DIH AGRIFOOD Data Space Rulebook (version 2.0)



DATA SPACE

1. Introduction

The purpose of this Rulebook is to describe how DIH AGRIFOOD Data Space (DADS) is established while setting out general terms, legal relations within the DADS and conditions for data sharing agreements, following a vision of promoting data economy in the agri-food sector and rural development.

This Rulebook and its respective sub-sections are based on the Rulebook model for a fair data economy (Version 3.0) published by Sitra[1], under the Creative Commons Attribute 4.0 International license[2] and modified in order to accommodate specific geographical, technical, economic and social conditions of the DIH AGRIFOOD ecosystem.

By following this approach, we have been pursuing the goal of different European Data Spaces using similar rulebooks, ensuring fair, sustainable, and ethical business within the data ecosystems, which in turn enables increasing know-how, trust, and common market practices. Moreover, this will simplify collaboration and data sharing between data spaces and make it easier for an organisation to participate in several data spaces.

[1] https://www.sitra.fi/en/publication/rulebook-for-a-fair-data-economy/
[2] https://creativecommons.org/licenses/by/4.0/

CONTENT

1. INTRODUCTION 2

2. GENERAL PART 4

2.1 DIH AGRIFOOD Data Space 5

2.2 The Roles and Interactions within the DADS eco-system 7

2.3 The structure of the DIH AGRIFOOD Data Space Rulebook 9

3. DEFINITIONS/GLOSSARY 10

4. DADS CONTRACTUAL FRAMEWORK 16

4.1 General Terms and Conditions 16

4.2 Constitutive Agreement 30

4.3 Accession Agreement 35

4.4 Dataset Terms of Use 38

4.5 Governance Model 44

4.6 Description of the DIH AGRIFOOD Data Space (DADS) 49

4.6.1 DADS description – Business part 49

4.6.2 DADS description – Technical part 50

5. DIH AGRIFOOD DATA SPACE CODE OF CONDUCT 54

6. DATA SECURITY OPERATIONAL MODEL 58

2. General part

The agri-food sector is undergoing a transformation in the direction of becoming digitally enhanced, with data being generated during agricultural production, food processing, delivery and consumption. This data is being collected, transferred, stored, processed and analysed. It is essential to acknowledge and make sure that the farmer, food producer, food processor or any actor producing data remains at the heart of the data collection, processing and management. The agri-food sector is also one of the main pillars of rural development and together with other sectors and actors, directly influences environmental, economic and social sustainability.

Digital technologies in agri-food and other rural-based sectors make the collection and exchange of data possible at an unprecedented level. In order to tap into all of the potential benefits, data sharing between different stakeholders must be conducted under fair and transparent rules. The increasing exchange of data poses a major challenge for these sectors since it raises questions about privacy, data protection, intellectual property, data ownership, relationships of trust, storage, conservation, usability and security.

The collection of agri-food data includes, among others, land and agronomic data, livestock and fishery data, climate data, machine data, financial data, farmer reporting data, etc. It is important to understand that some of this data may be considered to be personal data, sensitive data or be seen as confidential information. **Agri-food and other rural actors are willing to share data and engage in a more open data mindset only if the benefits and risks associated with sharing data are made clear to them while making sure that they can trust in data exchanges that are settled in a proper and fair way. Transparency and responsibility are key to gaining trust, and if such principles are established and followed, then it will be possible to construct new and exciting business models that benefit all stakeholders involved and the agri-food and rural sectors.**

Contrary to the many direct and indirect benefits that data sharing brings, there are lots of obstacles and challenges that prevent cross-organisational data sharing. They include:

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

The organisation around DADS, with the help of this Rulebook, is providing a great deal of support in overcoming these obstacles.

2.1 DIH AGRIFOOD Data Space

DIH AGRIFOOD Data Space (DADS) is a federally organised data-sharing platform where data from the agri-food sector and rural sectors is shared on the basis of pre-defined policies and rules defined by the data management model. The data management model is based on ethical principles and guidelines provided by the European Commission. These principles **guarantee data sovereignty of Data Providers and transparency of data collection and sharing among all stakeholders in the Data space**.



Figure 1: DIH AGRIFOOD Data Space (DADS) logo

The essence of DADS is not only technology, but an overall concept or set of approaches that enable faster digital transformation of the agri-food sector and rural areas, with a special focus on environmental, economic and social sustainability, while following the principles described above. The DADS follows the future-proof approach, where Data spaces should be ubiquitous, both geographically and in terms of linking different domains and data silos. Primarily, however, the **DADS is focused mainly on attracting all actors from agriculture, food processing, food supply and rural development.**

The DADS is technically provided, managed and governed (according to the Governance Model presented in this Rulebook) under the umbrella of the Digital Innovation Hub AGRIFOOD (DIH AGRIFOOD) and its members.

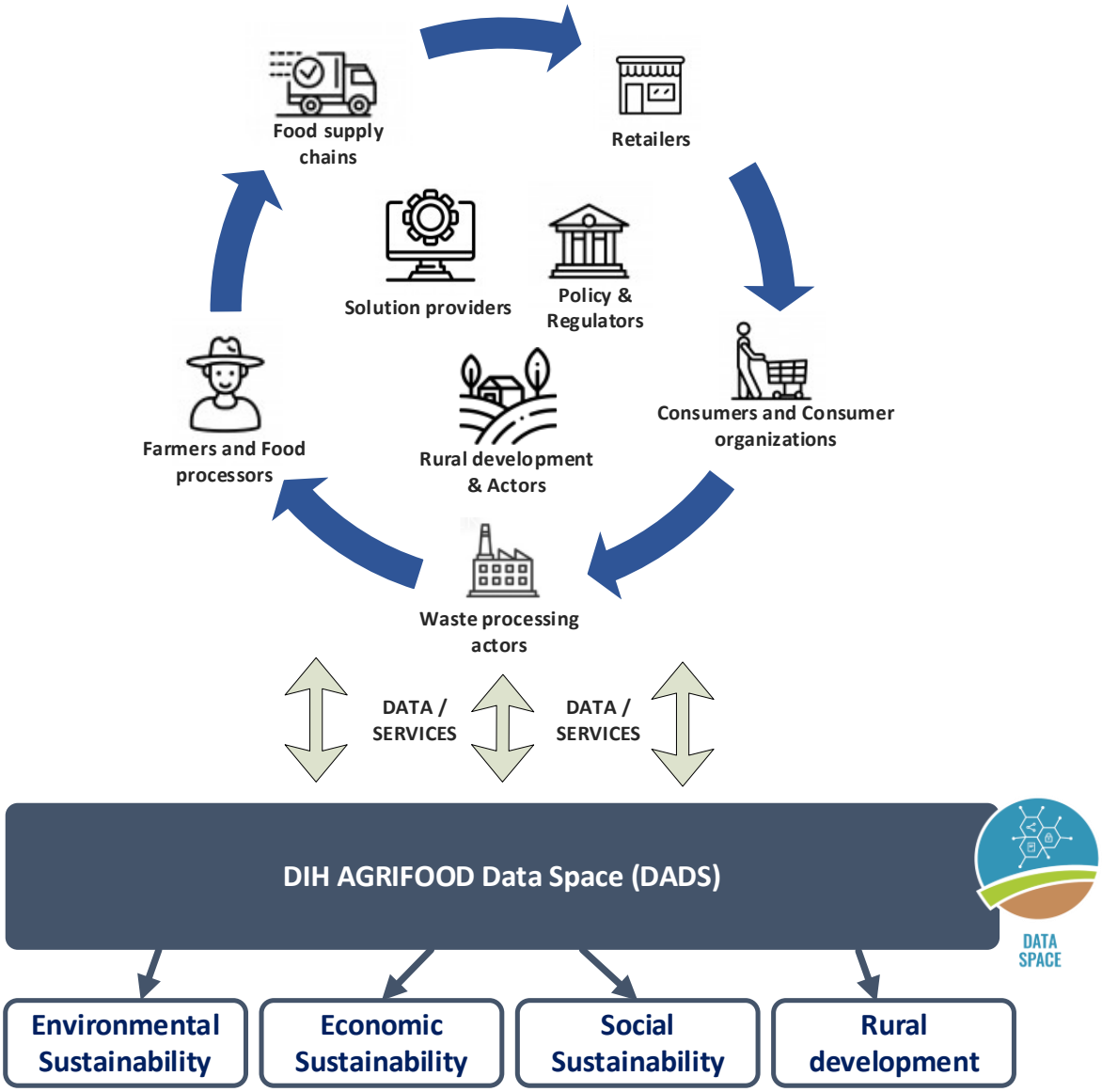


Figure 2: DADS strategic orientation

The DADS represents a technological/administrative data-sharing platform that defines:

- Agri-food and rural development domain terminology (how to name what and what it means);
- Translations of the attributes in the agri-food and rural development domain (in human-readable form);
- The semantics of the agri-food and rural development domain (how to structure data in the same way — machine-readable);
- Rules, definitions and operationalisation of how data is collected, stored, processed, shared and used.

The DADS allows any interested Data OwnerProvider, Data Service Provider or any stakeholder , to provide/share data or use data through the DADS. This includes the possibility that the stakeholder implements its own APIs or APIs and Connectors , which will allow access to the specific datasets. The functional and non-functional requirements, as well as the data structures of these APIs or APIs and Connectors, are defined in this Rulebook.

The DADS allows all stakeholders to access data through the APIs or APIs and Connectors of the Data Providers, accompanied by the following functionalities:

- Overview and selection of various data sources;
- Control of data rights by Data Providers;
- Unified semantic data model;
- The possibility of monetising the sharing of data.

The DADS thus represents one of the foundations for the development of the data economy in the agri-food sector and rural development, so that based on the data shared in the Data space, completely new services will be created, which will provide added value for all actors in the food supply chain and wider rural development.

2.2 The Roles and Interactions within the DADS eco-system

In order to be able to use its own and others' data, the individual or organisation needs to understand the business, legal, technical, and ethical perspectives of data sharing. It should, especially, recognise in which roles it acts in the DADS, which data processing and refining capabilities it needs to have, and what the minimum requirements are to participate in the DADS. The main roles of the actors within the DADS are the following:

- **Data Provider**: a Data Space participant that technically provides Data to the Data Users who have a right or duty to access and/or receive that Data.
- **Data User:** a Data Space participant to whom the rights to use Data are granted.
- **Operator:** a provider of one or several technical, legal, procedural or organisational services that enable data transactions to be performed within the Data Space. These may include, for example, identity management, consent management, logging, and/or service management and may or may not fall in the scope of the data intermediation service providers defined by the Data Governance Act (DGA).
- **Service provider:** a Data Space participant that provides value-added services on top of Data in the Data Space.
- **Data Rights Holder:** an entity (a human being or a legal entity) that has rights and/or obligations to use, grant access to, or share certain personal or non-personal Data. The Data Rights Holder has permission to process the Data and, taking into account other Data Rights Holders who may have rights to the same Data, may on his/her/its own behalf grant permissions to other actors to use the Data. There can be any number of these actors regarding certain Data, and they may transfer such rights to others.

- **Third-Party Data User:** an entity (a human being or a legal entity) that is not a participant of the Data Space that the rulebook governs, but who receives or uses data technically (otherwise like a “Data User”, but not a Data Space Participant).

In specific cases, the DADS can also introduce the role of the **Observer** (Auditor, Clearing House, Notary, etc.), in line with ISO/IEC 20151, with the responsibility of receiving transaction logs from other participants and offering services based on those.

The following Figure represents the roles and interactions within DADS.

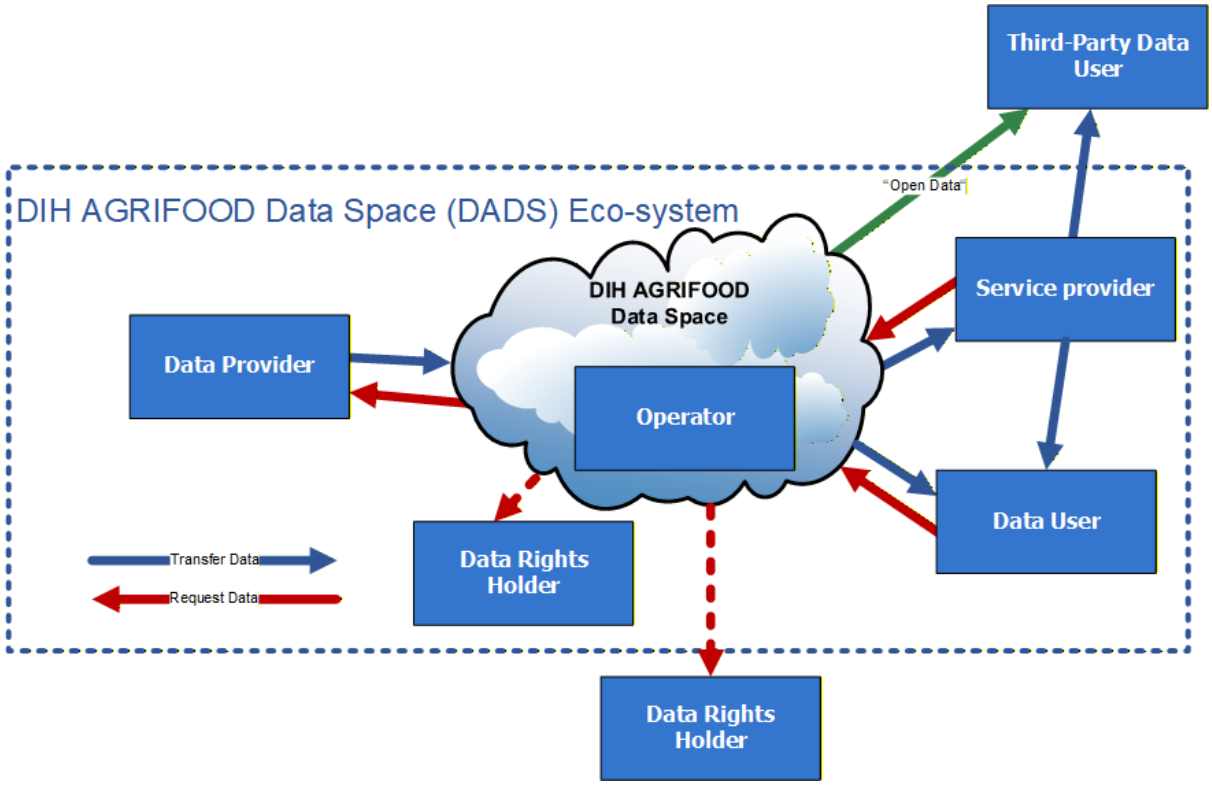


Figure 3: DADS Roles and Interactions

It is essential to keep in mind that each of the members of the data space can operate in multiple roles at the same time or change roles over time.

In terms of data requests and rights to use data, the DADS allow two types of approaches and functionalities:

(i) The Data Provider is allowing the use of its dataset according to the Dataset Terms of Use, which foresees a permanent definition of rights, defined at the time of identifying and assuring access to the new dataset.

(ii) The datasets of a specific Data Provider are provided based on a specific request for data, issued by the Data User or Service Provider. This particular case implies that the Data User or Service Provider is registered at the DADS, providing all technical and administrative means for the Data Providers' datasets to be available under issuing specific ‘’requests for

data'' that need to be approved by the Data Provider and other Data Rights Holders (if existing). Consequently, the Data Providers also need to be registered at the DADS, where they can manage and monitor their datasets.

2.3 The structure of the DIH AGRIFOOD Data Space Rulebook

The following Figure illustrates the relations between the different parts of a Rulebook for the DADS:

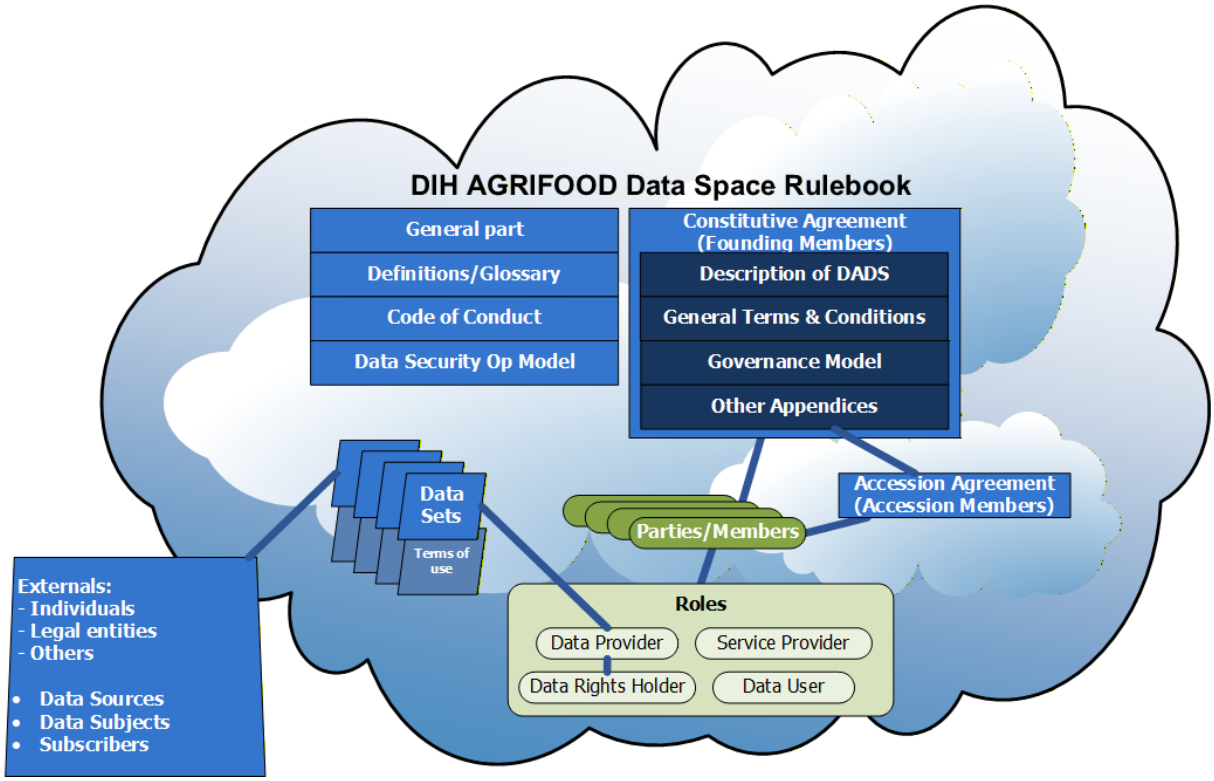


Figure 4: DADS Rulebook structure

The Rulebook structure for the DADS defines all legal, business, technical and governance elements that are necessary for the effective deployment of Data spaces (sometimes referred to as ''Data Networks'') such as DADS. Since many Data spaces will allow easy and secure data sharing within and between data spaces, we have decided to increase the level of interoperability by reusing the structure/model from Sitra[3]. It is easier and more cost-effective to create Data spaces and data ecosystems if the rulebooks of different Data spaces have a substantially similar basis. It simplifies collaboration and data sharing between Data spaces and makes it easier for an organisation to participate in several of them. This Rulebook shall therefore ensure fair, sustainable and ethical business within the data ecosystems, which in turn enables increasing know-how, trust and common market practices. Although we have built the DADS using the Sitra model, some parts of the Rulebook

[3] https://www.sitra.fi/en/publication/rulebook-for-a-fair-data-economy/

have been re-shaped and modified in order to accommodate specific geographical, technical, economic and social conditions of the DIH AGRIFOOD ecosystem.

3. Definitions/Glossary

For the purpose of this Rulebook and DADS in general, definitions are taken from three main sources and adjusted to respond to specific DADS requirements: the Glossary from Sitra Rulebook[4], the Code of Conduct for Agricultural Data Sharing by Contractual Agreement[5] and the Design Principles for Data Spaces[6]. The following definitions apply to the DADS:

TERM	DESCRIPTION
Aggregated Data	A combined dataset made up of a few or a wide range of sources (e.g. sensors, systems, farmers or data platforms). The aggregation of data can provide information (e.g. benchmarking and analytics) that can provide the Data Providers, Service Providers and/or Data Users with additional value when compared to data from a single source. Moreover, if revealing information is stripped away, the data aggregation can be done anonymously.
Agricultural Data	Data related to agricultural production, including farm data and all types of data generated within the farming processes.
Anonymised Data	Data that has been rendered anonymous, and is thus no longer personal, by irreversibly stripping it of any identifiable information. This makes it impossible to gain insights into a discreet individual, even by the party that is responsible for the anonymisation. Privacy laws, including GDPR, do not apply to anonymised data since it is not personal.
Application Programming Interface (API)	A technical interface consisting of a set of protocols and data structuring (API specifications) which enables computer systems to communicate directly with each other. Data or services can be directly requested from a server by adhering to the protocols.
Authentication	A process that is used to confirm that a claimed attribute of an entity is actually correct.
Authenticity	In the context of information security, authenticity refers to the truthfulness of the information and whether it has been transmitted or created by an authentic sender. Authenticity can be achieved, e.g. by digitally signing a message with the sender's private key. The recipient can verify the digital signature with the matching public key.

[4] https://www.sitra.fi/en/publications/rulebook-for-a-fair-data-economy/#preface-and-templates

[5] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi37ufu6KP8AhWocfEDHVg6Ci0QFnoECAgQAQ&url=https%3A%2F%2Ffefac.eu%2Fwp-content%2Fuploads%2F2020%2F07%2Feu_code_of_conduct_on_agricultural_data_sharing-1.pdf&usg=AOvVaw320fQ9hEpAvyLa9jASzaYA

[6] https://design-principles-for-data-spaces.org/

Authorisation	The process of giving someone or something permission to do something, for example, to gain access to services, data or other functionalities.
Authorisation Registry (AR)	An authorisation registry manages Records of Authorisation (and, if relevant, Records of Delegation) so that actors in the Data Spaces can verify whether a Data User is authorised to access specific data.
Big Data	Large volumes of highly diverse data that can be captured, analysed and used for decision-making.
Confidentiality	In the context of information security, confidentiality refers to the protection of information from disclosure to unauthorised parties.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Credentials	In the context of information security, credentials are used to control access of someone or something to something, for example, to services, data or other functionalities. The right credentials validate (i.e. Authentication) the identity claimed during Identification.
DADS	DIH AGRIFOOD Data Space
Data	All forms of information that are transferred between the Data Provider, Data User, Service Provider, Data Rights Holder or Third-Party Data User during the course of a business operation. Also, any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording. (DA Art 2(1), DGA Art 2(1))
Dataset	Dataset can be either a Data set, i.e., "a resource, comprising a collection of data published or curated by a single party and available for access or download in one or more representations", or a Data product, i.e., "a set of resources that complies with a data product specification and for which a data product owner has created and published a data product offering." In the Contractual Framework of the Rulebook, "Dataset" means a collection of Data the use of which is authorised by the Data Provider via the Data Space. Datasets and their related terms and conditions are defined in more detail in the respective Dataset Terms of Use.
Data Governance	A system that employs interoperability components (standards and policies) to ensure the acceptable use and high quality of data within a specific ecosystem. Manages the availability, usability, consistency, integrity, and security of the data used.
Data Lake	A data lake is a centralised repository designed to store, process, and secure large amounts of structured, semi-structured, and unstructured data.
Data Marketplace	A service through which Data Providers, Data Users, Service Providers or Data Rights Holders can offer, publish and access respective datasets and is a part of the DADS infrastructure. Data Marketplace contains a list of datasets with pointers facilitating access to those datasets and where the Data User or Service Provider is able to operate the applications (as an interface or for functionality) developed in the data platform.
Data Model	Description of how data can be stored, processed and accessed.

Data Platform	Software where applications are made available for data processing. Data platforms may be closed (just for members or open for Application Programming Interfaces - APIs), or may be open source hardware platforms and software libraries.
Data Portal	A list of datasets with pointers facilitating access to those datasets. Through portals, the Data User or Service Provider is able to operate the applications (as an interface or for functionality) developed in the data platform.
Data Processing	Any operation or set of operations that are performed on data or on datasets, whether by automated means or not, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or other methods of making the data available, alignment or combination, restriction, erasing or destruction.
Data Product	A structured, reusable package of data with metadata, usage terms, licensing, and delivery specifications. Designed for sharing within a data space, it enables secure data transactions and cross-organisational value creation while preserving data sovereignty.
Data Provenance	A record trail that accounts for the origin of a piece of data, together with an explanation of how and why it got to the present place.
Data Provider	A Data Space Participant that, in the context of a specific data transaction, technically provides Data to the Data Users that have a right or duty to access and/or receive that Data. In the Contractual Framework of the Rulebook, "Data Provider" means any natural person or organisation that provides Data for the Parties to use via the Data Space.
Data Rights Holder	An entity (a human being or a legal entity) that has rights and/or obligations to grant access to or share certain personal or non-personal data. The Data Rights Holder, taking into account other Data Rights Holders who have rights to the same data, may, on its own behalf, grant other actors' permissions to use the data. There can be any number of Data Rights Holders regarding certain Data, and they may transfer such rights to others. Also, an actor whose permission is needed to process data, e.g. an individual data subject (GDPR), an IPR rights holder (e.g. an author), a business having trade secrets, or a contracting party to have contractual rights in data.
Data Sharing	The practice of making data available to Data Users or Third-Party Data Users. Also, access to or processing of the same data by more than one authorised entity. Data can be shared, for example, (i) by allowing access to, or the execution of operations over, the original dataset, or (ii) by giving a copy of the data to the interested entity. The way in which data is shared fundamentally influences the available controls and the statements needed in the Rulebook. See also ISO/IEC 20151.
Data Sharing Economy	Creating the conditions for data trading, which requires a) non-financial incentive mechanisms, b) financial incentive mechanisms, including models to monetise data and methods to determine the value of data, and c) agreement mechanisms.

Data Sharing Interoperability	Providing the ability for all applications in Data spaces to create, use, transfer, and effectively exchange data. This requires, among others, the definition of data exchange APIs and data models supporting a) semantic interoperability, b) behavioural interoperability and c) policy interoperability.
Data Sharing trustworthiness	Ensuring that Data spaces operate according to expected requirements. This means that the development of data sharing applications must support a) security-by-design, b) privacy-by-design, and c) assurance-by-design.
Data Source	A source of data assets that are being exposed to Data Users or Service Providers by Data Providers or Data Rights Holders. A Data Source is responsible for collecting, storing, and controlling personal data that persons, operators, and data-using services may wish to access and use.
Data Sovereignty	The capability of an individual or organisation to be entirely self-determining with regard to their data.
Data Space	A distributed system defined by the Rulebook and enabling secure and trustworthy data transactions between participants while supporting trust and data sovereignty. A data space is implemented by one or more infrastructures and enables one or more use cases.
Data Space Governance Authority	One or more parties that establish, govern, manage and enforce the Rulebook of a Data Space. The Governance Model is a tool to define a contractual arrangement or a legal entity to set up the Data Space Governance Authority.
Data Space Participant	A party committed to the Rulebook of a particular Data Space and having a set of rights and obligations stemming from this Rulebook.
Data Storage	The recording (storing) of data in a storage medium. The Data Owner, Data Provider or Data Space Operator can store data in a primary location, in a data platform or in cloud-based storage platforms. The location in which data is stored is referred to as the “data storage location” or “storage location” or “storage site”.
Data User	A Data Space Participant to whom the right(s) to use Data are granted. A Data User can be a ‘data recipient’ as defined by DA 2(14) or a ‘data user’ as defined by DGA 2(9). In the Contractual Framework of the Rulebook, “Data 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.
Decision Support Information	Outcome of an application, usually information that supports decision-making.
DSXE	The DSX Engine extends the standard EDC framework to provide a decentralized dataspace. It introduces a decentralized participant discovery extension that connects each connector to a blockchain smart contract, allowing connectors to register and deregister themselves and maintain an up to date list of participants.
GDPR	General Data Protection Regulation, i.e. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the

	free movement of such data, and repealing Directive 95/46/EC. https://eur-lex.europa.eu/eli/reg/2016/679/
Governance	A system of rules, practices, and processes used to direct and manage a Data Space.
Interoperability	The ability of different systems to work in conjunction with each other and for devices, applications or products to connect and communicate in a coordinated way, without effort from the person.
IPR	Intellectual Property Rights, including copyright and its neighbouring or related rights, patents, trademarks, and other legal rights that protect intangible, intellectual property.
Metadata	Data that provides information on other data (e.g. author, units)
Open Data	Data that is provided by DADS (or any other data source) is openly accessible, exploitable, editable and shared by anyone for any purpose. Open data is the data/information that is published by DADS or (i.e.) other government-sanctioned portals, and this data is usually structured, machine-readable, open-licensed, and well-maintained.
Operator	A provider of one or several technical, legal, procedural or organisational services that enable data transactions to be performed within the Data Space. These may include, for example, identity management, consent management, logging, and/or service management and may or may not fall in the scope of the data intermediation service providers defined by the DGA. In the Contractual Framework of the Rulebook, "Operator" means any Party that provides data system or any other infrastructure services for the Data Space that are related, e.g., to identity or consent management, logging or service management.
Permission	Any legal right to the processing of Data (not only non-personal data as defined, e.g. in the Data Governance Act). A Permission can be, for example, a consent, a contractual obligation, a legal obligation, a vital interest, a public interest, an exercise of official authority, a legitimate interest, or the use of a connected product, if it legally authorises that specific processing of the Data.
Permissioning	Managing all kinds of legally relevant Permissions to use Data: not only active expressions of right holders' will, like consents, licenses, and agreements, but also, for example, direct legal rights to process Data for a specific purpose or processing data for the purposes of legitimate interests, subject to certain requirements. Permissioning is a process in which all the relevant Data Space Participants and external parties, e.g. Data Rights Holders, Data Users, Third Party Data Users, Operators, and Service Providers, contribute their share.
Personal Data	Any information and datasets relating to an identified or identifiable natural or legal person ('data subject'). An identifiable natural or legal person is someone who can be identified, directly or indirectly, notably by referring to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural or legal person.

	Also, any information relating to an identified or identifiable natural person. (GDPR Art 4(1))
Primary Data	Raw Data is transformed into values that are identifiable by people (primary processing). For example, field data (e.g. parcel, geological data, soil data, water data, cultivation, production-related data of a specific farm).
Provenance	Data origin.
Pseudonymisation	A procedure in which the most revealing fields within a data record are replaced by one or more artificial identifiers or pseudonyms. The pseudonym allows the data to be traced back to its origins, which distinguishes pseudonymisation from anonymisation. The purpose of pseudonymisation is to render the data record less identifiable and therefore lower the risks involved in its use.
Public Data	Data that can be freely used, reused and redistributed by anyone with no existing local, national or international legal restrictions on access or usage (e.g. Copernicus, weather data, Statistical office data, etc.). Very frequently, Public Data is unstructured and unruly, and its usage requirements are often vague. Public Data sources are often used to gather relevant data for DADS.
Raw Data	Data generated and collected without editing or any other form of processing.
Role	A function or set of responsibilities for a particular purpose.
Rulebook	A binding set of documents that records the Data Space governance structure and thus defines the Data Space.
Self-sovereign Identity (SSI)	A model for managing digital identities in which an individual or organisation has sole ownership over the ability to control their accounts and personal data without the need for intervening administrative authorities. SSI allows people to interact in the digital world with the same freedom and capacity for trust as they do in the offline world.
Service provider	A Data Space Participant that provides value-added services on top of Data or Datasets in the Data Space. In the Contractual Framework of the Rulebook, it is defined that “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 Data Users, other Service Providers or Third-Party Data Users.
Software Application	Processing of data (input) by transforming it into different data (output). Often presented as a graph, on a dashboard or in some other manner to allow for interpretation to be used as new decision-support information for value creation.
Structured Data Assets	Data that adheres to a predefined data model, useful primarily for interpretation by machines.
Third-Party Data User	An entity (a human being or a legal entity) that is not a participant of the Data Space that the rulebook governs, but who receives or uses data technically (otherwise like a “Data User”, but not a Data Space Participant).
Trust Framework	A structure that lets people and organisations do business securely and reliably online.
Unstructured Data Assets	Data that does not have a pre-defined data model or is not organised in a pre-defined way, making it primarily interpretable by humans.

4. DADS Contractual Framework

The DADS contractual framework is based on the following:

- General Terms and Conditions;
- Constitutive Agreement;
- Accession Agreement;
- Dataset Terms of Use;
- Governance Model.

4.1 General Terms and Conditions

1 APPLICABILITY, SCOPE AND GOVERNANCE

1.1 The DIH AGRIFOOD Data Space (DADS) is established by the Constitutive Agreement, which is signed by the Founding Members.

1.2 The provisions of these General Terms and Conditions will become applicable to and legally binding on the data sharing agreements of the Founding Members and Accession Members to the DADS, as applicable.

1.3 In the event that a discrepancy arises between any of the terms and conditions established in the Constitutive Agreement, 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 DADS as Accession Members.

Accession Members are parties in DADS that sign and execute the Accession 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 Founding Member or Accession Member.

Appendix means any appendix to the Constitutive Agreement or Accession 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 DADS is established and any of its appendices.

Data means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording, that Data Providers have distributed, transmitted, shared or otherwise made available to the DADS based on the Constitutive Agreement and/or Accession Agreement and during its period of validity as further defined in the respective Dataset Terms of Use.

Data Controller has the same meaning as defined in Article 4(7) of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). It refers to anyone who, alone or jointly with others, determines the purposes and means of the processing of personal data.

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 Processor has the same meaning as defined in Article 4(8) of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). It refers to anyone who processes personal data on behalf of the Data Controller.

Data Provider means any natural person or organisation that provides Data for the Parties to use via the Data Space.

Data Rights Holder means an entity (a human being or a legal entity) that alone or jointly with others has rights and/or obligations to grant access to or share certain personal or non-personal data.

Data Space means the group consisting of the Parties who share Data in DADS, in accordance with the Constitutive Agreement and Accession Agreement.

Data 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.

Dataset means a collection of Data whose use the Data Provider authorises via the Data Space. Datasets and their related terms and conditions are defined 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 Data Users and/or Service Providers.

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

Founding Members are the initial parties that execute the Constitutive Agreement and parties that sign and join the Constitutive Agreement at any given time, as per approval of the DADS Steering Committee.

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

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 Founding Members means a list of Parties that signed the Constitutive Agreement. The list is included as an appendix to the Constitutive Agreement and is updated upon the accession of new and the termination of existing Founding Members.

List of Accession Members means a list of Parties that signed the Accession Agreement. The updated list is published at the DADS Data Marketplace or Data Portal.

Operator means any Party that provides data system or any other infrastructure services for the DADS 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 DADS or to its Founding Members and/or Accession Members.

Party or Member means a DADS Participant, which is any Founding Member signing the Constitutive Agreement or any Accession Member signing an Accession Agreement.

Permission means any legal right to the processing of Data.

Permissioning means managing all kinds of legally relevant Permissions to use Data.

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**).

Request for Data means specific requests for certain Dataset(s) issued by the Data User and/or Service provider and approved by the Data Provider and/or Data Rights Holder (if needed), determining terms and conditions of such requested Data exchange and Data use. For the avoidance of doubt, the terms and conditions of Data exchange defined in the Request for Data shall be treated equally as the Dataset Terms of Use.

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 Data Users, other Service Providers or Third-Party Data Users.

Third Party means any party other than a Founding Member or an Accession Member.

Third Party Data 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 Founding Members, signing the Constitutive Agreement, and Accession Members signing the Accession Agreement (cumulatively addressed as Parties) are:

(1) the Data Provider,

(2) the Service Provider,

(3) the Data User and

(4) the Operator

A Party may simultaneously occupy multiple roles. In such a case, the relevant Party must comply with all applicable obligations related to each role and relevant Data. In addition, Third Party Data User is a role recognised under these General Terms and Conditions as applying to any stakeholders who are not a Party, but who receive Data.

3.2 A more specific description of the roles and the determination of role-specific responsibilities may be included in the Constitutive Agreement and/or the Accession 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 DADS. This includes the right to define the purposes for which relevant Data can be processed, the right to allow the redistribution of Data to Data Users and, where applicable, to Third Party Data Users, and the right to prohibit the unauthorised use of Data and the right to cease sharing Data within the DADS. The Data Provider must ensure that an adequate Permissioning mechanism is in place to make sure that the Data Rights Holders have control over their data to the extent applicable laws require, and the Data Users are able to get the Permissions they need. 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 Data Space being sent a notification of such change. Changes to the Dataset Terms of Use must not have a retroactive effect.

3.4 The Data Provider shall provide Data for the use of the DADS 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 methods).

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 DADS by approving the specific Request for Data issued by the Data User or Service Provider, subject to the definition of terms and conditions set out in the respective Request for Data.

3.6 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 DADS for a fixed period, in order to protect investments made in the DADS by specific Operators or Parties in good faith.

Service Provider

3.6 The Service Provider will be responsible for processing Data in accordance with the Constitutive Agreement and/or Accession Agreement and the applicable Dataset Terms of Use or in accordance with specific Requests for Data issued by the Service Provider.

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).

Data User

3.8 The Data User must use the Data in accordance with the Constitutive Agreement and/or Accession Agreement and the applicable Dataset Terms of Use or in accordance with specific Requests for Data issued by the Data User.

Operator

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

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.

3.12 Should an Operator or any other Party meet the definition of a data intermediary service provider under the Data Governance Act (DGA), the requirements set out in Chapter III of the DGA apply.

4 REDISTRIBUTION OF 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 Data Users only if permitted under the applicable Dataset Terms of Use or applicable laws.

4.2 If the Data Provider chooses to allow redistribution of the Data to Third Party Data 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 in any agreements or terms and conditions with Third Party Data Users.

4.3 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 ensuring that its Affiliates comply with the Constitutive Agreement and/or Accession Agreement.

Derived Material and its Redistribution

4.4 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.

4.5 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.

Processing and Redistribution of Personal Data

4.6 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

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 DADS and for the implementation of the Party's security policy.

5.2 Each Party to the DADS 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/or Accession Agreement, 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 any 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 DADS.

Subcontractors

5.6 The Parties will have the right to employ subcontractors to perform their obligations under the Constitutive Agreement and/or Accession 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 In general, Data is shared within the DADS free of charge, unless otherwise defined in the applicable Dataset Terms of Use. The Founding Members may decide and deploy a commercial model for Data sharing and DADS operation in the future, which shall be defined and presented in the Appendix: DADS description – Business part.

6.2 Notwithstanding the above, data will always be provided free of charge if required by the Data Act or other applicable law.

6.3 Each Accession Member will bear their own costs related to accessing the DADS and operating as a Member of the DADS.

6.4 Unless otherwise agreed by the Founding Members, the joint costs incurred for the maintenance and administration of the DADS will be allocated in equal shares between the Founding Parties. For the avoidance of doubt, the maintenance and administration of the DADS 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 DADS and/or regarding the DADS 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 DADS.

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

7.3 If a Party is, under the applicable law or an order issued by a competent authority, obliged to disclose another Party's Confidential Information to the authorities or Third Parties, the obliged Party must promptly notify the affected Party whose Confidential Information will

be disclosed of such disclosure if so permitted under the applicable law or the competent authority's order.

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

8.2 Signing the Constitutive Agreement or Accession Agreement and sharing any Data within the DADS 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 DADS 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 DADS, 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 processor. Where any such Data Processing Agreement is applicable in general to certain Dataset(s) or services provided, it must be included as an Appendix to the Dataset Terms of Use for each affected Dataset.

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 DADS 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.

10 TERMINATION AND VALIDITY

10.1 If the Constitutive Agreement or Accession 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 or Accession Agreement is concluded for an indefinite period, it will expire upon termination by the Founding Members or Accession Members.

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

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

10.4 Where the Founding Members have agreed on a process for amending the Constitutive Agreement otherwise than by the written consent of all Founding Members, any Founding Member 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 Founding Members thereof. The termination will become effective after the objecting Founding Member has submitted the aforementioned notice to the other Founding Members, after which the amendment will enter into force unless the agreeing Founding Members have agreed on a later date.

10.5 In the event that there are only two Founding Members to the Constitutive Agreement and one Founding Member commits a material breach of the provisions of the Constitutive Agreement, the other Founding Member will have the unilateral right to terminate the Constitutive Agreement with immediate effect by providing the other Founding Member 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 Founding Member/Founding Members may resolve to suspend the performance of their obligations under the Constitutive Agreement until the breaching Founding Member has rectified the breach.

10.8 In the event that the Accession Member commits a material breach of the provisions of these General Terms and Conditions, Accession Agreement, specific Dataset Terms of Use or Code of Conduct provisions as such, the Steering Committee will have the right to terminate the Accession Agreement with the breaching Accession Member with immediate effect. Notice of any such termination must be provided in writing to the affected Accession Member.

10.9 Where an Accession Member's membership in the Data Space is terminated as a consequence of the Accession Member's material breach of the Constitutive Agreement and/or Accession Agreement, the breaching Accession Member's right to use the Data will end at the date of the termination. The breaching Accession 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 Accession Member is entitled to retain the Data as required by the applicable law or competent authorities, provided that the breaching Accession 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 and/or Accession Agreement as defined hereinafter and, where applicable, in the Constitutive Agreement and/or Accession Agreement. Any other liabilities are hereby excluded unless otherwise specifically defined in the Constitutive Agreement and/or Accession 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.

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 and/or Accession 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 and/or Accession 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 of 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 are limited to verifying compliance with the material requirements of the Constitutive Agreement and/or Accession 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 be conducted by a mutually acceptable and/or certified independent Third party.

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

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 the dispute resolution mechanism defined in the Constitutive Agreement.

15 OTHER PROVISIONS

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

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

15.3 If any provision of the Constitutive Agreement and/or Accession 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 and/or Accession 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/or Accession Agreement, where applicable, to bind its Affiliates.

15.5 The Founding Members intend to create a DADS 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 Founding Members' principals, agents or employees. No Founding Member will have any right, power, or authority, express or implied, to bind any other Founding Member.

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 Founding Member in the Constitutive Agreement. Notices will be deemed to have been received three (3) days after being sent or on proof of delivery.

16.2 Clause 16.1 is not applicable to the Accession Members and the applicable Accession Agreement, where all notices relating to these General Terms and Conditions and the Accession Agreement can be sent in electronic form to the respective contact person.

16.3 Each Party is responsible for ensuring that its contact details are up-to-date.

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 or Accession Agreement in their entirety, together with any clauses of the Constitutive Agreement or Accession Agreement that logically ought to survive the termination.

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

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

4.2 Constitutive Agreement

PARTIES

(1) [Founding Member no. 1]

(2) [Founding Member no. 2]

[3] […]

(Together, the "**Founding Members**".)

Appendix	Description
1	Description of the DIH AGRIFOOD Data Space (DADS)
2	General Terms and Conditions
3	List of Founding Members and Contact Details
4	Governance Model
[5]	[Any other Appendices, such as Data Space Operator Service Agreement or any technical or data security specifications]
[●]	Code of Conduct

BACKGROUND AND PURPOSE

The Founding Members are contemplating the establishment of a DIH AGRIFOOD Data Space (DADS) in order to foster the digital transformation of the agri-food sector and rural development, ensure that data from the agri-food sector and rural based sectors is shared on the basis of pre-known policies and rules defined by the data management model, respecting ethical principles and guidelines provided by the European Commission. These principles guarantee the data sovereignty of Data Providers and transparency of data collection and sharing among all stakeholders in the Data space.

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.
"Representatives"	has the meaning set forth in Appendix 4.
"Secretary"	has the meaning set forth in Appendix 4.

"[defined term]" means [definition]

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

THE DIH AGRIFOOD Data Space (DADS)

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

The Founding Members agree that new members may join the DADS as Founding Members, subject to the following conditions:

- Candidate Founding Member holds an important role and contributes significantly to the digital transformation of the agri-food sector and rural development in Slovenia and/or wider region.
- Candidate Founding Member will contribute significantly to the DADS in terms of providing important services and knowledge essential for further development of DADS and the data economy, representing the relevant group of DADS stakeholders (such as Data Providers).
- Candidate Founding Member is holding at least one active role in the DADS (Data Provider, Service Provider or Data User).
- Candidate Founding Member is an organisation established and operational in Slovenia.

Appendix 3 (List of Founding Members and Contact Details) will be updated upon the accession of new Founding Members or termination of existing Founding Members, or any changes in the representatives or their contact details.

The ethical principles that apply to the DADS are laid down in **Appendix [X]** (Code of Conduct). The Founding Members agree to comply with these ethical principles in good faith in connection with their conduct within the DADS.

The DADS is subject to the following provisions:

NO EXCLUSIVITY

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

GOVERNANCE OF THE DADS

The governance framework that applies to the DADS is defined in further detail in **Appendix 4** (Governance Model).

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

DEROGATIONS TO THE GENERAL TERMS AND CONDITIONS

The Founding Members have agreed to replace the following clauses of the General Terms and Conditions as follows:

[Examples:

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

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

TERMINATION AND VALIDITY

This Agreement is concluded from the Effective Date, after which it remains in force for an indefinite period and is subject to a termination period of 3 months.

NOTICES

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

Any change in contact persons or relevant contact details must be disclosed immediately by the respective Founding Member to the Secretary of the Steering Committee.

LIMITATION OF LIABILITY

The Founding Members will only be liable for direct damages that result from a breach of the provisions of the Constitutive Agreement. Any other liabilities are hereby excluded.

Notwithstanding limitations of liability defined above, General Data Protection Regulation (GDPR), Article 82 applies 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

Every Founding Member agrees to promote, inform, communicate and actively support the use of DADS by new Members (Accession members such as Data Providers, Service Providers and data Users) and any other relevant stakeholders, by any means possible.

ENTRY INTO FORCE AND APPLICATION

This Agreement will enter into force when executed (signed) by all Parties.

APPLICABLE LAWS AND DISPUTE RESOLUTION

This Agreement is governed by and construed in accordance with the laws of Slovenia 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 Ljubljana Arbitration Centre at the Chamber of Commerce and Industry of Slovenia (LAC).

COUNTERPARTS

This agreement has been executed in **[x]** identical counterparts, one for each Founding member and one for the Steering Committee.

In _____, on xx.xx.20xx

[PARTY 1]	[PARTY 2]
_____	_____
Name: [Name]	Name: [Name]
Title: [Title]	Title: [Title]
[PARTY 1]	[PARTY 2]
_____	_____
Name: [Name]	Name: [Name]
Title: [Title]	Title: [Title]
[PARTY 3]	

_____

Name: [Name]

Title: [Title]

[PARTY 3]

_____

Name: [Name]

Title: [Title]

[Party 1] contact persons:

Contact person:

Name_Surname, e-mail, Tel.nr.

Designated contact person for data security matters:

Name_Surname, e-mail, Tel.nr.

[Party 2] contact persons:

Contact person:

Name_Surname, e-mail, Tel.nr.

Designated contact person for data security matters:

Name_Surname, e-mail, Tel.nr.

[Party 3] contact persons:

Contact person:

Name_Surname, e-mail, Tel.nr.

Designated contact person for data security matters:

Name_Surname, e-mail, Tel.nr.

4.3 Accession Agreement

ACCEDING MEMBER

(1) [Acceding Member]

APPENDICES

Appendix	Description
1	Constitutive Agreement
1.1	Description of the DIH AGRIFOOD Data Space (DADS)
1.2	General Terms and Conditions
1.3	List of Founding Members and Contact Details
1.4	Governance Model
1.5	Code of Conduct
1.6	[Any other Appendices to the Constitutive Agreement]

BACKGROUND

The Acceding Member has expressed its interest in acceding to the DIH AGRIFOOD Data Space (DADS) as an Accession Member. This gives Accession Member the right to use DADS in the capacity of one or more designated roles: Data Provider, Service Provider and/or Data User.

This will allow Accession Member to share data from the agri-food sector and other rural-based sectors, on the basis of pre-known policies and rules defined by the data management model defined in General Terms and Conditions, Accession Agreement and relevant Appendices, while respecting ethical principles and guidelines provided by the European Commission. These principles guarantee the data sovereignty of Data Providers and transparency of data collection and sharing among all stakeholders in the Data Space.

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 Member" means the entity defined under section Acceding Member.

"Accession Agreement"	means this Agreement.
"Constitutive Agreement"	means the Constitutive Agreement regarding the establishment of the DIH AGRIFOOD Data Space (DADS).
"[defined term]"	means [definition].

ACCESSION TO THE DADS

The Acceding Member has expressed its interest in acceding to the DIH AGRIFOOD Data Space (DADS), and the Constitutive Agreement allows new Parties to accede if they take one or more designated roles as Data Provider, Service Provider and/or Data User.

As the Acceding Member fulfils such requirements, the Acceding Member accedes to the DADS under this Accession Agreement.

ENTRY INTO FORCE AND APPLICATION

This Accession Agreement will enter into force as of its execution (signature) by the Acceding Member.

Each Accession Member must designate an Accession Member representative acting as a liaison between the DADS Steering Committee and the Accession Member and a contact person for data security matters, who is responsible for the relevant Accession Member's data systems that are connected to the DADS and for the implementation of the Accession Member's security policy.

GOVERNANCE OF THE DADS

The governance framework that applies to the DADS is defined in further detail in **Appendix 1.4** (Governance Model).

TERMINATION AND VALIDITY

This Agreement is concluded from the Effective Date, after which it remains in force for an indefinite period and is subject to a termination period of 1 month. The termination notice must be submitted in writing to the Secretary of the Steering Committee.

APPLICABLE LAWS AND DISPUTE RESOLUTION

This Agreement is governed by and construed in accordance with the laws of Slovenia 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 Ljubljana Arbitration Centre at the Chamber of Commerce and Industry of Slovenia (LAC).

COUNTERPARTS

This agreement has been executed in 2 identical counterparts, one for each Acceding Member and one for the Steering Committee.

In _____, on xx.xx.20xx

[ACCEDING MEMBER]

_____

Name: [Name]

Title: [Title]

Accession Member representative:

Name_Surname, e-mail, Tel.nr.

Designated contact person for data security matters:

Name_Surname, e-mail, Tel.nr.

4.4 Dataset Terms of Use

DATA PROVIDER & DATASET

[Data Provider name] acts as the Data Provider for the following Dataset - [Dataset name].

SCHEDULES

Schedule	Dataset description document title
1	Dataset Description for the [Dataset name]

BACKGROUND

The purpose of these Terms of Use is to define the Data that the Data Provider makes available through the DADS 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 Data User, Service Provider, Operator or Third Party Data User who processes any Data that is made available by the Data Provider under these Dataset Terms of Use.

"[defined term]" means [definition]

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

APPLICABILITY AND SCOPE

These Dataset Terms of Use apply to the Dataset provided by the Data Provider under a valid Accession Agreement 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 and/or Accession Agreement or any of its appendices and these Dataset Terms of Use, these Dataset Terms of Use and its Schedule 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 properties, as well as their location and method of distribution, are defined in the Dataset Description, Schedule 1.

The Data Provider shall ensure that it possesses all the necessary rights and authorisations 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 and a Service Provider a non-exclusive right to use the Data for the following purposes:

PERMISSION	THE PURPOSE	NOTE
Yes/No	**Research and innovation purposes**	Use of Data for academic research, non-profit research, government or public policy research, data shared to encourage innovation and collaboration, etc.
Yes/No	**Educational purposes**	Use of Data for educational purposes by educational or other institutions, for learning, self-education, or training without commercial purposes, educational content creation, etc.
Yes/No	**Supporting public advisory services**	Use of Data which upgrades and increases the quality and accuracy of agricultural advice and public advisory services in general.
Yes/No	**Training Artificial Intelligence & Machine Learning models**	Use of Data to teach AI and machine learning models.
Yes/No	**Development of standards**	Use of Data for creating industry standards, technical guidelines, or best practices.
Yes/No	**Commercial purposes**	Use of Data for product/service development, optimisation of processes, business analytics and forecasting, marketing and advertising, monetisation through third-party services, etc.
Yes/No	**Regulatory Compliance**	Use of Data for legal or regulatory reporting purposes to comply with government or industry-specific rules and regulations, and use of Data by third parties to verify processes, conduct audits, or ensure that certain compliance measures are in place.

RIGHTS AND RESTRICTIONS ON THE PROCESSING AND REDISTRIBUTION OF DATA

The Data Provider hereby grants the User a non-exclusive right to the Data, based on:

Option A: ''Open data'' terms and conditions	
Clarification: The Data Provider hereby grants the User a non-exclusive right to the Data to: - receive, process and reproduce; - refine and modify; and - redistribute the Data to the Third-Party Data User.	

Option B: ''Restricted/closed'' terms and conditions	
Clarification: The Data Provider hereby grants the User the right to: - receive, process and reproduce; - refine and modify; and - redistribute the Data to Third-Party Data User under restricted conditions	
B1: Restrictions in terms of User	1 – **All Users** have the right to: - receive, process and reproduce; - refine and modify; and - redistribute the Data to the Third-Party Data User 2 – **Only the following Users: (list of Users)**, and their own applications have the right to: - receive, process and reproduce; - refine and modify; and - redistribute the Data to the Third-Party Data User The rest of the Users will be granted rights as per the specific Request for Data. 3 – **All Users will be granted rights as per the specific Request for Data**.
B2: Fees and Payment Terms	1 – The use of Data **is not** subject to fees and charges. 2- The use of Data is subject to the **following fees and charges**: [text]
B3: Personal Data	1 – The Data includes no personal data, and/or the Data Provider is giving permission to the User to receive and process personal data. 2 - The Data includes personal data, and its reception and processing are subject to the following restrictions: [text]
B4: Other restrictions and/or limitations	1 - The Dataset includes **Confidential Information,** and consequently, its use and processing are subject to: [text] or NOT APPLICABLE

	2 - The use of Data is subject to the following specific **data security** obligation: [text] or NOT APPLICABLE 3 – The use of Data is subject to the following specific **Intellectual Property Rights** obligation: [text] or NOT APPLICABLE 4 - The use of Data is subject to the following specific **audit** obligations: [text] or NOT APPLICABLE 5 – The use of Data is subject to the following **duration (time)** limitations: [text] or NOT APPLICABLE 6 – Is the use of Data subject to any other restrictions or limitations? [text] or NO

The User is entitled to utilise software robots or other forms and applications of robotic process automation, 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.

PERMISSIONING

The following Data Rights Holders have permission to process the Data and, shall grant permissions to other Users to use the data, according to this Dataset Terms of Use:

[Data Rights Holder#1 Name_Surname, e-mail, Tel.nr.]

[Data Rights Holder#2 Name_Surname, e-mail, Tel.nr.]

.

.

[Data Rights Holder#N Name_Surname, e-mail, Tel.nr.]

Irrespectively of the above identified Data Rights Holders, the Data Provider always ensures that an adequate permissioning mechanism is in place to make sure that the Data Right Holders have control over their data to the extent applicable laws require, and the Data Users are able to get the permissions they need.

CEASE OF PROVISION OF THE DATA

The Data Provider may cease the provision of the Data by notifying the other Parties of the DADS 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.
(iii) Individual Data Providers of the Data can be identified from the Derived Material.
(iv) The Derived Material contains any Data Provider's Confidential Information.

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.

Derived Material shall preferably be shared and used under Creative Commons Attribution 4.0 International (https://creativecommons.org/licenses/by/4.0/) license terms.]

DISCLAIMER AND LIMITATION OF LIABILITY

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 3.3 and 11.1, 11.2 and 11.3 of the General Terms and Conditions and Permissioning clause above in these Dataset Terms of Use.

EFFECTS OF TERMINATION

Where the Accession Member's membership in the DADS is terminated as a consequence of the Accession Member's material breach defined in the General Terms and Conditions (Clause 10.8), the breaching Accession Member's right to use the Data will end at the date of the termination. The breaching Accession 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 Accession Member is entitled to retain the Data as required by the applicable law or competent authorities, provided that the breaching Accession Member notifies the Data Provider of such a data retention obligation by the date of termination.

ENTRY INTO FORCE AND APPLICATION

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

REFRAINING FROM SHARING DATA AND AMENDMENTS

The Data Provider may refrain from sharing Data within the DADS and change these terms and conditions (including but not limited to the content or quality of the Dataset) at any time by notifying all other Members to the DADS of such change in writing. The provision of Data will end, or the modified terms will enter into force within ninety (90) days after

the Data Provider has notified the other Members of the refraining from 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.

OTHER TERMS

For the avoidance of doubt, it is acknowledged that the 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

These Terms of Use are governed by and construed in accordance with the laws of Slovenia, 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 Ljubljana Arbitration Centre at the Chamber of Commerce and Industry of Slovenia (LAC).

ADDITIONAL AGREEMENTS RELEVANT TO THE DATASET

In acknowledgement of specific agreements relevant to the respective Dataset, the Data Provider provides the following appendices: [possibility to upload additional documents]

In _____, on xx.xx.20xx

[DATA OWNER]

_____

Name: [Name]

4.5 Governance Model

GENERAL PROVISIONS

The DIH AGRIFOOD Data Space (DADS) is established by the Constitutive Agreement, which is signed by the Founding Members of the DADS. This Appendix includes a description of the Governance Model of the DADS.

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

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

STEERING COMMITTEE

General

The Steering Committee is the ultimate decision-making body of the DADS. The purpose of the Steering Committee is to facilitate collaboration between all Parties and organise the administration of the DADS 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 any decision-making related to the DADS's business or to its legal, technical or ethical matters. The Steering Committee is responsible for preparing any changes required to ensure that the DADS continues to fulfil its purpose and meets the applicable requirements.

The Steering Committee is authorised to prepare any changes to the Constitutive Agreement, Accession Agreement or any of their Appendices and to approve any new Founding Members to the DADS 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 and if such approval is specifically required (defined in the Dataset Terms of Use) or in cases of disputes in initialising Datasets.

Composition, Meetings and Organisation

Each Founding Member appoints one representative to serve on the Steering Committee (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 Committee 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 who has requested the extraordinary meeting must send an email summarising the issue at hand and whether it is time sensitive.

At least one Steering Committee meeting per year shall be organised for openly inviting and including all Accession Members to be able to participate in the Steering Committee meeting and be able to raise any question, remark or proposal related to DADS.

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 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 DADS 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 Founding Members or the DADS, unless explicitly stated otherwise in the Constitutive Agreement or duly authorised by all Founding Members. 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 DADS 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 Founding Members to the DADS
- Approval of new Datasets and/or Dataset Terms of Use if they are subject to Steering Committee approval
- Operational and technical status of the DADS
- Any change requests concerning the DADS
- Acceptance of change request deliverables and monitoring their timelines
- Outstanding issues, open action points, conflicts at all levels of DADS, including those at the level of Founding members and Accession Members
- 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 DADS, 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 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 DADS with material negative impact vis-à-vis any of the Founding and/or Accession Members, must be agreed upon by a majority of 2/3 of Representatives present at the meeting.

New parties may join the DADS in the capacity of Founding Members by signing the Constitutive Agreement, and their accession must be approved by 2/3 of all Steering

Committee members. Appointment of the Steering Committee Chair must also be approved by 2/3 of all Steering Committee members.

Where the decision of the Steering Committee to amend the Constitutive Agreement would materially affect the rights or obligations of a Founding Member objecting to such amendment, the objecting Founding Member will be entitled to terminate the Constitutive Agreement by notifying the Steering Committee thereof in writing within fourteen days after the objecting Founding Member becomes aware of the Steering Committee's decision. This termination will become effective within thirty days as of the date on which the notice was submitted by the objecting Founding Member to the other Founding Members.

Subcommittees

The Steering Committee may authorise a subcommittee and/or the chair of the relevant subcommittee to explore a specific issue and/or to provide operational support to the DADS. Those subcommittees can either resolve ethical challenges and questions and/or provide dispute resolutions in DADS (Ethical and Dispute resolution Board), resolve technical issues, approve requests for the new datasets and provide technical guidance/support to the DADS Parties (Technical Board) or similar. The Steering Committee will appoint the chairs of the subcommittees and their members, in addition to defining their rules of procedure for operation.

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.

Subcommittee for Data Security

Trust among the DADS Parties is critical for the success of data spaces and sharing data, and adequate data security is a cornerstone of this trust. Therefore, a Subcommittee for Data Security is mandatory, responsible for developing, implementing, analysing and improving the Data security operating model for DADS to ensure secure processing of data and trust among DADS Parties.

Invited Attendees

The Steering Committee Representatives may invite necessary and appropriate persons to attend any Steering Committee meeting, which includes also relevant Accession Members, 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 DADS Member's organisation (Founding Member's or Accession 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 DADS, or the breach, termination or validity of the Constitutive Agreement and Accession Agreement must first be escalated to the Steering Committee. The Parties must strive to resolve any such conflict in good faith at the Steering Committee.

4.6 Description of the DIH AGRIFOOD Data Space (DADS)

4.6.1 DADS description – Business part

At the time of writing this Rulebook (the year 2026), the business model of a DADS is not fully defined yet. Some of the reasons for this are:

- European Data Space is a relatively new concept in the field of data economy
- Organisational and technical standards for data spaces are still in development
- Time is needed for the wide acceptance of the principles of data spaces among data providers, service providers, data users, other stakeholders, and the general public.

DADS, as an organisation, is a nonprofit organisation. However, it will create business value. Such business value does not necessarily need to be monetary but can manifest in a better product or service quality for all stakeholders and the general public.

Organisational and technical infrastructure support data monetisation, so data Providers and Service Providers, if they choose so, can enforce different monetisation models (e.g., in Dataset Terms of Use, or enforcing the payment through x402 protocol in DSX Engine).

The goal of implementing transformative data economy and its future business models in agrifood systems in the European Union is ambitious. To work towards a reality in which everyone benefits from this technological shift we need decentralized, community based interoperable solutions that can navigate the diverse realities and regulatory landscapes of the EU. These solutions are a step forward from how digital agriculture is often done today; instead of locking access to data and rendering it proprietary, voluntary contributions to a shared ecosystem can become the norm. Federation has proven to be a model to follow.

A federated model lets each partner control its own data, tools and infrastructure while still taking part in the wider network. Partners decide how much access to grant, on what terms and to whom, allowing partners to match the federated data sharing requirements to their own strategy and risk appetite. At the same time, partners can tap into technology, knowledge and services pooled by others. Federated systems thrive when participants share widely: opening resources to the broader network yields larger gains for each member and even greater benefits for the community.

By embedding FAIR principles and interoperable standards from the outset, a weather-risk algorithm coded in Poland can learn from Slovenian datasets without moving sensitive information, and a soil-health model built by a startup can speak the same language as a government registry. Most importantly, these federated digital commons put smallholders, cooperatives and public agencies on equal technological footing with large companies, turning shared infrastructure into a shared opportunity.

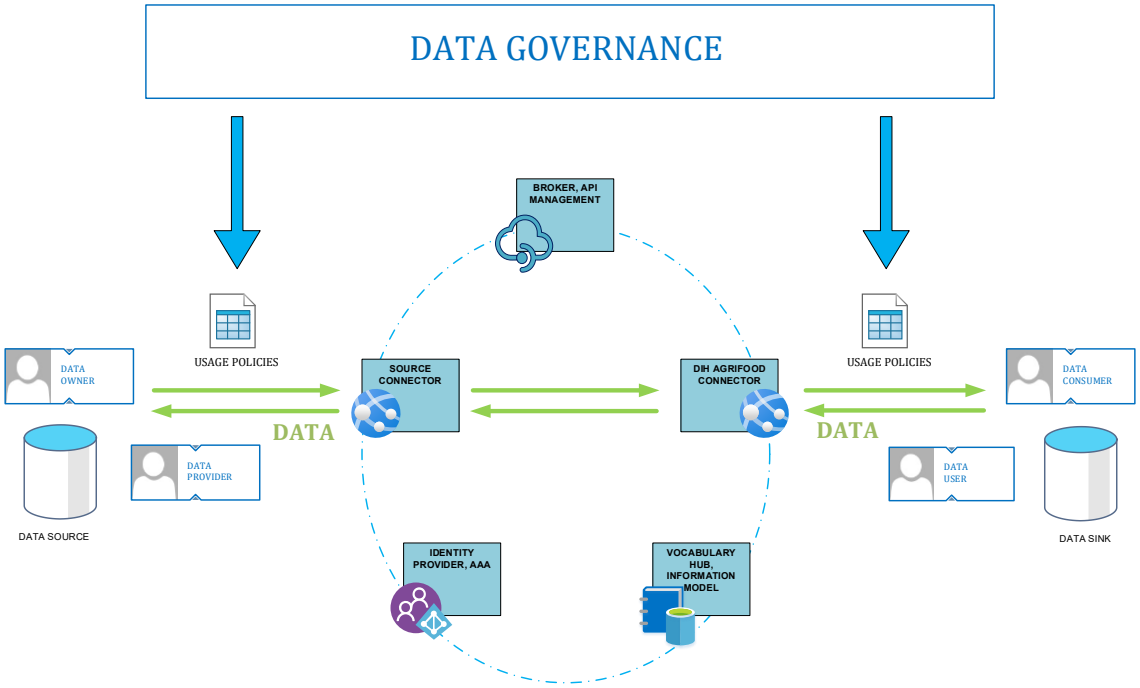


Figure 5: A business overview of the organisational and technical infrastructure of DADS

4.6.2 DADS description – Technical part

The technical infrastructure for DADS is hosted and deployed on the cloud service provider, where it datacentres resides in European Union. The Founding members of DADS are responsible for developing and maintaining the technical infrastructure.

Their responsibility also includes ensuring that services in DADS comply with modern standards regarding:

- Data security
- Backup of data
- Disaster recovery
- Compliance of services with national and EU legislative acts
- Technical documentation

Data sharing platform

Identity and Access Management – DADS uses Azure AD B2C as its identity management solution. Azure AD B2C is a business to customer identity as a service that provides a scalable identity platform; it allows customers to sign in using social, enterprise or local accounts and supports millions of users while handling security threats such as denial of service and brute

force attacks. In the DADS platform, Azure AD B2C provides signup/sign-in flows and implements federation with external identity providers. This ensures that data providers and data users authenticate securely using standards based protocols like OpenID Connect and OAuth 2.0, and that identity lifecycle management (registration, password reset, multi-factor authentication) is handled by a trusted cloud service.

Consent Management Platform (CMP) – This is a custom web application integrated with Azure AD B2C that allows data providers to create, view and manage consents for sharing their datasets, and enables data users to request access. The CMP provides a dashboard where data providers can grant or deny access to specific datasets, record the purpose and duration of each consent, and audit all data sharing interactions. The platform also issues and manages API keys that are bound to particular consents, ensuring that every API call can be traced back to a respective data user. By centralizing consent management, DADS ensures compliance with the Code of Conduct for Agricultural Data Sharing and provides transparent governance for personal and non personal data, aligned with European policy and regulatory framework.

API Market Service – The API Market service exposes datasets as programmable interfaces. It leverages Azure API Management, which comprises an API gateway, management plane and developer portal. The API gateway acts as a proxy to the back end services; it accepts API calls, routes them to appropriate data providers, verifies API keys and other credentials, enforces quotas and rate limits, and can transform requests and responses according to policy statements. It also caches responses to improve latency and emits logs and metrics for monitoring and troubleshooting. The developer portal is an automatically generated, customizable website that allows developers to discover and consume DADS APIs. Through the portal, data users can read documentation, test APIs in an interactive console, and download OpenAPI specification. By integrating these components, the API Market service gives data providers control over how their datasets are exposed and enables data users to integrate datasets into applications securely.

Platform architecture – Technically, the DADS platform is built as a micro service architecture with a web front end (developed using the Quasar framework) and back end services deployed in the cloud. Identity management, consent management and API management are deployed as managed services, while custom components handle dataset ingestion, metadata cataloguing and user dashboards. The platform logs all actions for accountability and auditing, and exposes an internal administration API to allow integration with other data spaces. Data providers can publish datasets to the platform via secure upload interfaces, define usage policies, and associate them with API endpoints. Data users discover available datasets through the developer portal or catalogues, request access via the CMP, and consume them through documented APIs. This modular design enables DADS to evolve as standards for data spaces mature and facilitates interoperability with future dataspace connectors.

Data Space

A data space is a federated, decentralized data infrastructure designed to enable cross organizational data sharing scenarios. Rather than centralizing all data, data spaces provide mechanisms such as distributed data sharing and metadata sharing to facilitate secure and trustworthy data exchange. They guarantee data sovereignty by ensuring that the data provider maintains control over who can access the shared data and under what condition. Reference architectures such as the International Data Spaces Association (IDSA) model define layers and components of a data space: the system layer includes data space connectors, a metadata broker, clearing house, app store, vocabulary hub and identity provider. Connectors provide access to data and verify participant identities, the clearing house logs transactions and events.

Dataspace connectors and the EDC framework – DADS adopts the Eclipse Dataspace Components (EDC) framework as the basis for its dataspace components. The EDC framework is an open source technology designed to enable sovereign, secure and policy controlled data exchange between organizations. It facilitates data sharing via a contract based exchange mechanism in which both parties agree on digital contracts that define who can access the data, for what purpose and under what conditions; these agreements are governed by machine readable usage policies that the connector enforces automatically. The EDC architecture follows a dual plane approach: the control plane acts as the core that manages contract negotiations, policy enforcement, service extensions, data transfer coordination and authentication/authorization, while the data plane handles the actual transfer of data using protocols like HTTPS and implements security measures during transfer. The framework includes core capabilities for data transfer, contract negotiation, access policy enforcement and service extensibility; an identity management subsystem that supports decentralized identities and OAuth2 authentication; a policy framework that defines and enforces usage control policies; and data management components that catalog available assets and ensure data integrity.

DSX Engine enhancements – The DSX Engine extends the standard EDC framework to provide a decentralized dataspace. It introduces a decentralized participant discovery extension that connects each connector to a blockchain smart contract, allowing connectors to register and deregister themselves and maintain an up to date list of participants. When a connector starts, it calls smart contract functions to register itself; when shutting down, it deregisters. Extensions then listen to blockchain events to update the participant list, and crawlers automatically dispatch to discover catalogs from other participants. DSXE also integrates decentralized identity mechanisms by adding support for Ethereum (did:ethr) and European Blockchain Services Infrastructure (did:ebsi) decentralized identifiers, which are resolved through blockchain based registries. This allows participants to manage their own identities without relying on a central identity provider. Another extension implements a decentralized clearing house, storing logs of asset creation, contract negotiations and catalog lookups on a blockchain, ensuring tamper proof audit trails. DSX retains all core EDC functionalities: control plane, data plane, identity hub and federated catalog; but enhance them with blockchain based discovery and auditing. Contract negotiations remain a core feature: participants

initiate negotiations by sending a contract request through the management API, referencing the asset and its policies. Once both connectors agree, the contract state becomes “Finalized,” and data transfer proceeds through the provider’s data plane, either via a push to the consumer’s endpoint or a pull by the consumer. The DSXE also support monetization models through support for x402 protocol, where payments are automatically executed with ERC-20 based tokens.

Implications for DADS – By integrating the DSX Engine, DADS extends its data sharing platform into a IDSA compliant dataspace. The connector acts as a gateway between an organization’s internal systems and the dataspace, enforcing data usage policies, handling contract negotiations and orchestrating secure data transfers. The metadata broker and vocabulary hub ensure that datasets published by different providers use consistent semantic models, enabling discoverability and interoperability. The clearing house component records transactions in a tamper proof manner, providing verifiable audit trails that ensures trust among participants. By adopting decentralized identity mechanisms, DADS empowers participants to control their credentials and reduces reliance on centralized authorities. The dataspace architecture also supports future monetization models: usage policies and smart contracts can specify payment terms, through x402 protocol and blockchain based tokens can automate compensation. Together, these components allow DADS to evolve from a single data platform into an interoperable node in the emerging network of European data spaces.

5. DIH AGRIFOOD Data Space Code of Conduct

The DADS is based on key principles of data collection and sharing, which shall be aligned with the Code of Conduct for Agricultural Data Sharing by Contractual Agreement[7]. The majority of those key principles are adopted in the DADS functionality in the best possible manner while being subject to constant upgrades and advancement of the DADS platform/system.

There is, however, a need to establish more detailed and commonly accepted norms that make cooperation between DADS Parties more efficient, while leveraging the building of trust in a data network such as DADS. This Code of Conduct (CoC) is based on respect between different stakeholders, transparent communication and the ambition to seek the values that are commonly acceptable.

This CoC is applicable to all DIH AGRIFOOD Data Space Parties and stakeholders, while it advises them on the main principles related to the rights and obligations of using and sharing data. Acknowledging and complying with this CoC ensures that the DADS Parties and stakeholders are all making sure and are confident that data is secured and handled in an appropriate manner and that all relevant regulations are secured (especially General Data Protection Regulation – GDPR for the personal data). Compliance with this CoC is mandatory for all DADS Parties that want to share or use data.

Accountability and Auditability

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

Avoid harm

All Parties and stakeholders in the DADS should avoid causing harm but instead focus on creating value (direct or indirect) for the whole DADS environment and all the people that are affected by the actions of the DADS.

Justified Processing of Personal Data

7 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi37ufu6KP8AhWocfEDHVg6Ci0QFnoECAgQAQ&url=https%3A%2F%2Ffefac.eu%2Fwp-content%2Fuploads%2F2020%2F07%2Feu_code_of_conduct_on_agricultural_data_sharing-1.pdf&usg=AOvVaw320fQ9hEpAvyLa9jASzaYA

Personal data shall be processed on a fair and lawful basis, like for example on the basis of an informed consent of the individual, in accordance with a contract with the individual, a legal obligation, a vital interest of the individual, in the public interest, or for the purposes of the legitimate interests, given that the interests and fundamental rights and freedoms of the individual are not threatened, in particular where an individual is a person who is not knowledgeable of threats associated with processing of personal data (marginalised groups, children, specific sectoral actors like farmers, etc.).

Fairness, justice, and equality

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

To ensure fair use of their information, individuals are granted true possibilities to understand and control their personal data that is collected, transferred and otherwise processed in the DADS.

The rules and the structure of the DADS secure the benefits and rightful expectations of all the Parties. This requires a balanced power structure in the DADS and transparent consensus-oriented governance.

Human-centricity and support for individuals

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

All the Members of the DADS should support individuals in (a) getting information about the use of their personal information, (b) understanding information, practices, contracts, and their consequences, and (c) participating, contributing, and influencing systems and practices when using personal information of those individuals. The aim is to ensure that if individuals need information or have justified demands for information, they are given the required and appropriate support (guidelines, personal help, etc.) in transparent ways. The emphasis should be on creating accessible, low-barrier means for individuals to review how their personal information is being used.

Privacy

Privacy is one of the central issues in the data economy. Therefore, privacy must be respected and protected. The DADS is based on the use of information, which sets high demands for privacy, as information can be sensitive and private. Thus, this means that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the individuals.

Personal data shall be collected for specified, explicit and legitimate purposes, and it shall not be processed further in a manner that is incompatible with those purposes. Only personal data, which are adequate, relevant and limited to what is necessary in relation to the expressed purposes, shall be processed.

Organisations do not collect personal information that they do not need. All the personal data that is processed has to be necessary for a specific use. The Parties of the DADS take reasonable measures to ensure that personal data is accurate and up to date. Personal data must not be stored longer than allowed or necessary for the purposes for which the personal data is processed.

To ensure the integrity and confidentiality of privacy, personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

To preserve the integrity, confidentiality and availability of the data, organisations need to develop and implement an information security policy framework. When merging datasets, privacy should be guarded even more carefully than normally. Anonymisation of data is recommended whenever feasible.

Any organisation must also be accountable, i.e., it needs to be able to demonstrate its compliance with the principles mentioned above. Therefore, the processing of personal data must be planned and documented. There should exist clear, documented processes for data collection, storage, use, and distribution.

For collected data, there needs to be a clearly documented life cycle plan where the collection, archiving and possible erasing of data are described. The relevant parts of the life cycle plan are available to Data Owners and individuals related to their data.

Security

All the Parties of the DADS are responsible for ensuring that their collection, use, storage, sharing, and other processing of data are secure. This means that proper security solutions and processes are used, and also that monitoring, patching, and reporting of security issues are properly designed.

Personal data on individuals must be properly secured, and the risks to the rights and freedoms of individuals should be analysed. All the necessary technical, organisational and personal actions must be implemented to minimise security threats to individuals whose information is processed. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, all the DADS Parties shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

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

Sustainability and Circular Economy

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

Transparency

The DADS is based on co-operation and respect for information sources. Transparency is important to develop trust. The data shall be processed lawfully, fairly and in a transparent manner. Any information addressed to the public or to individuals must be concise, easily accessible, easy to understand, and clear and plain language and, additionally, where appropriate, visualisation is used.

This does not mean that information is open to everybody without restriction. Instead, it means that all the DADS Parties should know (when/if possible) what data are offered in the DADS and by what requirements to promote transparency of the DADS. To support a real-time economy, the DADS Parties do not unnecessarily detain data but share it as soon as possible.

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

Continuous improving

Ethical issues vary, and different issues may come up on a case-by-case basis. Thus, ethical evaluation should be a continuous process in an organisation, and there should be institutional support for this. Therefore, the management of a DADS Party should support the organisation's employees by ensuring that they have real opportunities to uphold, promote, and respect the principles of the Code of Conduct.

Ethics is implemented in the daily actions of individuals, or it is not implemented at all, as only an individual can make a moral decision. However, without institutional support for ethical decisions, there is a higher risk of unethicality as individuals lack the needed autonomy to make moral decisions.

Communication

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

6. Data Security Operational Model

These instructions set out the principles for developing a data security operating model for DADS and represent a framework model for the Subcommittee for Data Security, responsible for managing and steering this important element in DADS. Data security needs vary considerably in different data spaces, so it is important to tailor the operating model for the DADS and update it with sufficient frequency.

Data security has been considered from the outset, already when planning the operations, and it is understood as a continuous activity throughout the life cycle of data sharing. The data security operating model is not part of the constitutive agreement of the DADS per se; it is therefore important that the rights and obligations critical to data security are provided as separate provisions hereafter.

The following diagram represents the development process of the data security operating model for DADS:

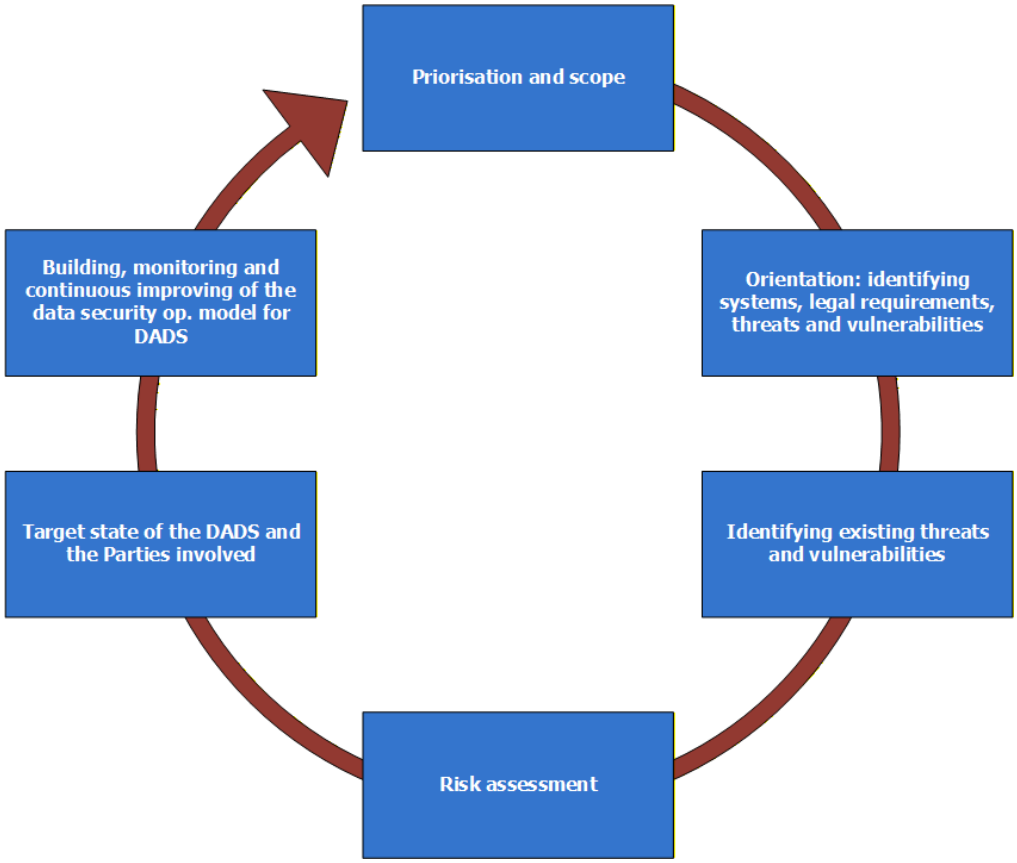


Figure 6: Data Security Operational Model for DADS

1. Prioritisation and scope

The Founding Members of the DADS appointed a Subcommittee for Data Security involving representatives of all Founding Members to prepare and implement an operational Data Security Operating Model.

The Subcommittee for Data Security is entitled to define the scope of data security covered by the DADS and determine the specific objects of protection (such as data covered by the rulebook, DADS Members or other assets).

The Subcommittee shall take into consideration all relevant national and EU legislation addressing Data security. In case of personal data, the data protection legislation shall be applied, with the key legislation being the EU's General Data Protection Regulation (GDPR), which applies to all processing of personal data. In addition, depending on the situation, national data protection provisions and provisions covering special sectors may also apply.

2. Orientation: identifying system, legal requirements, threats and vulnerabilities

Once all data security items outlined in the rulebook have been prioritised and specified, the objectives for data security shall be defined, along with the management methods to achieve them.

The Subcommittee shall define the objectives of the entire DADS with regard to data security, while individual Parties are also able to define their own objectives with regard to the DADS. Depending on the type of data shared and the sector of operation, compliance with relevant special legislation may be required.

Once objectives are set, appropriate data security management methods shall be identified. These methods typically fall into three categories: administrative, technical, and physical measures.

- Administrative Measures: Focus on risk management, security documentation, personal security, and training.
- Technical Measures: Utilise software or hardware solutions, such as centralised log management, firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and identity and access management systems.
- Physical Measures: Protect resources and personnel through means like fences, locks, lighting, and camera surveillance.

It is important to consider all different means of data security management to ensure that the DADS can reach a sufficient level of data security. Employing multiple layers of control, known as multi-layer protection, creates a robust defence around the assets being safeguarded.

At this stage, the focus should be on broadly exploring the available data security management methods. It is advisable for the DADS and the Parties involved to select the management methods best suited for their specific circumstances only after carrying out the security risk assessment process described below.

In the traditional local deployment model of applications, each organisation's sensitive data remains within the organisation and is subject to its physical, logical and personnel security and access control policies. However, the cloud model commonly used by data spaces stores the data outside the organisation's boundaries. For this reason, additional security checks must be carried out to ensure data security and to prevent data security breaches caused by data security flaws or malicious employees.

In the following, information security threats are discussed especially from the perspective of how they affect data sharing in data spaces:

Using data in a manner incompatible with the purpose

Data may also be used for purposes not agreed in the Constitutive Agreement and/or Accession Agreement or in the Dataset Terms of Use or not considered in the rulebook. This may bring up issues that the Data Provider has not taken into account, but to which it has committed itself. Typically, this involves harm suffered (e.g., data reveals some matters that the Party does not want to share) or some other Party building business from this without sufficient compensation to the Data Provider. Another subset of this is building and using models to replace data.

Data leaks

A data leak occurs when data ends up with the wrong party, deliberately or unintentionally. This may occur either through an IT error (close to traditional data security threats) or by a party transmitting the information, its subset or a data model built from the data to a third party. In data leaks, mistakes made by users and incompetence often play an essential role. These can be reduced by means of education and training. Data leaks may also take place in such a way that data has been used for a purpose, such as teaching artificial intelligence, with some confidential information having remained in the AI model, which may thus leak to outsiders through the model.

Responsibility for data

Data integrity issues arise when the data does not match agreed standards, is incorrect, or has been altered. These concerns inherently involve questions of liability: who is accountable if the data deviates from what was agreed or expected, or if it has been modified? These matters are addressed in detail in the contractual framework of the rulebook, especially in sections 3 Role-specific responsibilities, 5 General responsibilities and 11 Liability, and potential exceptions and specifications concerning them in the Constitutive Agreement and the Dataset Terms of Use.

Additionally, data liability may include unforeseen responsibilities, such as new obligations emerging from evolving regulatory interpretations – particularly concerning personal data processing. As data protection legislation continues to be clarified by authorities, unexpected liabilities may arise. By definition, it is difficult to take such eventualities into account, but to a certain extent, it is possible to take a stand on who will bear responsibility for them in the agreements.

Accidental sharing of data

Not all data loss events are the work of sophisticated cybercriminals. A significant number of breaches stem from employee errors, such as accidentally sharing, misplacing, or mishandling sensitive data. Employees may inadvertently grant access, lose devices, or process information improperly due to a lack of awareness about security practices. Careless handling of data storage devices, such as leaving them in public places or failing to secure them properly, further exacerbates the issue.

Another security threat related to people is the limited opportunities of the organisation's cybersecurity team to monitor all risks. System administrators are often overworked when trying to protect sensitive information. This leaves companies exposed, and it should increase the impetus to

implement automation wherever and whenever possible, without forgetting that automation itself may entail different risks.

Phishing and social engineering

Social engineering attacks are a primary vector used by attackers to access sensitive data. They involve manipulating or tricking individuals into providing private information or access to privileged accounts.

Phishing is a common form of social engineering. It involves messages that appear to be from a trusted source, but in fact are sent by an attacker. When victims comply, for example, by providing private information or clicking a malicious link, attackers can compromise their device or gain access to a corporate network.

Phishing emails are on the rise. At the same time, new technology and increased information accessibility are making these attacks more sophisticated, increasing the likelihood that hackers will successfully infiltrate IT systems. Despite every business's best efforts, these malicious messages may make their way into employees' inboxes. Managing this traffic and equipping employees with tools, education and training to defend against these threats will be critical.

Email addresses and passwords are in particularly high demand by cybercriminals. This is the primary data stolen in data breaches. Since this information can be used to deploy other, more diverse attacks, every company needs to be aware of how its data could be used against it.

Insider threats

Insider threats are employees who inadvertently or intentionally threaten the security of an organisation's data. There are three types of insider threats:

- Non-malicious insider – these are users who can cause harm accidentally, via negligence or incompetence.
- Malicious insider – these are users who actively attempt to steal data or cause harm to the organisation for personal gain.
- Compromised insider – these are users who are not aware that their accounts or credentials were compromised by an external attacker. The attacker can then perform malicious activity, pretending to be a legitimate user.

When companies consider their cybersecurity risks, malicious outsiders are typically at the top of their minds. Indeed, cybercriminals play a prominent role in some data heists, but company employees promulgate many others.

One form of insider threat is bribery. Company data and intellectual property are both incredibly valuable, and in some cases, employees can be bribed into revealing this information.

Ransomware attacks

Ransomware is malware that infects corporate devices and encrypts data, making it useless without the decryption key. Attackers display a ransom message asking for payment to release the key, but in many cases, even paying the ransom is ineffective, and the data is lost. Many ransomware attacks

begin at the employee level as phishing scams and other malicious communications invite these devastating attacks.

Many types of ransomware can spread rapidly and infect large parts of a corporate network. If an organisation does not maintain regular backups, or if the ransomware manages to infect the backup servers, there may be no way to recover.

Data loss in the cloud

Many organisations are moving data to the cloud to facilitate easier sharing and collaboration. However, when data moves to the cloud, it is more difficult to control and prevent data loss. Users access data from personal devices and over unsecured networks. It is all too easy to share a file with unauthorised parties, either accidentally or maliciously.

Bad password hygiene

Login information on the internet can be vulnerable to credential stuffing attacks that use stolen information to inflict further attacks on a company's IT network. Many login credentials are compromised in previous data breaches, and with many people using redundant or easy-to-guess passwords, that information can be used to access company data even when the networks are secure. Therefore, best practices like requiring routinely updated passwords are a simple but consequential way to address this preventable threat.

3. Identifying existing threats and vulnerabilities

Once the data security objectives have been defined and the management methods identified, it is advisable to assess and document the current situation. In this respect, the situation is significantly different if data is already shared between the parties in some way compared to the situation in which data sharing is only about to begin.

How has data security been ensured to the extent that data is already being shared between the parties? What will change from a data security perspective when data is shared in accordance with the rulebook?

In this matter, it is also worth taking into account the legal requirements and the extent to which international regulations, such as those at the EU level, and national provisions in different countries must be taken into account.

The key question is whether the data is shared directly between the Parties or whether the data is stored somewhere in a central repository from where each party can retrieve it. This also has an essential impact on assigning the data security management requirements to the right Parties. One option can be using an escrow-type operator, a reliable third party, which will manage certain obligations against a fee.

4. Risk assessment

As described above, the DADS and its participants must identify security threats and vulnerabilities. Next, they assess the severity of the risks by determining the likelihood of each threat and the extent of the damage in the event that the threat materialises.

In DADS, assessing risks is primarily the responsibility of the Subcommittee for Data Security, and particular attention should be paid to the perspective of the entire DADS.

The severity of the risk is the product of likelihood and the extent of damage. Since assigning a numerical value for the likelihood or the extent of damage can be quite difficult, in practice, it is often best to use some kind of classification in the risk assessment, such as a three-step approach, and then place the risks in a matrix where one axis represents the likelihood and the other the extent of damage. This makes it easier to identify the risks which are the most serious and require the most attention.

Risk Management encompasses the processes and practices used to identify, assess, and mitigate risks, as well as assign responsibility for these actions. To ensure consistency, the DADS should establish common operating procedures for risk management, particularly for risks affecting the entire DADS. The data security operating model should include clear definitions and guidelines for all aspects of risk management to support the collective security of the DADS.

5. Target state for the DADS and the Parties involved

Once the risks have been assessed, the Subcommittee for Data Security can agree on the target state of information security for the entire DADS and its individual Members. Regarding the extent to which the Parties want to make the target state legally binding, it is necessary to include these in the binding terms and conditions of the Constitutive Agreement, the Accession Agreement or the Dataset Terms of Use.

The DADS must have a common intent regarding the risk level and the extent of the measures. This may require a considerable number of negotiations and coordination of objectives, especially if the levels of knowledge, expertise and security requirements vary among the DADS participants. Depending on the nature of the DADS, the target state is documented by describing, for example, what the DADS aims to achieve in the following areas:

1. Data security policies
2. Personnel safety and security
3. Management of the data to be protected
4. Access control
5. Encryption
6. Physical and environmental safety
7. Operational safety
8. Communication security
9. Acquisition, development and maintenance of systems
10. Relations with suppliers
11. Security incident management

12. Data security aspects related to business continuity management
13. Compliance

5. Building, monitoring and continuous improving of Data security op. model for DADS

Once the target state has been defined, a Data security operating model to support the achievement, maintenance and continuous improvement of the target state will be built. It includes topics such as:

Organisation of data security

DADS Governance model established a steering committee subgroup (Subcommittee) to ensure information security and the achievement, maintenance and development of its target state. As part of organising data security, responsibilities for who reacts if any risks materialise and in what manner should be defined. This includes not only immediate measures to limit and rectify damages, but also communication and learning from what has happened.

The GDPR usually obliges parties involved to report personal data security breaches to the Data Protection Ombudsman and, in certain cases, the persons affected as well. As a rule, a notification to the Data Protection Ombudsman must be submitted no later than 72 hours after the data security breach has been discovered. This is such a short time that it is a good idea to plan in advance how to react to a data security breach and report it, so that it is not necessary to start considering it only after the breach has occurred.

Management's commitment to data security

Ensuring the management's commitment is essential for the data security operating model. Therefore, the Founding Members must identify the person or party who is in a leadership position regarding data security in the DADS and ensure their commitment to achieving the target state.

How is data security measured?

The DADS should agree on indicators for measuring data security. What indicators are used is essentially dependent on the type of DADS setup. The indicators should be defined in such a way that they are related to the objectives set above, that the Parties can influence them through their own measures and that they are particularly significant in terms of the risks assessed as most serious above.

What kind of audits and reviews are carried out in the DADS?

In order to build trust, the data security process must be sufficiently transparent. In particular, it is worth investing in transparent risk management of the DADS.

To ensure data security, it can also be agreed that the Parties have the right to audit and review each other's systems and facilities. If such audits and reviews are deemed necessary, a term could be included in the Constitutive Agreement, the Accession Agreement, the Dataset Terms of Use or the Governance model that obligates Parties who may be subject to such measures to allow access to their systems and facilities. The term must be so unambiguous and clear that there is no doubt about who it concerns, what the audit or review may focus on, who can perform it, who is responsible for the costs arising from it and what kind of confidentiality obligations the Party performing it has.

Documentation of the DADS's data security model

The data security operating model for the DADS will be incorporated into the DADS's rulebook. As a rule, it is a document which describes the mutual understanding between the Parties, but is not a contractually binding part of the Constitutive Agreement. Therefore, all obligations that should be contractually binding on the Parties must be recorded separately in the relevant sections of the Constitutive Agreement or its annexes. It is also possible to include the entire data security operating model as a binding annexe to the Constitutive Agreement. However, this may make the operating model too rigid when it should be possible to reform and maintain it in a flexible manner.

As regards documentation, it is also worth noting that Article 30 of the GDPR requires that a record of processing activities of personal data be maintained. This must also be made available to the supervisory authority on request, allowing them to assess the lawfulness of the processing activities. Furthermore, in accordance with Article 5, the controller has a general obligation to be able to demonstrate compliance with the regulation (accountability) at all times.

Continuous improving: how to ensure data security continuity and process development?

As the DADS develops, operations change and new Parties bring new needs to the DADS, it is important to ensure that data security remains at the desired level and that the data security process of the DADS is continuously improved. It is advisable to enter separately in the Governance model how the data security operating model is reviewed and updated whenever necessary and at agreed intervals.

Changes in the purpose of use of data and their management

The purpose of the use of data is defined in the specific Dataset Terms of Use. This is essential for the implementation of 1) the purpose limitation of data protection and 2) data access rights.

The purpose limitation of data protection in accordance with the General Data Protection Regulation (GDPR) restricts the purposes for which the controller can use information collected on people. There are two important aspects in purpose limitation: personal data shall be collected for specified, explicit and legitimate purposes (purpose specification) and not further processed in a manner that is incompatible with those purposes (compatible use). While data collected for one purpose may be processed for another, this is only permissible if the new purpose aligns with the original intent. This principle balances the protection of data subjects' expectations with the need for further use of personal data within defined limits.

However, when it comes to the rights of use, the essential question is for what purposes the holder of the rights, such as the holder of copyrights, producer's rights or the right to data based on the protection of trade secrets, has allowed the use of the data. Normally, they do not have the right to use it for any other purposes.

In other words, the basic rule is that data may not be used for purposes other than those specified. However, the circumstances change, new needs may arise for the parties to the DADS regarding data, and new Parties joining the DADS may bring with them needs that could not be anticipated. Therefore, there may be good grounds for changing the purpose of use. When such a need arises, it must be determined how it can be done in accordance with data protection legislation, such as by asking people

for their consent to process their personal data for a new purpose. On the other hand, it is usually necessary to negotiate about the terms of use that can be reformulated with the holder of the rights if the holder has the right of veto on the new purpose, and it does not fall within the scope of the old definition.