement, the breaching Member's right to use the Data will end at the date of the termination. The breaching Member must cease to use the Data and, upon request by any Party, verifiably return or destroy Data and any copies of Confidential Information including copies thereof. However, the breaching Member is entitled to retain the Data as required by the applicable law or

---

[39] **Note**: Please describe herein, where applicable, any specific reporting obligations that apply to the use of the Dataset(s).

[40] **Note**: Please describe herein, where applicable, any specific conditions for audits (see clause 13 of the General Terms and Conditions and the Constitutive Agreement).

[41] **Note**: Please describe herein, where applicable, any specific data security requirements for the Dataset(s) (see clause 5 of the General Terms and Conditions and the Constitutive Agreement).

[42] **Note**: Where the Dataset(s) include Confidential Information, the Data Provider should detail herein any specific requirements it deems necessary in order to make the Data available within the Network.

[43] **Note**: Clause 9 (see below) of the General Terms and Conditions defines the default terms and conditions that apply to data protection. In the event that the Data includes personal data, the Data Provider must consider defining herein the terms and conditions for the transfer and processing of personal data in further detail. In addition, further consideration is required where the Data includes personal data (or anonymised personal data), which would be redistributed to Third Party End Users.

[44] **Note**: Where the Data Provider considers it necessary to derogate from the default approach for Intellectual Property Rights (clause 8 of the General Terms and Conditions), Dataset specific derogations should be described herein. However, to manage the Intellectual Property Rights effectively, the Members should consider whether it would be feasible to define the default approach to Intellectual Property Rights for the Network by establishing a standard template for Dataset Terms of Use that apply to the specific Network.

[45] **Note**: Clause 11 of the General Terms and Conditions sets out provisions that apply to the limitation of liability. Any Dataset specific derogations regarding liability should be defined herein. Please note, where applicable, that the Members may have derogated from the liability clauses of the General Terms and Conditions, in which case such liability clauses should be referred to herein for clarity.

competent authorities provided that the breaching Member notifies the Data Provider of such a data retention obligation by the date of termination.][46]

ENTRY INTO FORCE AND APPLICATION

This right to use the Data will enter into force when the User accesses the Data and apply until the User stops processing the Data.

AMENDMENTS

The Data Provider may change these terms and conditions at any time by notifying all other Members to the Network of such change in writing. The modified terms will enter into force within thirty (30) days after the Data Provider has notified the other Members of the amendments made to these terms and conditions, but the amendments will not apply to any Data received by the Users prior to the entry into force of the amendments.

OTHER TERMS

[●][47]

[APPLICABLE LAWS AND DISPUTE RESOLUTION[48]

These Dataset Terms of Use are governed by and construed in accordance with the laws of Finland, without regard to its principles of private international law and conflict of laws rules.

Any dispute, controversy or claim arising out of or in relation to the Data shared under these Dataset Terms of Use, or the breach, termination or validity thereof, shall be finally settled by arbitration in accordance with the Arbitration Rules of the Finland Chamber of Commerce. The number of arbitrators shall be one, the seat of arbitration shall be Helsinki, Finland and the language of the arbitration shall be English.]

[46] **Note**: Clause 10.2 of the General Terms and Conditions allows the Parties to continue to use the Data during the term of the Constitutive Agreement notwithstanding its termination. The Data Providers and Members should consider the effects a Member's material breach of the agreement would have and include e.g. the following clause in the Dataset Terms of Use:

[47] **Note**: The Data Provider (and the Members of the Network) should consider, on a case-by-case basis, whether any other terms regarding the use of Data are considered necessary.

[48] **Note**: Please note that this clause is potentially relevant only where the Data can be redistributed to Third Party End Users as one of the conditions, which should be included in the agreement governing the redistribution of the Data to Third Party End Users.

4.5 Governance Model [template][49]

GENERAL PROVISIONS

The Data Network is established by the Constitutive Agreement, which is signed by the Members of the Network. This Appendix includes a description of the Governance Model of the Data Network.

The purpose of the Governance Model is to define the procedures and mandates for managing the Data Network and any related changes during the life cycle of the Data Network.

The Constitutive Agreement must include, as **Appendix 3**, a List of Members that also sets out the Parties to the Constitutive Agreement and the contact details of their representatives. The List of Members must be updated upon the accession of new Parties and the termination of incumbent Parties as well as when any contact details are changed.

STEERING COMMITTEE

General

The Steering Committee is the ultimate decision-making body of the Data Network. The purpose of the Steering Committee is to facilitate collaboration between the Parties and organise the administration of the Network appropriately on a strategic level. The Steering Committee also decides on matters that may have a significant financial or risk impact on the Parties.

Primary Functions

The Steering Committee is established to ensure the coordination of and any decision making related to the Data Network's business or to its legal, technical or ethical matters. The Steering Committee is responsible for preparing any changes required to ensure that the Data Network continues to fulfil its purpose and meets the applicable requirements.

The Steering Committee is authorised to prepare any changes to the Constitutive Agreement or any of its Appendices and to approve any new Members to the Data Network in accordance with the accession criteria defined in the Constitutive Agreement. The Steering Committee is also authorised to approve new Datasets and/or Dataset Terms of Use, where (if any) such approval is required.

Composition, Meetings and Organisation

Each Party appoints one representative to serve on the Steering Group (hereinafter referred to as the "Representatives"). The Steering Committee will select a chairperson (hereinafter the "Chair") and a secretary (hereinafter the "Secretary"). The Secretary cannot simultaneously serve as a Representative. The Chair will lead the Steering Committee meetings or appoint a Representative to lead the meeting in the Chair's stead.

Each Representative 1) should strive to be present or represented at all meetings; 2) may appoint a substitute or a proxy to attend and vote at any meeting; and 3) must participate in the meetings in the spirit of cooperation.

The Chair must convene an ordinary meeting of the Steering Group at least once every [three (3) months]. The Chair must convene an extraordinary meeting at any time upon the written request of the Chair or any Representative. Before scheduling an extraordinary meeting, the Chair or the Representative that has

[49] **Note**: This template only serves as a general description of the governance rules that could apply to the relevant Network. The Members should consider, where applicable, whether it would be pertinent to define further provisions that would apply to the governance of the Network. This could include e.g. rules that apply to any changes in the Network's participants or in its contractual, technical or business framework. In addition, the Members should consider if a separate process should be defined for introducing new Datasets within the Network and for the approval of the Dataset Terms of Use.

requested the extraordinary meeting must send an email summarising the issue at hand and whether it is time sensitive.

The meetings can be held or attended as video or teleconference calls when the Chair considers it necessary. The Steering Committee must annually hold at least one face-to-face meeting.

The Secretary coordinates matters related to the duties of the Steering Committee. In particular, the Secretary is responsible for

- preparing Steering Committee meetings, proposing agenda items, preparing the agenda of the Steering Committee meetings, composing the minutes of the meetings and monitoring the implementation of the decisions made by the Steering Committee;
- keeping the Constitutive Agreement and all of its Appendices updated and available;
- collecting, reviewing to verify consistency, and submitting any necessary documents[50] and specific requests made in relation to the Steering Committee's duties;
- coordinating and administering the day-to-day matters of the Steering Committee;
- promptly transmitting documents and notifications related to the Data Network to any Party concerned; and
- providing, upon request, the Parties with official copies or the originals of documents that are in the sole possession of the Secretary when such copies or originals are necessary for the Parties to present claims.

The Secretary is not entitled to act or make legally binding declarations on behalf of any of the Parties or the Data Network, unless explicitly stated otherwise in the Constitutive Agreement or duly authorised by all Parties. The Secretary must not seek to expand its role beyond the tasks specified in this Appendix.

Meeting Agenda

At each meeting, the topical issues affecting the Data Network will be reviewed using an agenda outline that is not limited to the following:

Introductory items such as:

- Introductions including any invited attendees
- Review agenda
- Minutes of the last meeting
- Review of any action points arising from previous meetings

Ongoing matters such as:

[50] **Note**: At least where all Dataset Terms of Use are shared with all Members of the Data Network, it would be logical that the Secretary maintains an up-to-date library of the various applicable Dataset Terms of Use unless other some other centralised solution is established.

- Approval of changes to the Constitutive Agreement and its Appendices
- [Approval of new Members to the Data Network][51]
- [Approval of new Datasets and/or Dataset Terms of Use][52]
- Operational and technical status of the Data Network
- Any change requests concerning the Data Network
- Acceptance of change request deliverables and monitoring their timelines
- Outstanding issues, open action points, conflicts
- Consideration of other relevant items
- Review and summary of actions from the meeting
- Next meeting
- Closing

Quorum and Decisions

A meeting constitutes a quorum when the Chair or his/her representative and at least [2/3] of the Representatives or their representatives are present. The Steering Committee strives to work on the basis of achieving a consensus. The Steering Committee will vote on decisions concerning the Network, if necessary. The Chair will have the casting vote.

In the event that the Committee is not able to achieve a consensus, a proposal that is supported by at least a majority of 2/3 OR 1/2 of the *Representatives present at the meeting* will be adopted as the Steering Committee's decision.

Any amendments to the Constitutive Agreement, [or to Appendix 2 – General Terms and Conditions or Appendix 4 Governance Model, as well as any changes to Appendix 1 – Description of the Data Network with material negative impact vis-à-vis any of the Members[53] must be agreed upon by a majority of 2/3 of *all Representatives*.

New Parties may join the Network by signing an Accession Agreement and their accession must be approved by [a Qualified Majority/a majority] of the Steering Committee. [These approving Parties must include all/a majority of 2/3/a majority of the Data Providers][54].

Where the decision of the Steering Committee to amend the Constitutive Agreement would materially affect the rights or obligations of a Party objecting to such amendment, the objecting Party will be entitled to terminate the Constitutive Agreement by notifying the Steering Committee thereof in writing within fourteen days after the objecting Party becomes aware of the Steering Committee's decision. This

[51] **Note**: If the Constitutive Agreement allows new Members to join the Network.

[52] **Note**: This is relevant only where the approval of new Datasets and/or Dataset Terms of Use is defined in the Constitutive Agreement to be subject to the Steering Committee's approval.

[53] **Note**: Please consider if certain decisions should require even a unanimous decision of all Members' Representatives instead of a qualified majority of all Representatives. The Members should also consider whether criteria for decisions that involve for example a certain financial impact or risk impact should be defined herein in further details.

[54] **Note**: Please consider if e.g. a specific majority of Data Providers should be a precondition for approving new Members to the Data Network.

termination will become effective within thirty days as of date on which the notice was submitted by the objecting Party to the other Parties.

Subcommittees

The Steering Committee may authorise a subcommittee and/or the chair of the relevant subcommittee to explore a specific issue. The Steering Committee will appoint the chairs of the subcommittees and their members in addition to defining their rules of procedure.

Subcommittee chair(s) will have the option of attending Steering Committee meetings when the Chair considers it necessary. The chair of the relevant subcommittee is responsible for disclosing all pertinent information the chair has learned at Steering Committee meetings they have attended to the members of their subcommittee.

All subcommittees must operate under a full consensus. Where a consensus cannot be reached among the members of the subcommittee, the subcommittee chair must escalate the issue to the Steering Committee for final resolution. Once the Steering Committee has been notified of the issue, it will be added to the agenda of the upcoming Steering Committee meeting or to the agenda of a newly scheduled extraordinary meeting (depending on whether the issue is time sensitive). Once the Steering Committee has made its final decision, it will be considered actionable. The Chair will inform the subcommittee chair of the Steering Committee's final decision.

Invited Attendees

The Steering Committee Representatives may invite necessary and appropriate persons to attend any Steering Committee meeting, and such persons will be considered to have been 'in attendance'. The Chair is entitled to decide whether the attendance of the relevant invitee is necessary and appropriate. In the event that an invitee is not from a Network Member's organisation, such an invitee must sign a non-disclosure agreement, unless waived by the Chair. It is the responsibility of the Chair to ensure that the invitee can be proven to be bound by a confidentiality obligation prior to him/her joining the meeting.

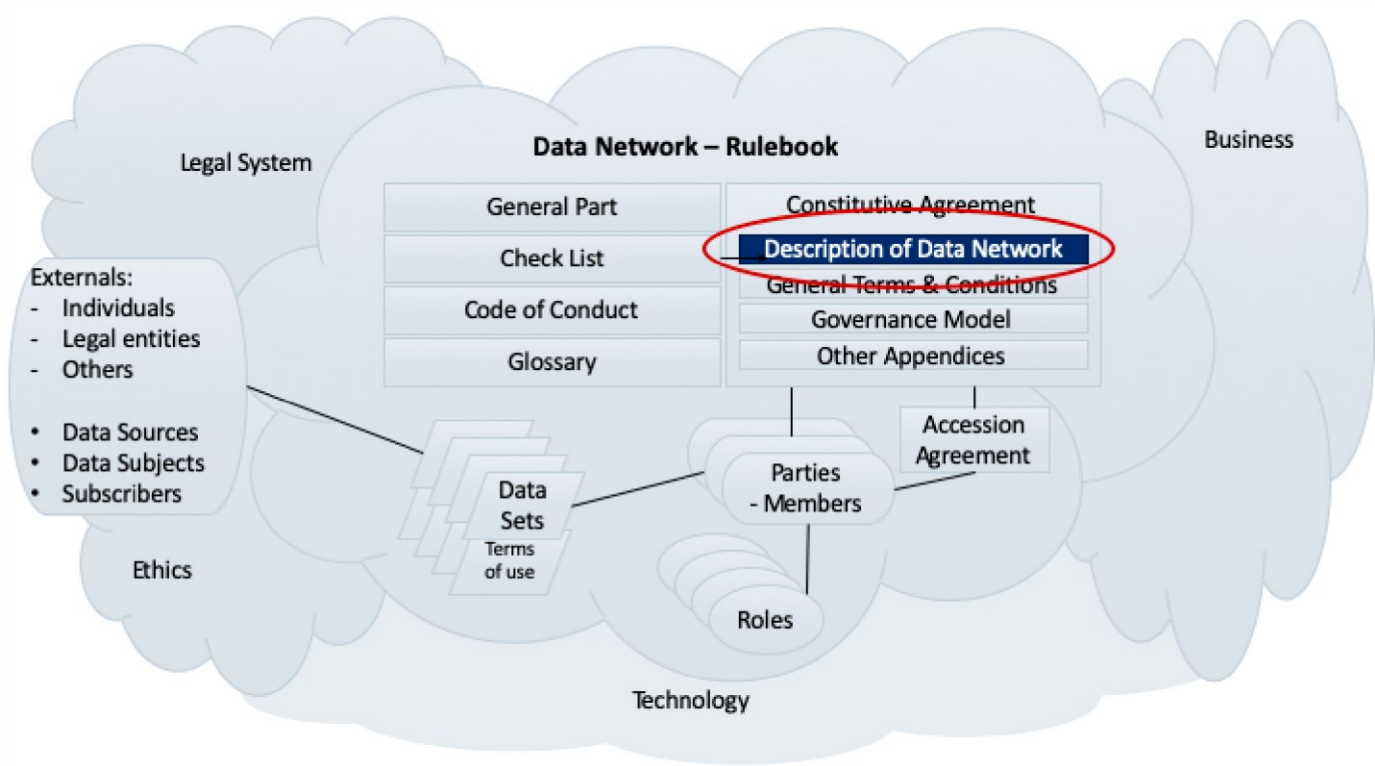
Conflicts

Any dispute, controversy or claim arising out of or relating to the Data Network, or the breach, termination or validity of the Constitutive Agreement must first be escalated to the Steering Committee. The Parties must strive to resolve any such conflict in good faith at the Steering Committee.

4.6 Description of the Data Network

This part of the Constitutive Agreement describes the Data Network. It consists of two subparts Business Annex and Technical Annex

Description of the Data Network is created on the basis of the answers given to the questions in the Check List (Appendix). The Check List and the Description of the Data Network complement each other. The Description of the Data Network includes references to the Check List (see numbering), and they should be read in parallel. The following picture illustrates the Descriptions position within the entirety of the Rulebook.



4.6.1 Business Part in the Description of the Data Network

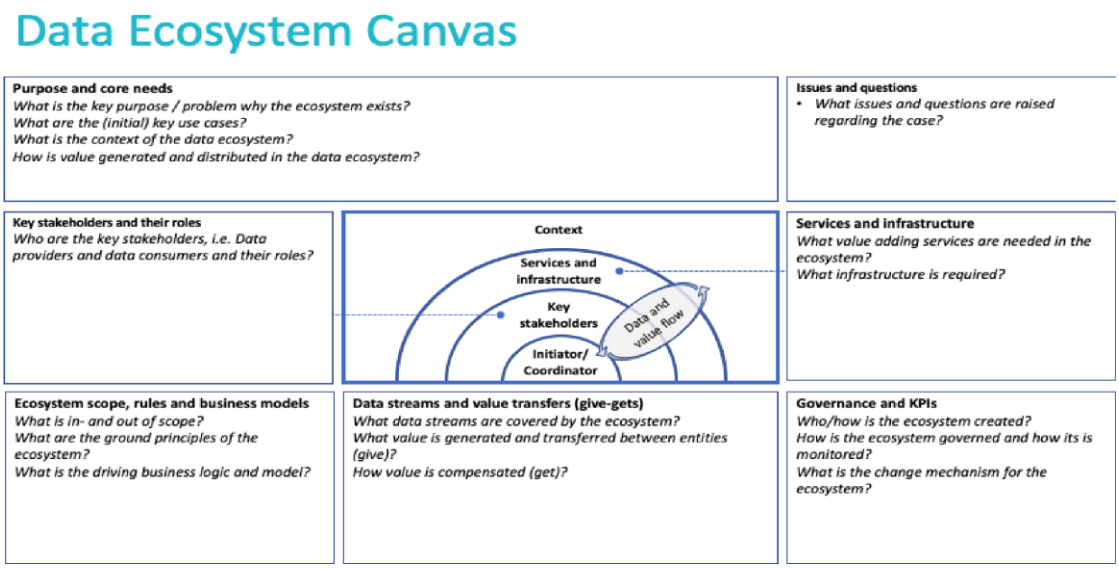
4.6.1.1 Introduction

This document is a part of a general framework for data sharing agreements developed to help companies to form new data networks and to promote the fair data economy in general. This document collects the business decisions raised via the rulebook checklist document and otherwise during the ecosystem design.

This business part is divided into two main parts; data ecosystem canvas and accompanying questions define the high level summary and structure for the business aspects of the data network, and subsequent chapters provide the more in depth business design information that does not fit in the canvas itself. Further design related documents (Contracts, presentations, etc.) can be added to provide additional level of detail for the data network, if available and needed.

4.6.1.2 Data ecosystem canvas

Fill in the following data ecosystem canvas a high-level summary of the business design for the data network under planning. Stated questions and separate rulebook checklist document help in defining the content in each of the canvas fields. Use the "Detailed definitions" chapter for more detailed info that doesn't fit in the reserved space or doesn't belong to the summary level presented by the canvas.



4.6.1.3 Detailed definitions

Continue the data ecosystem definition by using the answers given to the checklist questions. The core questions and requirements for the business aspects of the rulebook are described in the table below. There is a dedicated space for requirements that directly influence the formulation of contracts, and more space for other requirements and notes.

The answers cover the following categories:

- Purpose and core needs
- Key stakeholders and their roles
- Ecosystem scope, rules and business models
- Data streams and value transfers (give-gets)
- Services and infrastructure
- Governance and KPIs

Related checklist questions numbers are provided as a reference to the numbers used in the rulebook checklists.

The goal is not to answer thoroughly to each question listed below. If you have gone through the business checklist questions, use those answers as assistance in formulating the different aspects of the business design. Link further materials to the topics and add additional headers, if needed. Check also that the content here is in line with other parts of the rulebook, such as the technical section, and that potential overlaps are minimized.

Checklist item	**Key question**
1.1.1 Use cases for data	**What is the "job-to-be-done" that requires external data and related data network?**
Contract-level requirements: **Other business-related requirements and notes:**	
1.1.2. Business case **1.1.3 Value of data**	**Is the initial business case for data network defined?** **Is the generation and distribution of the value of data for network participants understood?** **Is the value of data to customer(s) and other stakeholders understood?** • In what form is the data value? • How will the data value be measured? • How is data valuated? • What are the applicable business models?

	• How is the data priced? • What are the main cost categories? • Does the data network have an overall business and governance plan? • What other drivers push for data sharing (e.g., public sector's open data principles)?
Contract-level requirements: **Other business-related requirements and notes:**	
1.3.4. Data network setup **1.3.2. Key actors** **1.3.1. Data Providers** **1.3.3. Roles and responsibilities**	**Who are key actors and their roles in the data network?** • Who is in a leadership position in the data network setup? • Are the limitations for who can join the network? • What are the key sources of data? Who controls the use of that data? • What kind of additional partners are sought for the data network? • What are minimum requirements to join the network? • What fees and costs are related to joining and participating the network? • Are the other stakeholders that should be considered (e.g., officials, influencers to the data etc.)? • Does the data network have the necessary prerequisites and means for fair and trusted collaboration? • Are critical roles fulfilled to launch the data network? • How performance in these roles is measured? • Are different roles and responsibilities related to data processing over its life cycle defined? • What is the change/nomination mechanism for roles?
Contract-level requirements: **Other business-related requirements and notes:**	
4.1.5. Culture	**Short description of the different parties' cultures and what common elements will be inherited to the data network.** • More detailed cultural and transformational aspects are to be managed separately e.g., at the participant's own implementation projects. • Further points to consider; is there a need for cross-cultural collaboration in data networks? If yes, how to implement and adapt cultural and societal differences in the data network? • How to manage cultural aspects and change? Understanding and adapting to multi-cultural environment? • Common transition plan for common activities in the data network?
Contract-level requirements: **Other business-related requirements and notes:**	
1.3.5. Data network solution fundamentals	**How are the fundamentals of the data network solved?** • Make, buy, rent?
Contract-level requirements: **Other business-related requirements and notes:**	
3.2.3. Consents	**Consent management for personal and other data?** • How are consents managed, monitored, and reported? • How is the interaction with consent owners (e.g., persons) managed?
Contract-level requirements: **Other business-related requirements and notes:**	
3.3.3. Change control **3.3.2. Data governance** **4.1.3. Data governance and responsibilities**	**What are the data storage and availability principles in the data network?** **What kind of principles and guarantees are defined for storage and availability of data?** **What are the data life cycle management principles?** • How is change management of different aspects handled (data, structures, systems, interfaces, governance-related)? • How are changes managed and communicated to different parts of the data infrastructure and related operations? • Mechanisms for archiving and deleting data, what systems and process exist to manage the last steps of data life cycle? • Who are responsible of data over its life cycle? Are there shared responsibilities? How is this responsible transferred?

Contract-level requirements: **Other business-related requirements and notes:**	
4.1.7. Skills and capabilities	**What data-related skills and capabilities are required from the data network and its members?** • How to acquire and maintain these capabilities?
Contract-level requirements: **Other business-related requirements and notes:**	
1.1.4. Monetary transactions	**Does the data have licensing fees or other monetary measures?** • Has the allocation of fees been agreed between parties? • How will they be calculated, measured, and monitored? • Are these applicable also for aggregated data? • In case data exchange includes monetary activities, have the potential taxation and other consequences been defined?
Contract-level requirements: **Other business-related requirements and notes:**	
1.1.5. Costs	**Have the data network related development and operating costs been identified?** • How will they be allocated and to whom? What other costs will be involved?
Contract-level requirements: **Other business-related requirements and notes:**	
1.1.6. Available services **4.1.4. Data services**	**Have the ecosystem-wide data-related services been defined?** • Who will provide these services? • Are there common rules and instructions related to these services? • Need and implementation of data-based services in the data network? Some aspects to consider include e.g., verifiable claims based on data, anonymization, analysis and visualization. • How is data and/or related services audited (who, requirements, frequency, related standards)?
Contract-level requirements: **Other business-related requirements and notes:**	
1.1.8. Level of commitment	**What kind of strategic bi-directional dependencies exist between the partners of the data network?** • What kind of incentives and mechanisms are there for data sharing? • How to ensure continuity of joint operations?
Contract-level requirements: **Other business-related requirements and notes:**	
1.1.9. Data utilization **1.2.2. Limitations and restrictions related to use** **1.2.3. Data access, manipulation and distribution** **1.2.4. Life cycle management**	• What are the permissions and restrictions on data use (users, domains, uses, locations, etc.)**?** • Does data have restrictions on the nature of use (e.g., on-off -use, perpetual license, R&D only, etc.)? • Has data restrictions in the domain of use? If yes, are these explicitly defined? • What activities need to be done to data before it can be used (e.g., anonymization)? • What kind of limitations will be set so that data sharing is still feasible, and data can be used for current and potential future needs, i.e., data is not completely locked down? • Can data be distributed further? By whom? • Does this need to be reported to data provider and/or other parties? • Is the data use, processing and/or storage geographically limited? • Are there legal or societal aspects that should be considered (e.g., different perspectives on personal data depending on legislation)? • How is data transferred and refined in the data network? • How is access to data implemented and monitored? • Is access and use logged? • Does the data provider provide a mechanism to ensure long-term data availability (e.g., Service Level Agreement)? • How potential termination and revocation of data rights is implemented and monitored? • What is the change mechanism for rights and restrictions to data?

Contract-level requirements: **Other business-related requirements and notes:**	
3.2.1. Interfaces **4.1.2. Data location and availability**	**What kind of interfaces are there?** **Have data location and availability practices been defined?** • How are commitments managed? • What are the data life cycle management principles? • Who are responsible of data over its life cycle? • How is this responsible transferred? • How is the development performed and are there e.g., common roadmaps?
Contract-level requirements: **Other business-related requirements and notes:**	
4.1.1. Data scope	**What data is in data network's scope? What data is not in scope or available via separate agreements (to the level important to the data collaboration)?**
Contract-level requirements: **Other business-related requirements and notes:**	
4.2.1. Formats and structures **4.2.2. Shared semantics**	**What is the format and structure of data and associated metadata?** • Is this structure described and shared? • What data standards are used? • Are data models semantically compatible? • Are differences significant? • How are the incompatibilities resolved? • Is semantic structure of data and metadata described and shared between participants? • How dynamic is the shared semantics, i.e., how frequent changes are expected the shared semantics?
Contract-level requirements: **Other business-related requirements and notes:**	
4.2.3. Data quality	**Is the data quality at sufficient level?** • If the quality is not sufficiently high (missing data, outdated data, metadata errors, semantic differences, real-time/latency requirements), what potential improvement actions are needed? • Who will perform these operations and how? • How is success measured?
Contract-level requirements: **Other business-related requirements and notes:**	
1.2.1 Nature of data and confidentiality	**What kind of data is handled in the ecosystem (e.g., confidential, proprietary, open)?** • Is data confidential? If yes, how is confidentiality ensured and monitored? • What kind of permissions and restrictions are needed (users, domains, uses, locations, etc.)**?**
Contract-level requirements: **Other business-related requirements and notes:**	
1.1.7. KPIs	**What KPIs are used to measure the success of the data network and its services)?**
Contract-level requirements: **Other business-related requirements and notes:**	
3.1.3. Data-related mitigations	**How to protect the data network and related services?** • How to prevent data leaks and hacking? • Exception management and damage control? • How to manage potential leaks and misuse? • How to limit damages e.g., in case of hacking?

Contract-level requirements: **Other business-related requirements and notes:**	
3.3.1. Monitoring and administration	**How is the monitoring and reporting of system and data use achieved?** • How is logging implemented (e.g., central or distributed implementation)? • What about related concepts, such as traceability or auditing?
Contract-level requirements: **Other business-related requirements and notes:**	

4.6.1.4 Issues and questions

4.6.1.5 Other related documentation

Add here other potential documentation related to the business design of the data network.

4.6.2 Technology Part in the Description of the Data Network

4.6.2.1 Introduction

This document is a part of a general framework for data sharing agreements developed to help companies to form new data networks and to promote the fair data economy in general. This document collects the technical decisions raised via the rulebook checklist document and otherwise during the infrastructure and system design for the data ecosystem. The checklist is a working document for technical design. It assists to identify and define common technical needs and their main characteristics. When this process is over, the results are transferred from the checklists to this and other main sections of the rulebook.

This document is currently mostly a placeholder but provides topics that should be covered and discussed in the course of designing the technical solution. This document acts as a master document for infrastructure specifications as well as for the work split between participants' systems and the common infrastructure. Further technical design related can be added or linked to provide additional level of detail for the data network, if available and needed.

4.6.2.1 Overview of the technical solution

The prerequisite of the technical design is that we have at least an initial understanding of the common needs, parties and roles involved, as well as requirements of the common solution. Checklist tool is aimed in supporting in the process as well as in identifying more detailed technical requirements. When the parties have reached an initial and common understanding of needs, parties and common core functionality, document here a short introduction for the technical part.

4.6.2.2 System architecture, high-level principles and common requirements

Based on checklist work and other design effort, provide a description of the system architecture as well as high level principles for the design, including e.g.:

- Work split between providers' systems and common infrastructure
- System architecture and common interfaces/APIs
- Common architectural requirements

4.6.2.3 Detailed specifications for the solution and its technical implementation

Summarize and document here the key technical aspects and requirements based on checklists and other design effort. These aspects reflect common architectural requirements and design principles following the checklist-based categorization:

- Capability requirements
- Purpose and system overview
- System design and architecture
- Functional and non-functional requirements
- Security
- References and standards

The following checklist-based structure is provided as a reference and starting point. The goal is not to answer thoroughly each checklist question, but to use the questions as assistance in formulating the different aspects of the business design. Link further materials to the topics or the chapter at the end of the section and add additional headers, if needed. Check also that the content here is in line with other parts of the rulebook, such as the business section, and that potential overlaps are minimized.

Checklist item	Key question
1.3.5. Solution fundamentals	**What are the expectations for the data network and its participants?** **What technical capabilities and solutions will be implemented as a common effort?**
Contract-level requirements: **Technical principles and requirements:**	
3.1.1. Key principles and design philosophy	**What are the design principles, focus areas and design philosophy for the data network's common technology solution?** • What is the design philosophy? For example, what is implemented as a shared solution, what is left to participants or what is the future roadmap for the solution? • Decisions related to overall architecture and technology choices (e.g., cloud solution, vendor independence), system architecture, functional and non-functional requirements, available standards and reference implementations, interfaces and APIs, common roadmap.
Contract-level requirements: **Technical principles and requirements:**	
3.1.2. Security and privacy	**What is the common technical solution related to security and privacy?** • How is data security ensured for the shared data throughout the data network? • What security and privacy features are needed in the common solution as well as at the participants and how will these be implemented and managed? What common activities are needed? • What are the references and standards to be used for security and in the data network?
Contract-level requirements: **Technical principles and requirements:**	
3.1.3. Data-related mitigations	**How to manage and prevent potential challenges in the data network and services related to it?** **How to handle the common exception management and damage control?** • How to prevent data leaks and hacking? How to protect the data network and related services? • Exception management and damage control? How to manage potential leaks and misuse? How to limit damages e.g., in case of hacking?
Contract-level requirements: **Technical principles and requirements:**	
3.1.4. Standards and common structure	**Standards and structures (Data, metadata, architecture) to be used?** • Change control and mechanisms to handle changes?
Contract-level requirements: **Technical principles and requirements:**	
3.2.1. Interfaces	**What APIs and interface descriptions are needed and defined?** • Are changes expected to interfaces or APIs and how the evolution of the interfaces will be governed? • APIs and interface descriptions? Roadmaps and commitments?
Contract-level requirements: **Technical principles and requirements:**	
3.2.2. Access control and Identities	**Access and identity management solution?** • What is the solution for identity, roles and access control? • Trusted identification of data network participants? How are identities created and governed?
Contract-level requirements: **Technical principles and requirements:**	
3.2.3. Consents	**How are permissions managed, monitored and reported?** • Consent management for personal and other data? • How is the interaction with consent owners (e.g., persons) managed?

Contract-level requirements:

Technical principles and requirements:

3.2.4. Transaction management **3.3.1. Monitoring and administration**	**How data related transactions are monitored and governed?** • What capabilities are required and how they are governed? • Monitoring, auditing and reporting of system and data use? • Agreeing and confirming transactions, e.g., digital signatures, access keys and identities? • Monitoring and reporting of system and data use (e.g., monitoring APIs)?

Contract-level requirements:

Technical principles and requirements:

3.3.2. Data governance **4.1.3. Data governance and responsibilities** **4.1.6. Data control**	**What are the data life cycle management and data governance principles?** • Who are responsible of data over its life cycle? Are there shared responsibilities? How is this responsibility transferred? • Data storage and availability principles? What kind of principles, guarantees and other means are defined for storage and availability of data? • Are the rights to use and mechanisms to track the data use agreed and implemented? How are these practices monitored and enforced? How is data security implemented? By whom? Response levels and potential sanctions? • Mechanisms for archiving and deleting data, what systems and process exist to manage the last steps of data life cycle?

Contract-level requirements:

Technical principles and requirements:

3.3.3. Change control	**Common change management principles?** • Technical requirements for the change management (e.g., data, structures, systems, interfaces, governance-related)? • How changes and managed to different parts of the data infrastructure and related operations?

Contract-level requirements:

Technical principles and requirements:

4.1.2. Data location and availability	**How data is used over its life cycle?** • Is data location and availability understood over data life cycle? Where is data located? Will data be transferred to other entities? • How to ensure data availability and accuracy? • How is metadata associated and managed in the data network?

Contract-level requirements:

Technical principles and requirements:

4.1.4. Data services	**What data services are provided centrally?** • Need and implementation of data-based services in the data network? • Requirements related to agreed data-based services in the data network? • How is data and/or related services audited (who, requirements, frequency, related standards)?

Contract-level requirements:

Technical principles and requirements:

4.2.2. Shared semantics	**What is the role of data models and semantics in the data network?** • How the data network agrees on the structure and semantics for shared data? How are the incompatibilities resolved? • What data standards are used? • Is semantic structure of data and metadata described and shared between participants? • How the data network agrees on the structure and semantics of the shared data?

Contract-level requirements:

Technical principles and requirements:

4.2.3. Data quality	**How data quality is managed?**

	• Is the data quality at sufficient level? If not (missing data, outdated data, metadata errors, semantic differences, real-time/latency requirements), what potential improvement actions are needed? Who will perform these operations and how? How is success measured? • What potential improvement actions are needed for data quality to be implemented with the common solution?
Contract-level requirements: **Technical principles and requirements:**	

4.6.2.4 ISSUES AND QUESTIONS

What other issues and questions have emerged during the planning?

4.6.2.5 Other related documentation

Add here other potential documentation related to the technology design of the data network.

5 Code of Conduct

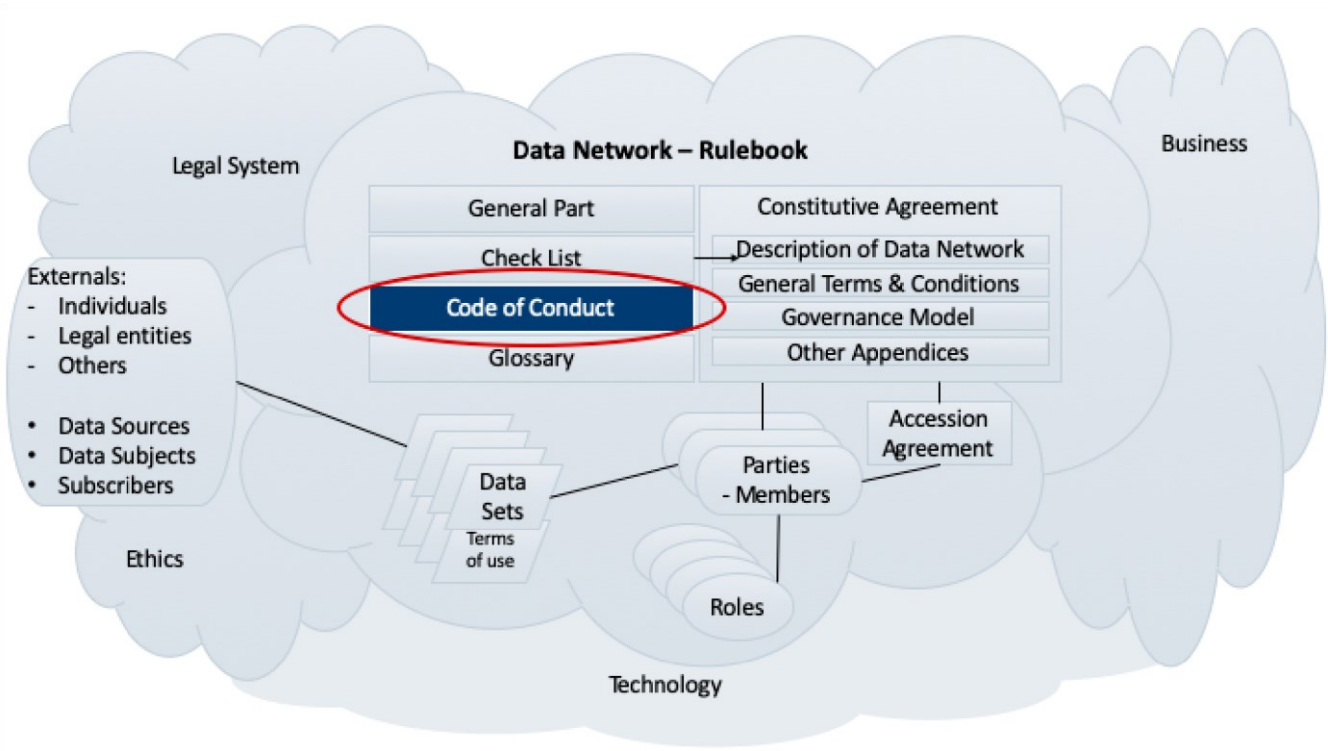
5.1 Introduction

This part works as a short guide to survey and improve the ethicality of the data network, and activities and organisations that are part of it. This Code of Conduct is not an ethical code as the organisations and networks – that want to utilise this – most likely are very different depending on context and various other reasons. Therefore, as different data networks using this rulebook may differ, case by case, this code cannot be seen as sufficient but necessary list of issues needed to be taken care of. This means that more detailed and specific codes or other ethical guides should be considered and reviewed - based on demands of specific data network or organisation that implements this code of conduct[55].

This code should not be seen as a way to restrict the actors of a data network but instead as a set of commonly acceptable norms that make cooperation between members more convenient by setting the direction for more detailed rules defined by implementing organisations. The code is not an obstacle. Like laws, it helps to create trust in a data network, which is needed for gaining real benefits and new business opportunities. This code of conduct is based on the respect between different stakeholders, transparent communication and ambition to seek the values that are commonly acceptable.

The code itself does not have intrinsic but instrumental value. Most important is that organisation has a real goal to improve its processes and policies to be more ethical. The mere mechanical following of codes is better than not following those. However, the aim should be changing the culture of the organisation to such that it put ethicality in everyday actions, so the change comes from inside – not from outside. In that case, change is durable and will help the organisation to meet demands that society justifiably sets for them.

Acting ethically is not a mere cost but possibility for a resilient business.



[55] The demands for ethical codes are different based on what kind of information is used and also the target of use may raise different ethical concerns. As an example, whilst using health information the medical codes of ethics need to be considered. As against, when data that are processed within a data network does not include any personal data, the focus should be in respecting e.g., intellectual property rights.

5.2 Ethical Basis and Shared values of the Data Network

There exists a consensus amongst normative theorists of cultural pluralism that dialogue is the key for securing just relation between different groups[56]. Discourse ethics is an applicable tool to bring different views under constructive communication[57] and thus to facilitate a more transparent and rational discourse. Discourse ethics provides a mechanism for considering different moral views and intuitions of different stakeholders.

However, this code of conduct does not focus on ethical theories. Instead, the purpose of this code is to approach the topic from the practitioners' point of view and to provide conceptual and analytical tools for assessing reasons on the basis of which the question "what should we do?" can be answered. This is done by presenting the values seen as important for data economy as well as by offering the maturity model (see next section) which can be employed in the analysis of the state of affairs in an organisation and consequently in the search of ways of improvement and development..

The following values have been found to be important in the research conducted during the IHAN project. In order the aim of fair data use to be achieved these values should be noted and respected in everyday practises..

5.2.1 Accountability and Auditability

The members of the data network are responsible for what they do, and they must be able to give satisfactory reasons for it. This means that all actors are expected to follow the Rule Book of the data network and especially its contract. All the contracts also should follow the Code of Conduct and the Rulebook of this data network. The responsibility is towards members of the data network, but also the external stakeholders – e.g., individuals, whose personal data may be processed in the data network. The operations within the data network must also be auditable, i.e., an auditor needs to be able to achieve a comprehensive examination of the data processing within the data network. Therefore, the members' records, logs and documents on data processing are well-organized and complete, their personnel are transparent in their dealings with the auditor, and the members have a good system of internal control, security and documentation in relation to data processing.

5.2.2 Avoid harm

All actors in the data network should avoid causing harm but instead focus on creating value (direct or indirect) for the whole data network and all the people that are affected by the actions of this data network.

5.2.3 Justified Processing of Personal Data

Personal data shall be processed on a fair and lawful basis, like for example on the basis of an informed consent of the individual, in accordance with a contract with the individual, a legal obligation, a vital interest of the individual, in the public interest, or for the purposes of the legitimate interests, given that the interests and fundamental rights and freedoms of the individual are not threaten, in particular where the individual is a child.

5.2.4 Fairness, justice, and equality

All actors in the data network should promote fairness, justice, and equality among individuals. Fairness means that everyone is treated with respect regardless of their socio-economical background or status. Likewise, the benefits (economical and others) must be balanced between all stakeholders in such a manner that individuals that are the source of data are not seen as mere exploitable resources.

To ensure fair use of their information, individuals are granted true possibilities to understand and control their personal data that are collected, transferred and otherwise processed in the data network.
The rules and the structure of the data network secure the benefits and rightful expectations of all the parties. This requires a balanced power structure in the data network and transparent consensus-oriented governance.

5.2.5 Human-centricity

People live in different environments and they have personal lived experiences of their own life. They must be respected and empowered. This means that individuals have to be seen and treated as active actors with opportunities to make their own choices in the data network. They must be able to keep full and effective self-determination. Furthermore, their needs and wishes should be taken account instead of reducing them as objects or subjects.

5.2.6 Privacy

Privacy is one of the central issues in data economy. Therefore, privacy must be respected and protected. The data network is based on the use of information, which sets high demands for privacy as information can be sensitive and private. Thus, this means that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the individuals. Personal data shall be collected for specified, explicit and legitimate purposes and it shall not be processed further in a manner that is incompatible with those purposes. Only personal data, which are adequate, relevant and limited to what is necessary in relation to the expressed purposes, shall be processed. Organizations do not collect personal information that they do not need. All the personal data that are processed have to be necessary for the specific use. The members of the data network take reasonable measures to ensure that personal data are accurate and up to date. Personal data must not be stored longer than necessary for the purposes for which the personal data is processed. To ensure the integrity and confidentiality of privacy, personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational

[56] James, M. R. (2003). Communicative Action, Strategic Action, and Inter-Group Dialogue. European Journal of Political Theory, 2(2), 157–182. https://doi.org/10.1177/147488510322003

[57] Stahl, B. C. (2012). Morality, ethics, and reflection: A categorization of normative IS research. Journal of the Association for Information Systems,13(8):636–65. https://doi.org/10.17705/1jais.00304

measures. To preserve the integrity, confidentiality and availability of the data, organizations need to develop and implement an information security policy framework. When merging data sets, privacy should be guarded even more carefully than normally. Anonymization of data is recommendable, whenever feasible. Any organization must also be accountable, i.e., it needs to be able to demonstrate its compliance with the principles mentioned above. Therefore, the processing of personal data must be planned and documented. There should exist clear, documented processes for data collection, storage, use, and distribution. For collected data, there needs to be a clearly documented life cycle plan where the collection, archiving and possible erasing of data are described. The relevant parts of the life cycle plan are available to data providers and individuals related to the data.

5.2.7 Security

All the members of the data network are responsible that their collection, use, storage, sharing, and other processing of data are secure. This means that proper security solutions and processes are used and also that monitoring, patching, and reporting of security issues are properly designed. Personal data on individuals must be properly secured and the risks to the rights and freedoms of individuals should be analysed. All the necessary technical, organisational and personal actions must be implemented to minimise security threats to individuals whose information is processed. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, all the members of the data network shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Likewise, data breaches must be responded without delays. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the responsible member of the data network shall communicate the personal data breach to the data subject without undue delay.

5.2.8 Sustainability and Circular Economy

All the members of the data network are guided and incentivised to develop and deploy sustainable solutions in alignment with a more sustainable, circular economy. The members will implement the data network in a manner to make its operations more sustainable and circular, thus reducing its negative externalities on the environment, climate, and natural resources.

5.2.9 Transparency

The data network is based on co-operation and respect for information sources. Transparency is important to develop trust. The data shall be processed lawfully, fairly and in a transparent manner. Any information addressed to the public or to individuals must be concise, easily accessible and easy to understand, and clear and plain language and, additionally, where appropriate, visualisation is used. This does not mean that information is open to everybody without restriction. Instead, it means that all the members in the data network should know (when/if possible), what data are offered in the data network and by what requirements to promote transparency of network. To support real-time economy, the members of the data network do not unnecessarily detain data but share them as soon as possible.

The use of unnecessary legal jargon should be avoided. If an individual is asked to give a consent or to accept an agreement, it must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, and using clear and plain language. Additionally, honest information should be provided to individuals for understanding what data regarding them is being collected and how it is being processed.

5.2.10 Continuous improving

Ethical issues vary and different issues may come up case by case. Thus, ethical evaluation should be a continuous process in organisation and there should be institutional support for this. Therefore, the management of a network member should support the organization's employees by ensuring that they have real opportunities to uphold, promote, and respect the principles of the Code of Conduct. Ethics is implemented in daily actions of individuals or it is not implemented at all, as only individual can make the moral decision. However, without institutional support for ethical decisions there is a higher risk of unethicality as individuals lack the needed autonomy for being able to make moral decisions.

5.2.11 Support for individuals

All the members of the data network should support individuals in (a) getting information about use of their personal information, (b) understanding information, practices, contracts, and their consequences, and (c) participating, contributing, and influencing in systems and practices when using personal information of those individuals. The aim is to ensure that if individuals need information or have justified demands for Information, they are given needed support (Guidelines, personal help etc.) in transparent ways. The focus should be in creating low-barrier way to look overuse of personal information for those individuals from whom it is directly collected or other way received.

5.2.12 Communication

Appropriate communication is fundamental throughout the data network's life circle. It is essential for individuals, organizations, and the society as a whole. Each of them needs in addition to different contents and timing, also apposite communication channels and manners. The above-mentioned ethical principles are put into practice with communication. Furthermore, communication is the way to demonstrate the organization´s commitment to them. The management has a special responsibility to articulate, apply, and support the organization's culture and processes that reflect the principles of this Code of Conduct.

5.3 Ethical maturity model

The maturity model presented in next page is tool that is developed to helps organisation to evaluate its ethical maturity. However, it is developed such way that it would help the practitioners to have deeper view of situation in own organisation. Likewise, it provides conceptual and analytical tool that can be used to clarify the question “what should we do” by emphasising issues that needs not only to deal with but give deeper focus and considerations. Hence, the maturity model should not be seen as mere list of checkbox items, that is filled and

forgotten. At best maturity model can serve as ground for discussion about organisational culture and values by providing different themes that help to start to critical self-investigation in personal and organisational levels.

Table 1. Ethical maturity model

	Security	Commitment to ethical practices	Transparency and communication	Sustainability	Human-centricity	Fair Networking	Purpose
Level 0	"I believe that this is very secure"	"We prefer not to commit, we are free"	"Just trust us"	"Let it burn"	"What this has to do with the people?"	"Anarchy"	"We do what we want to do"
Level 1	There are proper Antivirus, Firewall and other needed security tools in use and they are properly updated.	Organisation follows regulations and the best practices of its own field.	Organisation follows the regulations and uses truthful communication.	Organisation has documented sustainability plan/program.	The individuals are recognised as stakeholder and their rights are taken account.	Organisation aligns it rules and regulations to best practices of industry	Organization has stated reasons for data collection and usage
Level 2	There is a dedicated person to keep up with information security.	Organisation has implemented and is committed to following ethical code(s) or other codes of conduct.	Organisation supports open internal communication and responsible information sharing.	There is an evaluation model for sustainability with clear indicators.	The organisation collects information of the needs of individuals to improve people-centricity.	Organization defines and documents practices and provides the needed information for network partners	Organization has transparent rules how data can be used in the future
Level 3	There are clearly documented procedures for the preparation of security threats.	There are clear well documented procedures for actions to be taken when ethical issues occur.	There is a transparent, documented plan for internal and external communication	Organisation impact on the environment is neutral or positive.	Individuals have low-level ways to communicate with the organisation and their opinions are systematically noted.	Organisation supports and encourages a fair data sharing in ecosystems.	The organisation negotiates with information sources to gain mutual understanding of fair information use
Level 4	The whole organisation has internalised the importance of security and it is constantly monitored and developed through the organization.	Organisational policies and procedures are developed critically from ethical perspective together with all relevant stakeholders.	Organisation openly communicates its procedures and policies.	Organisation is actively advancing the sustainability of its business field.	Organisation will actively involve all relevant stakeholders in decision making.	Organisation actively seeks to ways to advance possibilities of whole ecosystems.	Organisation has clear, public, documented goals and procedure of information use

5.4 Further Material on Ethics

ACM code of ethics is ethical code that gives insights for computing professionals and managers to ethical issues that should be taken account in practice.

https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-booklet.pdf

Ethics Guidelines for Trustworthy Artificial Intelligence by High-Level Expert Group on AI set up by the European Commission.

https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Data ethics canvas provided by ODI (Open Data Institute) that focuses on helping identify and manage ethical issues of using data.

https://theodi.org/wp-content/uploads/2019/07/ODI-Data-Ethics-Canvas-2019-05.pdf

The ethics of Big Data: Balancing economic benefits and ethical questions of Big Data in the EU policy context

https://www.eesc.europa.eu/sites/default/files/resources/docs/qe-04-17-306-en-n.pdf

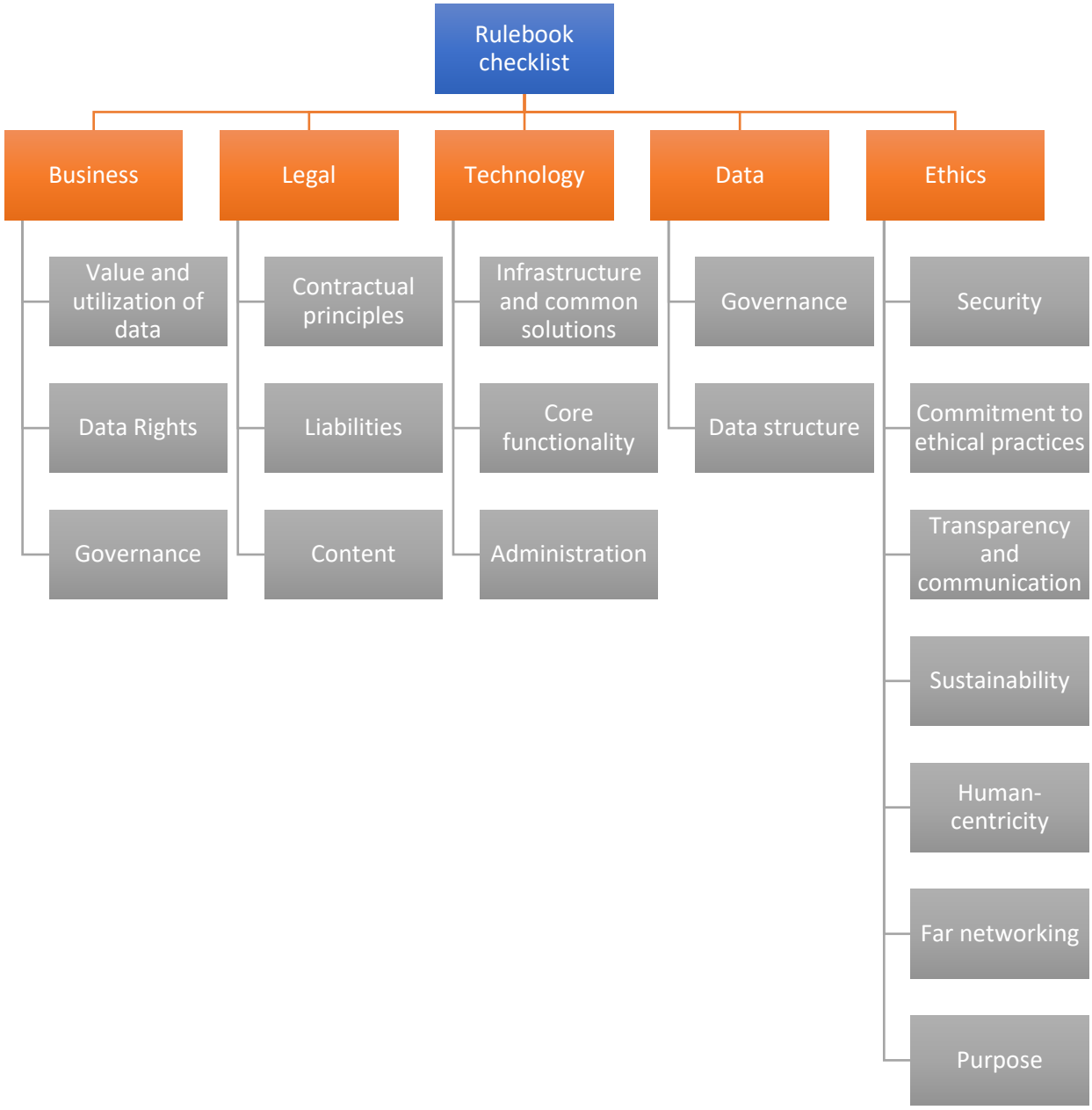
Appendix: Checklists

1 INTRODUCTION

This document is part of the Rulebook Template for Data Networks developed to help organisations to form new data networks and to promote the fair data economy in general. The purpose of the following checklists is to provide a list of key data related control questions to be used as a tool in the rulebook and contractual framework creation process.

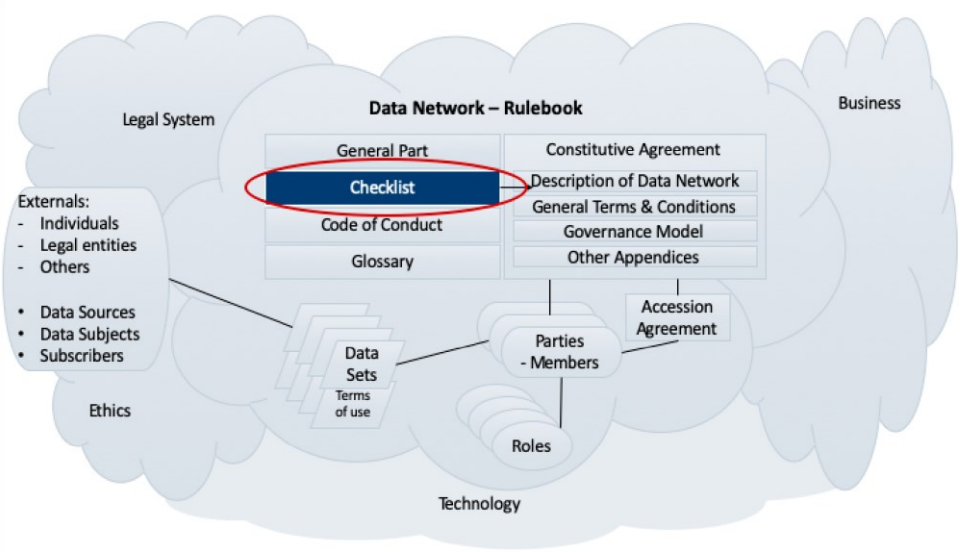
The checklists act as a template document highlighting the most important aspects to consider when planning and building a data-driven collaboration and network. Even though the checklists may contain some questions and aspects not relevant to all data-driven activities, it is still advisable to go through the whole lists carefully and decide per each step its relevance and potential further actions required.

The checklists are divided into top-level categories, which are then further divided to subcategories. These subcategories help in assessing the overall maturity of the planning as well as guide potential further actions to certain areas. Each question is also prioritized to further highlight and identify each question's role in the process. The structure of the categorization is as follows:



Please note that many of the checklist topics require a combination of business, legal, technology, data and ethics related activities to be resolved. For example, an entity controlling a data provider need a business motivation to participate in the data network, a solid legal framework to cover potential challenges with the collaboration, fitted IT-solution and infrastructure to deliver the data, detailed description of the qualities, format and nature of data, as well as shared understanding of the ecosystem and its key principles.

The figure below illustrates this Checklist's position within the whole context of the Rule Book.



1.1 General checklist notation

OK = This question has relevance, and we have a sufficient level of understanding how the question and its related aspects will be managed in our data network.

NOK = This question has relevance, but we don't currently have enough understanding how this question will be handled in our data network.

N/A = Not applicable. This topic is not currently relevant for our data network.

NOTE: See documents mentioned in the Comments/Further info for more detailed description about the question.

2 BUSINESS QUESTIONS

2.1 Value and utilization of data

ID	Checkpoint	OK	NOK	N/A	Comments
1.1.1	**Use cases for data** What is the "job-to-be-done" that requires external data and related data network?				Business document: Purpose and core needs
1.1.2	**Business case** Is initial business case for data network defined? What are the applicable business models?				Business document: Ecosystem scope and business models Contractual Framework: Constitutive Agreement and Network Description
1.1.3	**Value of data** Is the value of data to customer(s) and other stakeholders understood? How is the data priced? How is data compensated?				Business Document: Data streams and value transfers, Purpose and core needs Contractual Framework: Constitutive Agreement and Dataset Terms of Use

1.1.4	**Monetary transactions** Does the data have licensing fees or other monetary measures? How are these calculated, measured and monitored?				Business Document: Ecosystem scope, rules, and business models Governance and KPIs
1.1.5	**Costs** Are the data network related development and operating costs been identified and allocated? Are other costs involved?				Business Document: Ecosystem scope, rules, and business models Contractual Framework: Constitutive Agreement
1.1.6	**Available services** Have the data-related services provided by the data network been defined, priced and agreed? Who performs the activities?				Business Document: Services and Infrastructure, Ecosystem scope, rules, and business models Key stakeholders and their roles Constitutive Agreement, Network Description, Dataset Terms of Use
1.1.7	**Key Performance Indicators (KPI)** What essential KPIs are defined and used in data network?				Business Document: Governance and KPIs Contractual Framework: Constitutive Agreement, Dataset Terms of Use, Service Level Agreements (if applicable)
1.1.8	**Level of commitment** What are incentives and mechanisms for data sharing?				Business Document: Ecosystem scope, rules, and business models Data streams and value transfers, Governance and KPIs Contractual Framework: Constitutive Agreement, Network Description, Dataset Terms of Use, Service Level Agreements, Governmental Model
1.1.9	**Data utilization** How is data transferred and refined in the data network? What are the permissions, restrictions and limitations on data use and sharing so that sharing is still feasible, and data is available long-term?				Business Document: Services and Infrastructure, Ecosystem scope, rules, and business models Contractual Framework: Constitutive Agreement, Network Description, Dataset Terms of Use, Service Level Agreements,

2.2 Data rights

ID	Checkpoint	OK	NOK	N/A	Comments
1.2.1	**Nature of data and confidentiality** What kind of data is handled in the ecosystem (e.g., confidential, proprietary, open)? What kind of permissions and restrictions are needed?				Business Document: Data streams and value transfers, Governance and KPIs Contractual Framework: Constitutive Agreement, Dataset Terms of Use, Security and Technical Requirements

1.2.2	**Limitations and restrictions related to use** Can data be distributed further and by whom? Are there restrictions related to geographical, legal, or societal aspects? Does field or nature of use impact the use and sharing? What kind of limitations will be set so that data sharing is still feasible, and data can be used for current and potential future needs, i.e., data is not completely locked down?				Business Document: Ecosystem scope, rules, and business models Governance and KPIs Contractual Framework: Constitutive Agreement, Dataset Terms of Use
1.2.3	**Data access, manipulation and distribution** What are the rules related to data use over its life cycle? How is access to data implemented and monitored?				Business Document: Services and infrastructure, Ecosystem scope, rules, and business models Governance and KPIs Contractual Framework: Constitutive Agreement, Dataset Terms of Use, Service Level Agreements, Technical Requirements
1.2.4	**Life cycle management** How potential termination and revocation of data rights is implemented and monitored? How are these governed?				Business Document: Services and infrastructure, Governance and KPIs Contractual Framework: Constitutive Agreement, Dataset Terms of Use, Governmental Model

2.3 Governance

ID	Checkpoint	OK	NOK	N/A	Comments
1.3.1	**Data Providers** Key sources and other stakeholders related to controlling the data and its use?				Business Document: Key stakeholders and their roles, Data streams and value transfers Contractual Framework: Constitutive Agreement, Network Description, Dataset Terms of Use
1.3.2	**Key actors** Who are key actors and their roles in the data network?				Business Document: Key stakeholders and their roles Contractual Framework: Constitutive Agreement, Network Description, Dataset Terms of Use
1.3.3	**Roles and responsibilities** Are different roles and responsibilities as well as their actors related to data processing over its life cycle defined? How are these roles monitored and governed?				Business Document: Key stakeholders and their roles, Governance and KPIs Contractual Framework: Constitutive Agreement, Network Description, Governmental Model, Service Level Agreements

1.3.4	**Data network setup** Does the data network have the necessary prerequisites and means for fair and trusted collaboration, including e.g., governance?				Business Document: Ecosystem scope, rules, and business models Key stakeholders and their roles, Governance and KPIs Contractual Framework: Constitutive Agreement, Network Description, Governmental Model, Service Level Agreements, Code of Conduct
1.3.5	**Solution fundamentals** Make, buy, rent? What expectations are set to the data network and its participants?				Business Document: Key stakeholders and their roles, Services and infrastructure Technical document: Capability requirements Contractual Framework: Constitutive Agreement, Technical Requirements, Network Description, Service Level Agreements

3 LEGAL QUESTIONS

3.1 Contractual principles

General structure and gist for the data network contract; what are the key aspects to consider from the legal perspective:

ID	Checkpoint	OK	NOK	N/A	Comments
2.1.1	**Clarity** Drive for easy understanding with minimum interpretation.				Contractual Framework: Constitutive Agreement and its Appendices should be prepared carefully
2.1.2	**Transparency** No pitfalls or hidden drivers/goals.				Link to potential target in the legal framework, if any
2.1.3	**Standardization and compliance** Content and structure based on common rulebook definition, templates and related standards. For example, adapts to regulation related to different types of data.				Contractual Framework: Constitutive Agreement and its Appendices should be prepared to take into account general and industry specific regulatory requirements
2.1.4	**Wide Coverage** Covers all contracts, recommendations, promises, and binding/non-binding materials like rule of conduct, including also negative use cases. Ability to manage also misuse, termination and exits (e.g., rights to data, data life cycle).				Contractual Framework: Constitutive Agreement and its Appendices should be prepared to take into account different scenarios. A sound Governmental Model is vital for ensuring its relevance in the long term.
2.1.5	**Control** Define the control of derivative data and products.				Contractual Framework: Constitutive Agreement and Dataset Terms of Use
2.1.6	**Precedence** Define to precedence of secondary or related rulebooks and contracts as well as relationship to existing common and domain specific laws (e.g., GDPR, IPR, health, occupational law, trade secrets, competition law, ...)				Contractual Framework: Constitutive Agreement
2.1.7	**Confidentiality** relation to other confidentiality agreements.				Contractual Framework: Constitutive Agreement
2.1.8	**Scalability** Scalable contractual structure allowing machine and distributed use, e.g., readiness to support blockchains.				Contractual Framework: Constitutive Agreement, Network Description, Governmental Model
2.1.9	**Governance** Governance covers all participants and use cases and adheres to common laws, rules, and regulations.				Contractual Framework: Constitutive Agreement, Governmental Model
2.1.10	**Commitments and penalties** What kind of commitments and penalties are given (e.g., Service Level Agreement; contract breach fees, trade secrets, IPR-protection, indemnification).				Contractual Framework: Constitutive Agreement, Service Level Agreements, Dataset Terms of Use

3.2 Liabilities

ID	Checkpoint	OK	NOK	N/A	Comments
2.2.1	**Real-world actions** Have the liabilities for the data-related real-world processes been defined?				Contractual Framework: Constitutive Agreement, Dataset Terms of Use
2.2.2	**3rd party participation** Is the role towards 3rd parties clear? Who is responsible for 3rd party infringements? What commitments does the data provider give toward 3rd parties?				Contractual Framework: Constitutive Agreement, Dataset Terms of Use
2.2.3	**Disclaimers** Have the data related disclaimers been defined for data network participants?				Contractual Framework: Constitutive Agreement, Dataset Terms of Use

3.3 Content

ID	Checkpoint	OK	NOK	N/A
2.3.1	**Applicable data types** Does the data contain photos, audio – or video content, computer programs, etc. that have special legal requirements?				Contractual Framework: Constitutive Agreement, Network Description, Dataset Terms of Use
2.3.2	**Database rights** Are database rights applicable to data (i.e., data collection forms an entity and has required substantial effort)?				Contractual Framework: Constitutive Agreement, Dataset Terms of Use
2.3.3	**Common contractual aspects** Define the data network's approach for example on • Member rights and responsibilities • 3rd party transfers • Exclusivity/Access • Confidentiality • Liabilities and disclaimers • Audit rights • Applicable law and dispute resolution				Contractual Framework: Constitutive Agreement, Network Description
2.3.4	**Data-specific aspects** Define the data network's approach for example on • Conditions to exchange data • Clarity of usage rights • Right to assess, analyse and learn from data • Restrictions on data use within data network • IPR limitations and monitoring of IPR use Management of data originating from outside current data network • Conflicts related to data utilization				Contractual Framework: Constitutive Agreement, Dataset Terms of Use

4 TECHNOLOGY QUESTIONS

These questions are provided as examples of questions to be solved as part of the data network solution. Actual needs and related questions are strongly dependent on the approach (make, buy, rent) and scope of the solution (what is implemented centrally, what is implemented internally at data network participants).

4.1 Infrastructure and common solutions

ID	Checkpoint	OK	NOK	N/A	Comments
3.1.1	**Key principles and design philosophy** Design key principles for technology solution, including e.g., key technology choices, requirements, interfaces and system architecture?				Technical document: Purpose and system overview, System design and architecture, Functional and non-functional requirements, References and standards Contractual Framework: Constitutive Agreement, Network Description, Technical Requirements
3.1.2	**Security and privacy** How security and privacy are implemented in the data network?				Technical document: System design and architecture, Functional and non-functional requirements – security, References and standards Contractual Framework: Constitutive Agreement, Network Description, Security Requirements, Dataset Terms of Use
3.1.3	**Data-related mitigations** How to mitigate potential challenges in the data network and related services? Exception management and damage control?				Business document: Governance and KPIs Technical document: Purpose and system overview, System design and architecture, Functional and non-functional requirements -security Contractual Framework: Constitutive Agreement, Security Requirements, Governmental Model
3.1.4	**Standards and common structure** What common standards and structures are used? How they are governed?				Technical document: Purpose and system overview, System design and architecture, References and standards Contractual Framework: Constitutive Agreement, Network Description, Technical Requirements, Governmental Model

4.2 Core functionality

ID	Checkpoint	OK	NOK	N/A	Comments
3.2.1	**Interfaces** APIs and interface descriptions? Roadmaps and commitments?				Business document: Ecosystem scope, rules, and business models Technical document: Purpose and system overview, System design and architecture, Functional and non-functional requirements Contractual Framework: Constitutive Agreement, Network Description, Technical Requirements
3.2.2	**Access control and Identities** Are architectural standards or other standards and structures needed and defined?				Technical document: Purpose and system overview, System design and architecture, Functional and non-functional requirements, Contractual Framework: Constitutive Agreement, Network Description, Governmental Model, Service Level Agreements
3.2.3	**Consents** How are consents managed in the data network?				Business Document: Key stakeholders and their roles, Governance and KPIs Technical document: Functional and non-functional requirements – security, System design and architecture Contractual Framework: Constitutive Agreement, Network Description, Technical Requirements, Service Level Agreements
3.2.4	**Transaction management** How are transactions managed?				Technical document: Functional and non-functional requirements – security Contractual Framework: Constitutive Agreement, Network Description, Service Level Agreements, Technical Requirements

4.3 Administration

ID	Checkpoint	OK	NOK	N/A	Comments
3.3.1	**Monitoring and administration** What mechanisms exist for monitoring and administering of system and data use?				Business Document: Governance and KPIs Technical document: Functional and non-functional requirements, System design and architecture Contractual Framework: Constitutive Agreement, Dataset Terms of Use, Network Description, Governmental Model
3.3.2	**Data governance** What are the data governance (e.g., storage and availability) principles?				Business Document: Key stakeholders and their roles, Governance and KPIs, Ecosystem scope, rules, and business models Technical document: Functional and non-functional requirements - security System design and architecture Contractual Framework: Constitutive Agreement, Governmental Model
3.3.3	**Change control** What are the core change management principles?				Business Document: Key stakeholders and their roles, Governance and KPIs, Services and Infrastructure Technical document: Functional and non-functional requirements System design and architecture Contractual Framework: Constitutive Agreement, Governmental Model

5 DATA QUESTIONS

5.1 Governance

ID	Checkpoint	OK	NOK	N/A	Comments
4.1.1	**Data scope** What data is in data network's scope?				Business Document: Ecosystem scope, rules, and business models, Data streams and value transfers Contractual Framework: Constitutive Agreement, Network Description, Dataset Terms of Use
4.1.2	**Data location and availability** Where is data and related metadata located and how it is made available?				Business Document: Services and infrastructure, Data streams and value transfers, Governance and KPIs Technical document: Purpose and system overview, System design and architecture, Functional and non-functional requirements Contractual Framework: Constitutive Agreement, Dataset Terms of Use, Technical Requirements
4.1.3	**Data governance and responsibilities** Data life cycle management principles?				Business Document: Ecosystem scope, rules, and business models, Governance and KPIs Technical document: Purpose and system overview, System design and architecture, Functional and non-functional requirements Contractual Framework: Constitutive Agreement, Network Description, Dataset Terms of Use
4.1.4	**Data services** Need, implementation and monitoring of data-based services in the data network?				Business Document: Ecosystem scope, rules, and business models, Services and infrastructure, Governance and KPIs Technical document: Purpose and system overview, System design and architecture, Functional and non-functional requirements Contractual Framework: Constitutive Agreement, Network Description, Service Level Agreements

4.1.5	**Culture** What are high level cultural and transformational aspects enabling the collaboration and success in the data network? How those are managed?				Business Document: Purpose and core needs, Ecosystem scope, rules, and business models, Governance and KPIs Contractual Framework: Constitutive Agreement, Network Description, Governmental Model, Code of Conduct
4.1.6	**Data control** Are the rights to use and mechanisms to track the data use defined and monitored? How about data security?				Business Document: Ecosystem scope, rules, and business models, Services and infrastructure, Governance and KPIs Technical document: Purpose and system overview, System design and architecture, Functional and non-functional requirements Contractual Framework: Constitutive Agreement, Network Description, Security Requirements
4.1.7	**Skills and capabilities** What data-related skills and capabilities are required?				Business Document: Ecosystem scope, rules, and business models, Key stakeholders and their roles, Services and infrastructure, Governance and KPIs Contractual Framework: Constitutive Agreement, Network Description, Governmental Model

5.2 Data structure

ID	Checkpoint	**OK**	**NOK**	**N/A**	**Comments**
4.2.1	**Formats and structures** What common formats and structures exist in the data network?				Business Document: Data streams and value transfers, Ecosystem scope, rules, and business models Contractual Framework: Constitutive Agreement, Technical Requirements, Dataset Terms of Use

4.2.2	**Shared semantics** What data standards and shared semantics are used? How are these governed?				Business Document: Data streams and value transfers, Ecosystem scope, rules, and business models, Governance and KPIs Technical document: References and standards, Functional and non-functional requirements Constitutive Agreement, Network Description, Dataset Terms of Use, Governmental Model
4.2.3	**Data quality** What are the critical factors related to data quality and what actions are related to data quality?				Business Document: Data streams and value transfers, Governance and KPIs Technical document: System design and architecture, Functional and non-functional requirements Contractual Framework: Constitutive Agreement, Network Description, Service Level Agreements

6 ETHICAL QUESTIONS

6.1 Security

	Level description	**Checklist**
Level 0	"I believe that this is very secure"	
Level 1	There are proper security tools (e.g., antivirus and firewall) in use and updated.	-There are proper Antivirus, Firewall and other needed security tools in use and they are all properly updated.
Level 2	There is a dedicated person whose task is to keep up with information security.	-There is a dedicated person whose task is to keep up with information security.
Level 3	There are clearly documented procedures for the preparation of security threats.	-There are clearly documented procedures for the preparation of security threats -These security procedures and documents are updated when needed
Level 4	The whole organisation has internalised the importance of security and it is constantly monitored and developed through the organization.	-All employee roles are evaluated considering security issues and employees are given proper guidance. -Yearly report of security and plan for next year is yearly produced.

6.2 Commitment to ethical practices

	Level description	Checklist
Level 0	"We prefer not to commit, we are free"	
Level 1	Organisation follows regulations and best practices of the field of its own.	-Organisation is aware of the regulations and other provisions that concerns it and follows them -Organisation is aware and follows the best practices of its field
Level 2	Organisation has implemented and committed to following ethical code(s) or other codes of conduct.	-There is a dedicated person whose duty is to work with ethical issues and to ensure that codes are updated. -The codes are public (unless there is an acceptable reason not to publish some of them) and easy to find. -The employees are aware of codes and they have been instructed to follow them.
Level 3	There are clear procedures and documentation for the actions to be taken when ethical issues occur.	-Actions of organisation are evaluated and documented from ethical perspective and perceived problems are taken care -Clear support form management for ethical behaviour and there are official ways to inform about perceived issues (also without need for reveal identity of informer) -All members of organisation are committed to ethical working and there are support and resources available (working time and budget) for improving ethical issues.
Level 4	Organisational policies and procedures are developed critically form ethical perspective together with all relevant stakeholders.	-The aim is to ensure the ethicality and advance the benefits of all stakeholders, including the stakeholders outside own organisation- Individuals, other organisations and society -Public report of ethical situation and plans for the following years are produced and published annually. (Compare: financial statement)

6.3 Transparency and communication

	Level description	Checklist
Level 0	"Just Trust us"	
Level 1	Organisation follows the regulations and communicates truthfully.	-The communication in the organisation is truthful as regards both internal and external parties. -Organisation follows the laws and best practices of the field in respect of communication.
Level 2	Organisation supports open internal communication and responsible information sharing.	-Bringing forth of problems is encouraged and there are clear and supporting statement for this. -there are suitable official communication channels for individuals to bring forth their opinions with their names or anonymously.

Level 3	There is a transparent, documented plan for internal and external communication	-There exists a clearly written plan for internal and external communication that includes clear rules for communication for all the members of the organisation. -The communication rules support open communication instead of creating hostile and suppressing culture where fear of consequences prevents to real communication of “challenging“ issues.
Level 4	Organisation openly communicates its procedures and policies.	-The communication practises and culture are systematically evaluated and adequate adjustments in communication plan and in the organisation overall are conducted -Report of communication and plans for the following years is produced and published annually internally (and externally if relevant)

6.4 Sustainability

	Level description	**Checklist**
Level 0	“Let it burn”	
Level 1	Organisation has a documented sustainability plan/program.	-The organisation has a documented sustainability plan/program.
Level 2	There is an evaluation model for sustainability with clear indicators.	-There is a documented and validated evaluation model for sustainability with clear indicators.
Level 3	Organisation’s impact on the environment is neutral or positive.	-There is documented evidence of the current situation (see level 2).
Level 4	Organisation is actively advancing the sustainability of its business field.	-There is co-operation with other actors of the field (or beyond) that aims to sustainability in business field level by advancing and developing best sustainability practises.

6.5 Human-centricity

	Level description	Checklist
Level 0	"What has this to do with people?"	
Level 1	The individuals are recognised as stakeholders and their rights are taken into account.	-The use of personal information is analysed form the perspective of individuals whose information is used. -Risks to individuals are noted and mitigated.
Level 2	The organisation collects information about needs of individuals to improve human-centricity.	-Organization collects needed information with surveys, test cases, etc. to meet expectations of individuals
Level 3	Individuals have low-level ways to communicate with the organisation, and their opinions are systematically noted.	-It is easy to find communication channels for individuals (e.g., email, chat-boxes, etc.) for getting their opinions and concerns. -The received feedback is collected, documented and appropriately responded if possible.
Level 4	Organisation will actively involve all the relevant stakeholders in decision making.	-There is a clear way to include different parties in decision making. Representation of individuals (ombudsman, guardian of interests, etc.) in decision making bodies (e.g., board meetings) is implemented on an adequate level. -The gained feedback from individuals is actively used as a source for improving human-centricity by yearly updated plans.

6.6 Fair Networking

	Level description	Checklist
Level 0	"Anarchy"	
Level 1	Organisation aligns it rules and regulations to best practices of industry.	- Organisation is aware of regulations and best practises of its field. - Organisation follows those regulations and practices.
Level 2	Organization defines and documents practices and provides the needed information for network partners to advance co-	-The organisation is aware of its practises in network -The practices are documented and shared with

	operation with them.	partners to help cooperation in the ecosystem.
Level 3	Organisation supports and encourages a fair data sharing in ecosystems.	-The fair rules – how information is shared in the data ecosystem – is created together with ecosystem partners. -The rules are updated together when needed to ensure fairness.
Level 4	Organisation actively seeks ways to advance possibilities of the whole ecosystem.	- Organisation has procedures and a dedicated person to actively seek ways to advance the business possibilities in the data ecosystem.

6.7 Purpose

	Level description	**Checklist**
Level 0	"We do what we want to do"	
Level 1	Organization has stated reasons for data collection and usage	-Organisation has general principles for data collection and use.
Level 2	Organization has transparent rules how data can be used in the future	-There are public rules for data use in the organisation (e.g., in web-page)
Level 3	The organisation negotiates with information providers to gain mutual understanding of fair information use	-The information providers have clear procedures and channels to negotiate with the organisation on information use -The information use is based on mutual understanding between the organisation and information providers. -The mutual understanding is based on real communication – it is not mere consent procedure.
Level 4	Organisation has clear, public, documented goals and procedure of information use	-Organisation has clear, public, documented goals and procedure of information use which are publicly and easily available

	- Documentation contains current practises, known future plans, and risk analysis of the data use