RULEBOOK FOR A FAIR DATA ECONOMY – PART 2

The templates in the Part 2 of the *Rulebook for a fair data economy* enable organisations to create their own rulebooks for their data networks and support when defining the legal relations within networks. The templates are provided in an editable form so that they can easily be made into an actual rulebook to be adopted by a specific data network.

Editors:
Juhani Luoma-Kyyny, Leading Specialist, Sitra
Olli Pitkänen, CEO, 1001 Lakes Oy

Preface

The rulebook for a fair data economy (version 2.0) is a guide for creators of fair data economy networks. Agreement templates and other tools make it easier to build and join new data networks which highlight transparency in data sharing.

The rulebook contains:

- model agreement templates for legal, business, technical and administrative rules
- a range of control questions
- code of conduct templates

The rulebook consists of two parts: general content in the part 1 and editable templates in this part 2.

New in this version 2.0:

1. Completely new security part: Data Security Operating Model
2. Revised structure
   - Division in two parts: Part 1: “Why and How Rulebooks” introduction and Part 2: Rulebook templates
   - Checklists are embedded within the template structure, not as a separate Appendix
3. Improved readability and guidance
   - More instructions have been added to the templates
   - Overall improvements in readability and consistency throughout the document

The Rulebook Template was created by the Rulebook Working group under Sitra’s Fair Data Economy theme.

The Rulebook Template has been actively contributed to by Olli Pitkänen (editor, 1001 Lakes Oy), Sami Jokela (1001 Lakes Oy), Marko Turpeinen (1001 Lakes Oy), Viivi Lähteenoja (1001 Lakes), Jyrki Suokas (Sitra), Juhani Luoma-Kyyny (editor, Sitra), Saara Malkamäki (Sitra), Anna Wäyrynen (Sitra and Adesso Nordics Oy), Jorma Yli-Jaakkola (Borenius Attorneys Ltd and Lexia Attorneys Ltd), Otto Lindholm (Dottir Attorneys Ltd), Jani Koskinen (University of Turku), Jussi Mäkinen (Technology Industries of Finland), Kai Kuohuva (TietoEVRY Oyj, Fortum Oyj), Kari Hiekkanen (Aalto University), 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), and Sari Isokorpi (Medifilm Oy).

The Data Security Operating Model has been created on the initiative of Digipooli (Technology Industries of Finland), the organization of the Service Security, and with the support of The National Emergency Supply Agency. The Data Security Operating Model has been developed by 1001 Lakes Oy's experts Olli Pitkänen, Sami Jokela and Marko Turpeinen and Digipooli's pool secretary Antti Nyqvist. Digipooli members have actively participated in the work by presenting their views in workshops and commenting on the model.

Recommended citation: Sitra (2022), *Rulebook for a Fair Data Economy*, version 2.0

PART 2: RULEBOOK TEMPLATE

1 Introduction to Part 2

The purpose of this Rulebook Template as a whole is to provide an easily accessible and usable 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, it is important to note that the parties still need to check for 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.

The General Terms of the Rulebook Template as well as most of the Glossary, Code of Conduct, and Checklists in contract Annexes are the same for all the data networks that use the Fair Data Economy Rulebook 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.

The following templates that will enable organisations to establish rulebooks for their Data Networks have been prepared to support 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 rulebook 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.

This Part 2 of the Rulebook is provided as an editable text document so that it can be easily modified into the actual Rulebook that can be adopted by a specific data network. Once the modifications are ready, the contracts can then be copied directly and signed by the parties involved as needed.

The templates provided include:

- a template for establishing the answers to the contractual framework's key **Legal Questions**
- a template for a **Description of the Data Network**
- a template for a **Code of Conduct**
- the **General Terms and Conditions** (to be used as-is)
- a template for the **Constitutive Agreement**
- a template for the **Accession Agreement**
- a template for the **Governance Model**
- a template for the **Dataset Terms of Use**

We recommend that the network's founding members work together to modify each of the templates. Various tools are provided in the templates to support the modification and adaptation work. Different roles from the different parties should be involved in the modification process from the beginning. Specifically, modifications to templates A and E-H, as well as getting to know the terms D, should always include parties' legal roles. Work on templates B, C, H will benefit from executive, business development, and technical roles' contributions in addition. It is possible and even encouraged to work on the different parts of the Rulebook simultaneously, as decisions made in one context will affect possibilities in another. We do, however, recommend beginning work with template B, the description of the data network, to begin more concretely co-defining the objectives and motivations for the network.

2 Contractual framework: Legal questions [Template]

2.1 Contractual principles

General principles for the data network contractual framework; what are the key aspects to consider from the legal perspective:

Clarity	**Drive for easy understanding with minimum interpretation.** **(Affects: Constitutive Agreement and its Appendices should be prepared carefully)**
<your description here> **Contract-level requirements:** **Other requirements and notes:**	
Transparency	No pitfalls or hidden drivers/goals. (Affects: Link to potential target in the legal framework, if any)
<your description here> **Contract-level requirements:** **Other requirements and notes:**	
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. (Affects: Constitutive Agreement and its Appendices should be prepared to take into account general and industry specific regulatory requirements)
<your description here>	

Contract-level requirements:

Other requirements and notes:

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). (Affects: 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.)

<your description here>

Contract-level requirements:

Other requirements and notes:

Control

Define the control of derivative data and products.

(Affects: Constitutive Agreement and Dataset Terms of Use)

<your description here>

Contract-level requirements:

Other requirements and notes:

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, ...)

(Affects: Constitutive Agreement)

<your description here>

Contract-level requirements: **Other requirements and notes:**	
Confidentiality	relation to other confidentiality agreements. (Affects: Constitutive Agreement)
<your description here> **Contract-level requirements:** **Other requirements and notes:**	
Scalability	Scalable contractual structure allowing machine and distributed use, e.g., readiness to support blockchains. (Affects: Constitutive Agreement, Network Description, Governmental Model)
<your description here> **Contract-level requirements:** **Other requirements and notes:**	
Governance	Governance covers all participants and use cases and adheres to common laws, rules, and regulations. (Affects: Constitutive Agreement, Governmental Model)
<your description here>	

Contract-level requirements:

Other requirements and notes:

Commitments and penalties	What kind of commitments and penalties are given (e.g., Service Level Agreement; contract breach fees, trade secrets, IPR-protection, indemnification). (Affects: Constitutive Agreement, Service Level Agreements, Dataset Terms of Use)

<your description here>

Contract-level requirements:

Other requirements and notes:

2.2 Liabilities

Real-world actions	**Have the liabilities for the data-related real-world processes been defined? (Affects Constitutive Agreement, Dataset Terms of Use)**
<your description here> *Contract-level requirements:* *Other requirements and notes:*	

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? (Affects: Constitutive Agreement, Dataset Terms of Use
<your description here> *Contract-level requirements:* *Other requirements and notes:*	
Disclaimers	Have the data related disclaimers been defined for data network participants? (Affects: Constitutive Agreement, Dataset Terms of Use)

<your description here>

Contract-level requirements:

Other requirements and notes:

Content

Applicable data types	**Does the data contain photos, audio – or video content, computer programs, etc. that have special legal requirements?** **(Affects: Constitutive Agreement, Network Description, Dataset Terms of Use)**
<your description here> *Contract-level requirements:*	

Other requirements and notes:	
Database rights	Are database rights applicable to data (i.e., data collection forms an entity and has required substantial effort)? (Affects: Constitutive Agreement, Dataset Terms of Use)
<your description here> *Contract-level requirements:* *Other requirements and notes:*	
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 (Affects: Constitutive Agreement, Network Description)
<your description here> *Contract-level requirements:* *Other requirements and notes:*	
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 (Affects: Constitutive Agreement, Dataset Terms of Use)
<your description here> *Contract-level requirements:* *Other requirements and notes:*	

3 Description of the Data Network [Template]

3.1 Data Ecosystem Canvas [TOOL]

The Data Ecosystem Canvas below helps to describe the logic of the business and operational aspects of your data network. Use crisp and short answers to describe the key points. The various areas of the Data Ecosystem Canvas are specified in more detail in the Business and Operations Checklist.

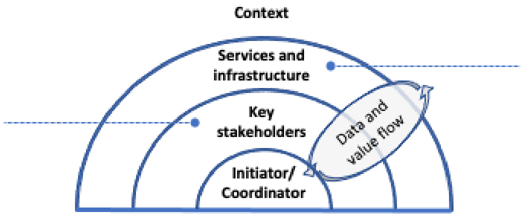
Data Ecosystem Canvas		
Purpose and core needs *What is the key purpose / problem why the ecosystem exists?* *What are the (initial) key use cases?* *What is the context of the data ecosystem?* *How is value generated and distributed in the data ecosystem?*		**Issues and questions** *What issues and questions are raised regarding the case?*
Key stakeholder and their roles *Who are the key stakeholders, i.e. Data providers and data consumers and their roles?*	 Context Services and infrastructure Key stakeholders Initiator/ Coordinator Data and value flow	**Services and infrastructure** *What value adding services are needed in the ecosystem?* *What infrastructure is required?*
Ecosystem scope, rules and business models *What is in- and out of scope?* *What are the ground principles of the ecosystem?* *What is the driving business logic and model?*	**Data streams and value transfer (give-gets)** *What data streams are covered by the ecosystem?* *What value is generated and transferred between entities (give)?* *How value is compensated (get)?*	**Governance and KPIs** *Who/how is the ecosystem created?* *How is the ecosystem governed and how its is monitored?* *What is the change mechanism for the ecosystem?*

Figure 1 Data Ecosystem Canvas.

3.2 Business and Operations Checklist [TOOL]

The Data Ecosystem Canvas is completed and extended by answering the business and operational checklist questions in the table below. There is also a dedicated space for requirements that directly influence the formulation of contracts, and more space for other requirements and notes. Comments provide further instructions and guidance for fulfilling these questions.

Business and Operations questions are categorized as follows:

- Purpose and goals
- Roles and responsibilities
- Business logic and data value
- Governance
- Data services and infrastructure

BO.1 PURPOSE AND GOALS

B0.1.1 Key purpose (DEC)	What is the purpose or problem why the ecosystem exists? [Describe the “raison d'être” for the network of participants that form the ecosystem. Examples: supply chain, maintenance services, research and innovation activity, logistics, business cooperative, data marketplace or platform, testbed.]
<your description here> Contract-level requirements: Other requirements and notes:	
Use cases for data (1.1.1)	What is the “job-to-be-done” that requires data sharing? [Give your use case a crisp and illustrative name type “Managing vehicle service recalls in the automotive industry” or “Calculating carbon footprint of a food product”. If you have no specific use cases in mind, skip this checklist question.]
<your description here> Contract-level requirements: Other requirements and notes:	
BO.2 ROLES AND RESPONSIBILITIES	
B0.2.1 Data network stakeholders (1.3.2, 1.3.3)	Who are the actors in the data network? [Is the data network ready for fair and trusted collaboration? Are there limitations or minimal requirements regarding joining the network? What kind of additional partners are sought for the data network? Are there other stakeholders that should be considered (e.g., officials, influencers to the data etc.)?]

<your description here> Contract-level requirements: Other requirements and notes:	
B0.2.2 Stakeholder roles (1.3.4)	What are the roles of the actors in the data network? [Who is in a leadership position? Are critical roles fulfilled to launch the data network? Example roles: Data controller, data holder, data producer, data using service, end customer, data intermediary, MyData operator, public sector actors, other stakeholders. What is the change/nomination mechanism for roles? Note: One actor can be in multiple roles.]
<your description here> Contract-level requirements: Other requirements and notes:	
B0.2.3 Stakeholder rights and responsibilities (1.3.4)	What are the rights and responsibilities of the actors in the data network?
<your description here> Contract-level requirements: Other requirements and notes:	

B0.2.4 Data provision (1.3.1)	What are the data sources? Who controls the use of the data? [What data is in data network’s scope? What data is available via separate agreements (to the level important to the data collaboration)?]
<your description here> Contract-level requirements: Other requirements and notes:	
BO.3 BUSINESS LOGIC AND DATA VALUE	
B0.3.1 Business case (1.1.2)	What is the business case for the data network? [What are the applicable business models? Examples of possible business models: data marketplace, one-time payment for data, subscription payment for a data stream, reduction of costs, dividing profits from services, advertising. If the business case has not been defined, or is not relevant for your data sharing network, then skip this checklist question.]
<your description here> Contract-level requirements: Other requirements and notes:	
B0.3.2 Data value (1.1.3)	How is the data value generated and distributed amongst the participants? How is the data value compensated? [Possible aspects to consider: In what form is the data value? How will the data value be measured, priced and monetized? What other drivers push for data sharing (e.g., public sector’s open data principles)? If relevant and possible, take also into consideration the value of aggregated data, data analysis and learned models. What are the safeguards and monitoring

	mechanisms for value? Does the data have licensing fees or other monetary measures?]
<your description here> Contract-level requirements: Other requirements and notes:	
B0.3.3 Data network solution fundamentals (1.1.5, 1.3.5)	Have the data network related development and operating costs been identified? How will those be shared? [Options to implement the solutions: make, buy, or rent. How will the costs be allocated and to whom? Consider the costs of both the data network setup phase and the operating phase.]
<your description here> Contract-level requirements: Other requirements and notes:	
B0.3.4 Level of commitment (1.1.8)	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? For example; how do we ensure both fair use and fair supply of data in the network?]
<your description here> Contract-level requirements: Other requirements and notes:	

BO.4 GOVERNANCE	
B0.4.2 Data governance (3.3.2, 3.3.3, 4.1.3)	What are the data governance principles and responsibilities in the data network? [What are the data storage and availability principles in the data network? 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? What are the 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?]
<your description here> Contract-level requirements: Other requirements and notes:	
B0.4.3 Risk management (3.1.3)	What is your risk identification, management and mitigation process? [How are data-related incidents or disputes managed?]
<your description here> Contract-level requirements: Other requirements and notes:	
BO.5 DATA SERVICES AND INFRASTRUCTURE	
B0.5.1 Data ecosystem services (1.1.6, 4.1.4)	What ecosystem-wide data-related services are provided? [Focus here on responsibilities and operational aspects of service provision: technical details are filled in technical annex. 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)?]
<your description here> Contract-level requirements: Other requirements and notes:	
B0.5.2 Data usage control (1.1.9, 1.2.2, 1.2.3, 1.2.4)	What are the permissions and restrictions on data use? [Consider different dimensions of data use: Data utilization; Limitations and restrictions related to use; Data access, manipulation and distribution; Data life cycle management; Does data have restrictions on the nature of use (e.g., on-off -use, perpetual license, R&D only, etc.)? How is the confidentiality of data ensured? 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?]
<your description here> Contract-level requirements: Other requirements and notes:	
B0.5.3 Consent management (3.2.3)	How are consents for personal data managed, monitored, and reported? [This question is linked to previous one. Note also that the issues of personal data management are also discussed under the security part. What are the overall mechanisms for data usage control? How is the interaction with consent owners (e.g., persons) managed?]
<your description here>	

Contract-level requirements: Other requirements and notes:	
B0.5.4 Data location and availability (4.1.2)	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?]
<your description here> Contract-level requirements: Dataset SLA definitions Other requirements and notes:	
B0.5.5 Data quality (4.2.3)	How to ensure that the data quality is 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?]
<your description here> Contract-level requirements: Other requirements and notes:	
B0.5.6 Operational monitoring and administration (3.3.1)	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? How is the monitoring performed, real-time or after-the-fact? How is this implemented?]

<your description here> Contract-level requirements: Other requirements and notes:

3.2.1 Issues and questions

In this part, please consider open issues and questions related to the Business and Operational Annex.

A special dimension to consider is the required skills and capabilities, and you can use the space below for your remarks.

3.2.2 Links to related documentation

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

3.3 Technical and Security Checklist [TOOL]

Summarize and document here the key technical and security aspects and requirements. These aspects reflect common architectural requirements and design principles following the categorization:

- Capability requirements
- System design and architecture
- Functional requirements
- Information management
- Security
- Privacy and personal data

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.

TS.1 CAPABILITY REQUIREMENTS	
TS.1.1 Technical solution fundamentals (1.3.5)	What technical capabilities and solutions will be implemented as a common effort?

	[What key components are provided centrally and by whom? How are those developed? How are different parties integrated together?]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.1.2 Skills and capabilities (1.3.5)	What data-related capabilities are required from the data network and its members? [How to acquire and maintain these capabilities?]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.2 SYSTEM DESIGN AND ARCHITECTURE	
TS.2.1 System design principles (3.1.1)	What are the design principles, focus areas and design philosophy for the data network's common technology solution? [What existing data sharing, infrastructure and other reference solutions are used as the basis for the common solution? What are the key decisions related to overall architecture and technology choices (e.g., cloud solution, vendor independence), • To the extend needed, what are the key functional and non-functional requirements, available standards and reference implementations, interfaces and APIs, common roadmap.]
<your description here> Contract-level requirements:	

Other requirements and notes:	
TS.2.2 Metadata and data formats (4.2.1, 4.2.2)	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?]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.3 FUNCTIONAL REQUIREMENTS	
TS.3.1 Technical interfaces (3.2.1)	What interface descriptions are needed? How are they defined? [What kinds of interfaces does to solution provide? How mature are those interfaces or are changes expected? How will the evolution of the interfaces be managed, e.g., in regards to backward compatibility? Do you have a plan and/or roadmap for their evolution?]
<your description here> Contract-level requirements: Other requirements and notes:	

<table>
<tr><td>TS.3.2 Access control and
Identities (3.2.2)</td><td>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?
• Are there additional requirements for the identity and access management not readily solved by the selected solution, such as data stream identities or need to merge or split identities?</td></tr>
<tr><td colspan="2">&lt;your description here>
Contract-level requirements:
Other requirements and notes:</td></tr>
<tr><td>TS.3.3 Data usage control solution (3.2.3)</td><td>How are permissions and consents managed, monitored and reported?
• Consent management for personal and other data?
• How is the interaction with consent owners (e.g., persons) managed?
• What standards and/or solutions are used?</td></tr>
<tr><td colspan="2">&lt;your description here>
Contract-level requirements:
Other requirements and notes:</td></tr>
<tr><td>TS.3.4 Transaction management (3.2.4)</td><td>How data related transactions are monitored and governed?
[What capabilities are required and how they are governed? Agreeing and confirming transactions, e.g., digital signatures, access keys and identities? Monitoring and reporting of system and data use (e.g., monitoring APIs)?]</td></tr>
<tr><td colspan="2">&lt;your description here>
Contract-level requirements:</td></tr>
</table>

Other requirements and notes:	
TS.3.5 Data governance solution (3.3.2)	What are the data life cycle management and data governance technical solutions? [Will data be stored in the system? If yes, how do you plan to manage the data over its lifecycle from creation to use to its potential deletion? How do you, for example, manage personal data so that it is GDPR-compliant?]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.4 INFORMATION MANAGEMENT	
TS.4.1 Change control (3.3.3)	What are the 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?]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.4.2 Data location and availability (4.1.2)	How is data 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?]

<your description here> Contract-level requirements: Other requirements and notes:	
TS.4.3 Data services (technical implementation) (4.1.4)	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)?]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.4.4 Data quality (technical implementation) (4.2.3)	How is data quality 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?]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.5 SECURITY	

TS.5.1 Security risk and threat assessment (SEC, 3.1.3)	How are the risks and threats identified and assessed? [Data sharing is characterised by the movement of data across organisational boundaries from one physical location to another, for example via a cloud solution. Security risk assessments need to consider not only physical security and individual organisational issues, but also the risks associated with data networks and network interoperability. How are the risks at the data sharing network level collectively identified?]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.5.2 Data and data network related threats (SEC)	What threats are related to data and the operation of the data network? [What general data security threats should be addressed in the rulebook? How to manage and prevent potential challenges in the data network and services related to it? These threats include unintentional or intentional disclosure of data, user-based threats (phishing, social manipulation, access control), data hijacking (man-in-the-middle), insider threats, and technical threats such as data loss, ransomware, and cloud challenges. Which data-related security threats should be addressed in the rulebook? These threats include misuse of data, data leaks, inaccurate or poor quality of data, and data-related liability issues.]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.5.3 Security objectives and regulation (SEC)	What are the security objectives of each participant and the data network as a whole?

	[Does some specific regulation exists considering the data security of the planned data network? Security objectives should be defined from the perspective of both the individual participants and the network as a whole. In addition to general data legislation (e.g., processing of personal data), the target area of the rulebook may identify specific legislation that needs to be considered when defining security objectives and policies. How has security been addressed in existing data sharing solutions? What is the existing legislation in this area?]
<your description here> . Contract-level requirements: Other requirements and notes:	
TS.5.4 Risk and security management process and tools (SEC)	What risk and security management process and tools are applied to the data network? How? [Once threats and vulnerabilities have been identified, the severity of the threats to the data network can be assessed, for example by determining the probability of each risk and the magnitude of the damage if the risk materialises. This will help identify the risks that are most critical to address in the design of the data network. How to handle the common exception management and damage control? What combination of management tools will achieve the required level of security and transparency?]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.5.5 Confidentiality of data (4.1.2)	How is confidentiality of data defined and managed in the data network? What is the value of information to the various parties involved?

	[What is the damage if information is intentionally or unintentionally disclosed to third parties without the consent of the source and/or the network, or if it is used in breach of contract?]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.6 PRIVACY AND PERSONAL DATA	
TS.6.1 Inclusion of personal data (SEC)	Does the data transmitted on the data network contain personal data or is it even indirectly related to any identifiable human being? What are the purposes for personal data collection? [Personal data means any information relating to an identified or identifiable individual. Only if it can be certain that the data does not contain personal data can data protection legislation be disregarded.]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.6.2 Personal data management solution (3.2.3)	How are permissions for personal data processing technically managed, logged, monitored and reported? Is there a needed e.g., for anonymisation? [Processing data, for example by aggregating them so that they can no longer identify any individual person at all (anonymisation), can help to avoid the obligations of data protection legislation, whereby the data are no longer considered personal data. Anonymisation often requires a case-by-case assessment, but as a general requirement, identification must be irreversibly prevented and in such a way that the controller or other third party can no longer use the data in its possession to make the data re-identifiable.

	Note also that pseudonymisation, where personal data can be traced back to a specific individual, for example by means of a code key, is still interpreted as personal data.]
<your description here> Contract-level requirements: Other requirements and notes:	
TS.6.3 Personal data related obligations (SEC)	What are the obligations regarding the personal data? [In principle, the information obligations and right of the data subjects based on regulation apply to each party processing personal data, but a rulebook may agree on the joint handling of the information obligations for personal data. Alternatively, they may not be agreed separately, but each party will manage its own obligations.]
<your description here> Contract-level requirements: Other requirements and notes:	

3.3.1 Issues and Questions

What other issues and questions have emerged during the planning?

3.3.2 Links to related documentation

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

- References and standards

4 Code of Conduct [TEMPLATE]

4.1 Ethical maturity model [TOOL]

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	Organisation 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.	Organisation collects information of the needs of individuals to improve people-centricity.	Organisation defines and documents practices and provides the needed information for network partners	Organisation 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.	Organisation negotiates with information sources to gain mutual understanding of fair information use
Level 4	The whole organisation	Organisational policies and	Organisation openly	Organisation is actively	Organisation will actively	Organisation actively	Organisation has clear,

	has internalised the importance of security and it is constantly monitored and developed through the organisation.	procedures are developed critically from ethical perspective together with all relevant stakeholders.	communicates its procedures and policies.	advancing the sustainability of its business field.	involve all relevant stakeholders in decision making.	seeks to ways to advance possibilities of whole ecosystems.	public, documented goals and procedure of information use.

5 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 If 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 provided it is: (a) if disclosed in writing or in other tangible form, clearly marked as confidential or proprietary by the disclosing Party at the time of disclosure, or (b) if disclosed in other than tangible form, identified as confidential at the time of disclosure and confirmed and designated in writing to the receiving Party within fourteen (14) calendar days from the disclosure as confidential information by the disclosing Party.

"**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 Network” means the group consisting of the Parties who share Data in accordance with the Constitutive Agreement.

“**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. In case there is a need to clarify the borderline between Data and Derived material, additional requirements for what is not considered Derived Material shall be identified in the respective Dataset Terms of Use,

“**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 determination of role-specific responsibilities may be included in the Constitutive Agreement.

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 cease 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.

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).

End User

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

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

Redistribution of the Data

4.1 The Parties shall have the right to redistribute the Data to the other Parties, unless such redistribution has been specifically prohibited under applicable Dataset Terms of Use. Parties can redistribute Data to Third Party End Users only if permitted under the applicable Dataset Terms of Use.

4.2

4.3 If the Data Provider chooses to allow redistribution of the Data to Third Party End users, the Data Provider shall be responsible for determining those Dataset Terms of Use which apply to the redistribution. A Service Provider must include such terms and conditions concerning Data redistribution into any agreements or terms and conditions with Third Party End Users.

4.4 Notwithstanding the above, the Parties shall have the right to redistribute Data to their Affiliates, unless applicable Dataset Terms of use explicitly prohibit such redistribution. each Party shall be responsible for ensure that their Affiliates comply with the Constitutive Agreement.

4.5 Derived Material and its Redistribution

4.6 Rights to Derived Material shall belong to the Party generating such Derived Material and the restrictions of use set out for the Data in the Dataset Terms of Use shall not cover Derived Material. Any restrictions for the use or redistribution of Derived Material shall be explicitly set out in the Dataset Terms of Use, if any.

4.7 The Parties are entitled to redistribute Derived Materials to the other Parties and any Third Party, unless specifically prohibited in the applicable Dataset Terms of Use.

4.8 Processing and Redistribution of Personal Data

4.9 The redistribution of any Personal Data or Derived Materials created on the basis of any Personal Data may be subject to more detailed requirements and restrictions. Each Data Controller shall on its own behalf ensure that any redistribution and other use of Derived Material shall take place in accordance with applicable data protection legislation. Additionally, any conduct between Data Controllers and Data Processors shall be subject to the applicable Data Processing Agreements. The Parties may also choose to separately agree on more detailed stipulations about the processing of Personal Data as part of the Dataset Terms of Use.

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 these 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 Data Provider is responsible for ensuring that it has sufficient rights for the provision of Data in accordance with the Dataset Terms of Use.

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. 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 applicable data protection legislation and case law, unless otherwise prescribed by the applicable Dataset Terms of Use.

9.6 The Parties commit to provide reasonable assistance to the other Parties where such assistance is need in order for the other Party to comply with its obligations under the applicable data protection legislation.

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 Steering Committee_will have the right to terminate the Constitutive Agreement with the breaching Party with immediate effect. 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.

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

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.[1]

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

11.3 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 Parties are responsible for imposing the same auditing obligations as set out herein on their Affiliates and the Parties will act in good faith to ensure that the objectives of the Data Provider's audit rights materialise with regard to the subcontractors of a Party.

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

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

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.

6 Constitutive Agreement [Template]

PARTIES

1. [Founding Member no. 1]
2. [Founding Member no. 2]
3. […][1]

(Together the “**Parties**” or “**Founding Members**”.)

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

BACKGROUND AND PURPOSE

The Parties are contemplating the establishment of a Data Network in order to [●][6].

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.
”Representatives”	has the meaning set forth in Appendix 4.
“Secretary”	has the meaning set forth in Appendix 4.
""[7]	means

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:.][8] **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 updated List of Members is available to the Parties [●][9]

[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.][10]

The Data Network is subject to the following provisions:[11]

NO EXCLUSIVITY[12]

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**[13].

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.

DEROGATIONS TO THE GENERAL TERMS AND CONDITIONS

The Parties have agreed to replace the following clauses of the General Terms and Conditions as follows:[14]

[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
i. 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[15]

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.[16]

Any change in contact persons or relevant contact details must be disclosed immediately by the respective Party to [the secretary of the Steering Committee].[17]

LIMITATION OF LIABILITY

[The annual total liability of any Party[18] 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[19]

ENTRY INTO FORCE AND APPLICATION

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

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 Data shared under this Agreement, 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]

Page Break

______________________________	______________________________
Name:	Name:
Title:	Title:

______________________________	______________________________
Name:	Name:
Title:	Title:

7 Accession Agreement [Template]

ACCEDING PARTY

1. [Acceding Party][20]

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][21]

BACKGROUND

The Acceding Party has expressed its interest to accede to the Constitutive Agreement regarding [●] that was signed on [●].[22]

The Constitutive Agreement allows new [Parties][23] to accede the Data Network [provided that [●].[24]

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 [●].

"" means .

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 [●]].[25]

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 Data shared under this Agreement, 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 [●][26] identical counterparts, one for [each Party/Acceding Party and one for the Steering Committee].

In __________, on ______________ 20

[Signatures on the next page]

Page Break

______________________________	______________________________
Name:	Name:
Title:	Title:

______________________________	______________________________
Name:	Name:
Title:	Title:

8 Governance Model [Template]

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 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[28] 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:

- Approval of changes to the Constitutive Agreement and its Appendices
- [Approval of new Members to the Data Network][29]
- [Approval of new Datasets and/or Dataset Terms of Use][30]
- 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[31] 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][32].

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 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.

9 Dataset Terms of Use [Template]

DATA PROVIDER

(1) ________________ acts as the Data Provider.

SCHEDULES

Schedule	Description
1	Dataset Description [no. 1][2]
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.
"[defined term]"[3]	means [definition]

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

[2] **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.

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

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[●]][4] 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.

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[- ●]**[5]).

The Data Provider shall ensure that it possess all the necessary rights and authorizations to make the Data available for the use of the other Parties in accordance with the applicable terms and conditions.

PURPOSE(S) OF USE OF THE DATA

Subject to these Data Set Terms of Use, the Data Provider hereby grants the User a non-exclusive right to use the Data for the following purposes:[6]

(a)

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. 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 AND REDISTRIBUTION OF DATA

The Data may not be processed for [●].[7]

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

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

[6] **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.

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

CEASE OF PROVISION OF THE DATA

The Data Provider may cease the provision of the Data by notifying the other Parties of the Data Network at least [thirty (30) days] prior to the end of provision of. the concerned Data.

DERIVED MATERIAL

The following shall not be considered as Derived Material and the rules relating to the use of Data continue to apply in case:

[(i) the Data can be readily converted, reverted or implied from the Derived Material to recreate the Data;

(ii) the Derived Material can be used as a substitute for the Data;

(vi) individual Data Providers of the Data can be identified from the Derived Material;

(vii) the Derived Material contains any Data Provider's Confidential Information; or

(viii) (v) ...]

[For the avoidance of doubt, in case a Dataset is modified only in minor ways and used for substituting the original Dataset, it shall not be regarded as Derived Material and remains under the restrictions set out above for the Data.]

[RESTRICTIONS ON THE USE AND REDISTRIBUTION OF DERIVED MATERIAL]

Derived Material may not be used for [●]]

FEES AND PAYMENT TERMS

The use of Data is subject to fees and charges, as further defined in **Schedule 1**.[8]

REPORTING

The use of Data is subject to the following specific reporting obligations: [●].[9]

AUDIT

The use of Data is subject to the following specific audit obligations: [●].[10]

[8] **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.

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

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

DATA SECURITY

The use of Data is subject to the following specific data security obligation: [●].[11]

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: [●].[12]

DATA PROTECTION

The Data includes personal data, and its reception and processing is subject to the following: [●].[13]

INTELLECTUAL PROPERTY RIGHTS

[●][14]

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]].[15]

EFFECTS OF TERMINATION

[●]

[11] **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).

[12] **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.

[13] **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.

[14] **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.

[15] **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.

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.

REFRAINING FROM SHARING DATA AND AMENDMENTS

The Data Provider may refrain from sharing Data within the Network and change these terms and conditions (including but nor limited to the content or quality of the Dataset) at any time by notifying all other Members to the Network of such change in writing. The provision of Data will end or the modified terms will enter into force within ninetyfourteen (1490) days after the Data Provider has notified the other Members of the refraining of sharing or 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.

[●][16]

OTHER TERMS

For the avoidance of doubt, it is acknowledged that above terms and conditions shall in no way restrict the rights of the users that are based on applicable mandatory law. In case of any discrepancy between such mandatory law and these terms and conditions, the mandatory law shall prevail.

APPLICABLE LAWS AND DISPUTE RESOLUTION[17]

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.

[16] **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.

[17] **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.